25th ANNIVERSARY CIO&LEADER
TRACK TECHNOLOGY • BUILD BUSINESS • SHAPE SELF

State of Enterprise Technology Survey

2024

In association with

bmnxt
business & market advisory

Contents

MANAGEMENT
Managing Director: **Dr Pramath Raj Sinha**
Printer & Publisher / Editorial Director: **Vikas Gupta**
Executive Director - B2B Tech:
Sachin Nandkishor Mhashilkar (+91 99203 48755)

EDITORIAL
Group Editor - 9.9 Group: **R Giridhar**
Executive Editor - B2B Tech: **Jatinder Singh**
Correspondent - B2B Tech: **Praneeta**

CONSULTING ANALYST
Founder Analyst & Chief Research Officer, BM Nxt: **Deepak Kumar**

DESIGN
Creative Director: **Shokeen Saifi**
Sr. Designer: **Vipin Rai**

SALES & MARKETING
Director - B2B Tech: **Vandana Chauhan (+91 99589 84581)**
Sales Director - B2B Tech: **BN Raghavendra (+91 98453 81683)**
National Sales Head (CSO Forum): **Vaibhav Kumar (+91 97176 74460)**
Senior Manager Brand & Strategy: **Pratika Barua**
Brand Manager: **Sheena Dawar**

COMMUNITY ENGAGEMENT & DEVELOPMENT
Head - Projects:
Dipanjan Mitra
Senior Manager - Community Development:
Neelam Adhangale
Assistant Manager Community Development:
Vaishali Banerjee
Assistant Manager Community Development:
Snehal Thosar
Assistant Manager Community Development:
Shabana Shariff
Assistant Manager Community Development:
Reetu Pande
Senior Executive Audience Development:
Merly Davidson

OPERATIONS
Head - Digital & Event Operations: **Naveen Kumar**
Head - Digital Operations: **Atul Kumar Pandey**
Senior Executive Commercial: **Nitika Karyet**

PRODUCTION & LOGISTICS
Senior Manager - Operations: **Mahendra Kumar Singh**

Preface

The second edition of the annual CIO&Leader research report, State of Enterprise IT in India, is being produced this year in collaboration with consulting firm BM Nxt. It draws on the insights from more than 350 IT decision-makers, and serves as a crucial indicator of the technology trends in Indian organizations.

The study, based on a survey combining both qualitative and quantitative approaches, was conducted between April to July 2024, and provides a comprehensive overview of technology deployments, challenges, and future plans. It covers key areas including Cloud Infrastructure, Security, Data Analytics, and Artificial Intelligence (AI).

Led by the CIO&Leader Research team and Deepak Kumar, Founder Analyst at BM Nxt, the research highlights interesting trends—from the transformative impact of AI to the persistent reliance on on-premise solutions despite the growth of cloud technologies.

The study reveals a robust interest in deploying AI, though it also underscores a significant gap in organizational readiness. Enterprises are advancing in their use of AI and ML, with CIOs spearheading initiatives to drive business outcomes, improve efficiency, and foster innovation. AI and ML are increasingly integrated into key business functions, including IT operations, customer services, and sales.

There is a growing maturity in data aggregation and organization, with an anticipated expansion into advanced analytics and AI. However, CIOs recognize that human factors remain a critical vulnerability. To address this, improved training, enhanced security automation, and a vigilant organizational culture are essential to mitigating the impact of security incidents.

Challenges persist, such as demonstrating AI's value, identifying relevant use cases, and ensuring regulatory compliance. Nevertheless, executive leadership is showing increased willingness to invest in these technologies.

This study is rich in data, and has detailed analysis on the adoption of various tools, technologies, and processes across the broad enterprise IT categories covered. It is duly supplemented by a comprehensive analysis of trends–and comparisons with last year's survey data. We are hopeful that CIOs and IT leaders will find this report a useful aid for decision-making and strategy planning.

Beyond data, this report also reflects the aspirations and challenges faced by Indian enterprises in the digital era. It acts as a guide to the future trajectory of enterprise IT in India by leveraging qualitative insights from leading CIOs and CTOs.

We are grateful to all IT leaders who participated in this study, and offered their frank views and valuable perspectives through their responses. Your contributions have greatly enriched the depth and breadth of this study.

We welcome your feedback on this report and look forward to enhancing its utility in future editions.

R. Giridhar
Group Editor
9.9 Group

Jatinder Singh
Executive Editor
CIO&Leader

Executive Summary

The State of Enterprise Technology 2024 is a comprehensive annual study presented by CIO&Leader that presents dominant technology trends shaping Indian businesses. The report is based on an extensive survey conducted by CIO&Leader and BM Nxt to capture the current adoption levels and trends of various IT technologies and solutions across enterprises in India. The survey, conducted during June 2024, focused on four broad segments: AI & ML, Cloud & Infrastructure, Data & Analytics, and IT Security. Additionally, AI was probed as a horizontal theme. The survey results have validated that AI is actively interlaced with all the other four segments, underscoring AI's pervasive influence in modern IT strategies.

AI stands at the forefront of today's technological evolution, promising unprecedented advancements in efficiency, decision-making, and automation. However, AI also poses significant threats to employment, fueling the fires of neo-Luddism. Jobs that involve routine tasks, data analysis, and even customer service are increasingly at risk of automation, leading to widespread concerns about job security. However, the counterview is that as AI takes over routine and repetitive tasks, it frees up human workers to focus on more complex, creative, and strategic activities. This can lead to the creation of new jobs through AI-driven innovation.

> The survey results have validated that AI is actively interlaced with all the other four segments covered in this survey, underscoring AI's pervasive influence in modern IT strategies.

This apprehension is not unfounded. Studies suggest that AI and automation could displace millions of jobs worldwide. The World Economic Forum predicts that by 2025, automation could supplant 85 million jobs, even as it creates 97 million new roles. This dichotomy between job displacement and creation underscores the need for proactive measures to mitigate the adverse effects of AI on employment.

Despite the challenges posed by AI and the echoes of neo-Luddism, enterprise IT and infosec leaders are driving innovations to leverage technology for sustainable business growth. By adopting a strategic approach, these leaders are integrating AI with other IT technologies, such as cloud computing, analytics, and IT security, to enhance operational efficiency and competitiveness.

For instance, cloud computing offers scalable and flexible infrastructure, enabling businesses to deploy AI solutions efficiently. This synergy between AI and cloud computing accelerates innovation and drives business agility. Analytics also plays a crucial role in harnessing the power of AI. Advanced analytics tools can process vast amounts of data, uncovering actionable insights and enabling data-driven decision-making. By combining AI with analytics, organizations can gain a deeper understanding of market trends, customer preferences, and operational inefficiencies, driving strategic initiatives and improving overall performance.

In the realm of IT security, AI-powered solutions are revolutionizing threat detection and response. Machine learning algorithms can analyze patterns and anomalies in network traffic, identifying potential security breaches in real time. This proactive approach enhances cybersecurity defenses and minimizes the risk of data breaches and cyberattacks.

> With over 360 respondents, the survey targeted a balanced mix of large and medium enterprises to ensure a comprehensive view of the industry's stance on IT adoption.

Furthermore, enterprise IT leaders are fostering a culture of innovation within their organizations. By encouraging cross-functional collaboration and embracing agile methodologies, they create an environment conducive to experimentation and continuous improvement. This culture of innovation enables businesses to stay ahead of the curve, adapt to changing market dynamics, and capitalize on emerging opportunities.

Survey Methodology: The survey methodology employed structured questionnaires distributed to CIOs, CISOs, and other IT leaders across various business sectors in India. A balanced mix of large and medium enterprises was targeted to ensure a comprehensive view of the industry's stance on IT adoption. With over 360 respondents participating, each segment received more than 100 completed responses, providing a robust dataset for analysis.

Study Overview

AI & ML: The survey delved into the adoption and impact of AI and ML across enterprises. A significant finding was the increasing integration of AI in IT security, with many enterprises currently leveraging AI for IT & network asset management (54%), monitoring & vulnerability management (48%), and incident response & remediation (47%). The future looks promising with substantial growth anticipated in the next 12 to 18 months in areas likeidentity & authentication management (56%) and governance & risk management (49%).

The timeline for AI implementation to tackle data gravity issues revealed that within the next 12 months, 48% of enterprises plan to enhance data processing strategies, while 46% aim to improve data management processes. Longer-term priorities include reduce risk through predictive analytics (37%) and improve cost management (31%).

AI's impact on cloud platforms is also noteworthy. Currently, AI is helping improve cloud orchestration and managementfor 31% of respondents and reducing cost to train and deploy AI models for 26% respondents. Looking ahead, AI's role in providing better functionality to address ethical and copyright concernsand delivering reliable industry-specific AI models is expected to increase substantially (for 49% of respondents in each case) in the next 12 to 18 months.

Cloud & Infrastructure: Cloud services are seeing widespread adoption, with Software as a Service (SaaS) leading the charge at 69% in production. Infrastructure as a Service (IaaS) follows closely at 68%. Enterprises are also exploring newer offerings such as Application Platform as a Service (aPaaS) and Security as a Service (SECaaS), with 54% and 35% adoption rates, respectively.

Cloud delivery models vary by application categories, with public cloud being a popular choice for office productivity as well as collaboration and communication solutions (56% each) and CRM and marketing solutions (52%). Private clouds are predominantly used for backup, DR, and BCP solutions (40%) and enterprise solutions like ERP, SCM, and HR (35%).

Key drivers for cloud adoption over the next 12 months include digital transformation and business innovation (83%), infrastructure modernization and performance upgrades (61%), and improving the speed and agility of infrastructure provisioning (59%). Security remains a top concern area, with 80% of respondents citing cloud security as a very important factor.

Data & Analytics: Data and analytics continue to be critical areas for enterprises. The survey highlighted that enterprises are focusing on enhancing their data strategies and policies. Data integration with third-party sources is already in production for 63% of respondents, and data warehouses are implemented by 58%. The importance of data governance policies is also growing, with 45% of enterprises having these capabilities in production.

Measures to ensure data integrity include data backups (70%), data security controls (63%), and data encryption (58%). The maturity level of advance analytics usage across business functions such as business planning and strategy (37%), sales and marketing (35%), and finance and customer service (33% each) indicate a growing reliance on data-driven decision-making processes.

Key challenges in implementing robust analytics programs include obtaining business or leadership support (85%), ensuring the quality of data (82%), and identifying the right use cases (81%). Addressing these challenges is crucial for maximizing the benefits of data analytics initiatives.

IT Security: The state of IT security in 2024 reflects the evolving threat landscape and the measures enterprises are taking to safeguard their digital assets. Phishing attacks remain the most severe threat, with 50% of respondents experiencing high-severity incidents. Password/identity-based attacks (44%) and ransomware attacks (38%) are also prevalent concerns.

The impact of these security incidents on organizations is significant, with disruptions to business operations (24%), loss of critical data (23%), and financial losses (20%) being the most high-severity consequences. The frequency of IT security incidents further underscores the need for robust security measures, with human error and malware being the most repeatedly occurring common causes.

To address these threats, enterprises are focusing the most on providing training for employees (69%), re-training technical staff (64%), and partnering with experts/consultants (59%), among other measures.

Artificial Intelligence in Enterprise

Leadership Lens: Navigating Challenges and Priorities

In recent years, AI has become a significant buzzword in the enterprise tech landscape, with many organizations eager to harness its potential. However, it's essential to approach AI with a realistic perspective. While AI can offer substantial benefits when implemented correctly, it is not a silver bullet capable of solving all challenges effortlessly.

Success with AI requires a considerable investment of time and effort tailored to specific problems or business needs. Therefore, setting realistic expectations from the outset is crucial. This ensures alignment between teams and management, fostering a shared understanding of AI's capabilities and limitations.

Adoption and overall usage of AI should be key metrics, with other value parameters including the committed business ROI defined over time. If there is a regular demand for numerous AI programs, it indicates that the AI Program Office is functioning smoothly.

Organizations should prioritize the use of AI in areas where it can deliver the highest business benefits, such as IT operations, customer services, and regulatory compliance. As a CIO, it is crucial to balance various organizational perspectives to ensure the successful implementation of an AI project. This involves engaging multiple business units, maintaining regular communication through meetings and other modes of interaction, and setting clear objectives with a robust evaluation framework.

For successful AI project implementation, a holistic approach is essential. This includes forming a cross-departmental team, establishing a clear change management strategy with procedural adjustments, and implementing effective risk and compliance management. Additionally, a structured evaluation procedure should monitor progress and outcomes.

To assess the success of an AI project, key metrics should include its impact on business—such as cost reduction and revenue growth—the correctness of the AI output, its adoption in day-to-day activities, and feedback from various stakeholders post-implementation.

"While AI can offer substantial benefits when implemented correctly, it is not a silver bullet that can solve all challenges effortlessly."

Ashish Pandey
Global Chief
Information Officer,
Dabur India

"For successful AI implementation, a holistic approach is key: form a cross-departmental team, establish clear change management, and ensure effective risk and compliance management."

Sajeev Maheshwari
Executive Director - Information
Technology and Fare Collection
System, Delhi Metro Rail
Corporation

TURBOCHARGING BUSINESS GROWTH

With significantly increased investments in AI and ML, enterprises are geared to optimally leverage these technologies for innovation, operational efficiency, and competitive advantage.

Priority Actions for CIOs

1. Implement AI in IT operations and customer services: Prioritize deploying AI in cybersecurity, systems monitoring, and customer interactions to enhance efficiency and responsiveness.

2. Enhance customer experience: Leverage AI to boost customer satisfaction and drive business innovation, making it a top business priority.

3. Scale up AI deployments: Transition from pilot projects to substantial AI deployments that impact daily operations, driving both efficiency and innovation across the organization.

4. Leverage external expertise: Engage with external AI experts and invest in scalable, flexible AI solutions to compensate for limited internal expertise.

5. Demonstrate business value: Develop clear metrics and KPIs to measure and communicate the business value of AI initiatives to stakeholders.

6. Integrate AI with existing technologies: Focus on seamless integration of AI and ML systems with current technology stacks to maximize efficiency and functionality.

7. Ensure regulatory compliance: Stay ahead of regulations and ensure all AI systems comply with applicable laws to mitigate risks and maintain trust.

8. Prioritize AI-readiness in procurement: Make AI-readiness a key criterion in purchasing decisions, especially for solutions that directly enhance operational efficiency and security.

Executive Summary

Today, the landscape for Artificial Intelligence (AI) and Machine Learning (ML) in enterprises is marked by significant advancements and strategic shifts. CIOs are at the forefront of leveraging these technologies to drive business outcomes, enhance operational efficiencies, and foster innovation. According to the survey results, the primary business outcomes expected from AI and ML projects include discovering useful insights to improve decision-making (72% deeming it very important), innovating or improving products and services (74%), and enhancing customer experience and engagement (77%).

Adoption of AI and ML across organizational functions is also expanding. IT operations lead with 21% of organizations reporting wider deployment across multiple processes, followed by customer services and engagement at 19%, and sales and marketing at 18%. This trend underscores the growing integration of AI and ML into core business functions, emphasizing their critical role in modern enterprise strategies.

Spending on AI and ML is poised for growth, with 39% of enterprises planning to increase their spending somewhat, and 37% expecting a significant increase. This investment reflects the recognition of AI and ML as pivotal drivers of competitive advantage and operational excellence.

Enterprises are exploring various acquisition models for AI solutions. Building or developing through partners is the most likely approach (39%), followed closely by using AI-as-a-service (38%), and building or developing internally (35%). This indicates a balanced approach towards leveraging external expertise while fostering internal capabilities.

However, deploying AI and ML systems comes with its challenges. Demonstrating business value (46%), identifying the right use cases (44%), and integrating AI with existing technologies and systems (44%) are the top hurdles. These challenges highlight the need for robust strategies to ensure that AI initiatives align with business objectives and deliver tangible benefits.

Operational concerns also play a significant role, with ensuring AI compliance with regulations (57%), developing relevant AI models (54%), and governance of AI systems (54%) being the top issues. These concerns point to the necessity of maintaining stringent governance frameworks and adhering to regulatory standards to mitigate risks. Organizational culture elements are critical to AI's success. Executive leadership support for AI and ML is deemed very important by 75% of respondents, followed by change management during AI solution deployment (63%) and cross-organization collaboration (58%). These elements are essential for fostering an environment conducive to AI innovation and ensuring that AI initiatives receive the necessary support and resources.

In summary, the AI and ML landscape in 2024 is characterized by increasing investments, strategic deployment across various business functions, and a focus on overcoming operational and cultural challenges. CIOs must navigate these dynamics to harness the full potential of AI and ML, driving transformative outcomes for their organizations.

Business Expectations from AI/ML

Top 3 business objectives	Ranking in 2024	Ranking in 2023
Improve customer experience and engagement	1 ↑	2
Innovate or improve products and services	2 ↑	9
Discover useful insights, improve decision-making	3 ↓	1

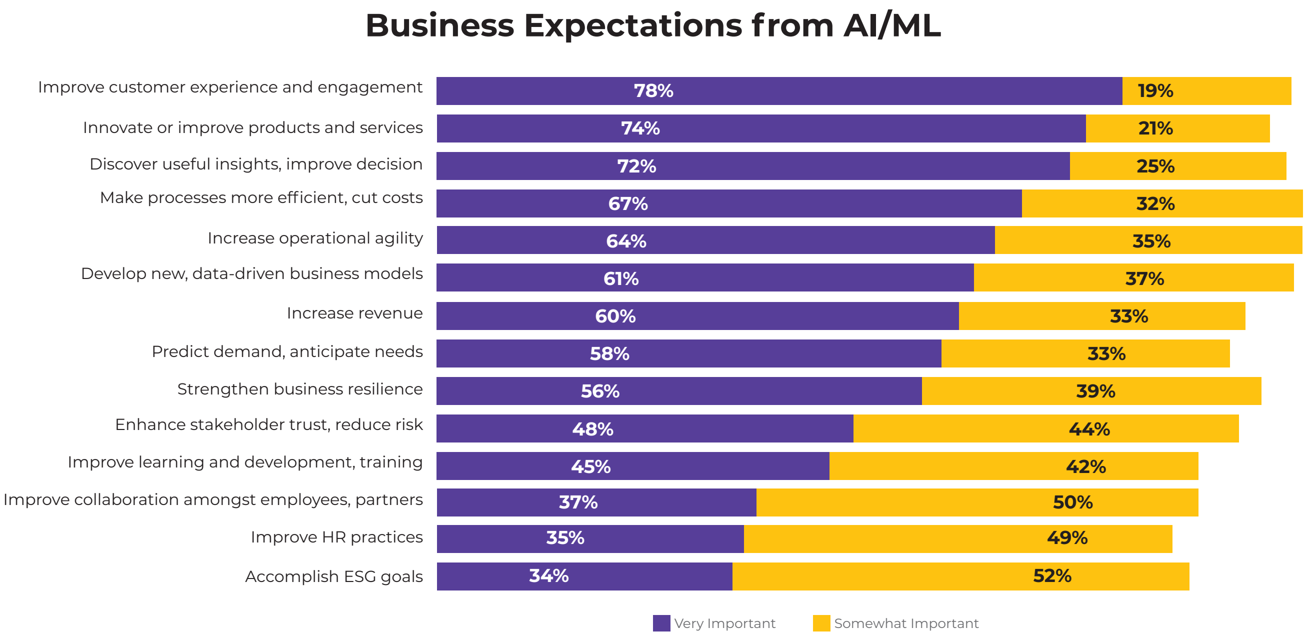

Business Expectations from AI/ML

Figure 1: Enterprises are prioritizing customer experience, products innovation, and insights gathering for better decision-making through AI and ML projects.

Top 3 Business Priorities: 78% of respondents consider improving customer experience and engagement as “Very Important,” making it the top priority for AI and ML projects in 2024. This highlights the crucial role of AI in understanding customer needs, personalizing interactions, and enhancing overall customer satisfaction.

74% of respondents rate innovating or improving products and services as “Very Important.” AI’s potential to drive innovation and enhance product offerings is seen as a critical business outcome.

72% of respondents highlight the importance of discovering useful insights and improving decision-making. AI’s ability to process large datasets and provide actionable insights is crucial for strategic planning and operational decisions (See Figure 1).

Trend and Analysis: Improving customer experience and engagement remained a high priority, with a slight increase from 75% in 2023 to 77% in 2024. This consistency underscores the ongoing focus on enhancing customer interactions through AI.The persistent emphasis on customer experience indicates that businesses recognize the long-term value of AI in building strong customer relationships and ensuring satisfaction. Companies are likely to invest more in technologies that enhance personalization and customer satisfaction.Continued investment in AI technologies that enhance customer experience is essential.

The importance of innovating or improving products and services increased from 54% in 2023 to 74% in 2024. This substantial rise indicates a growing recognition of AI’s role in driving product innovation.

This trend reflects a shift towards utilizing AI to stay competitive by continuously improving and innovating product offerings. Organizations are increasingly relying on AI to gain insights into market needs and innovate accordingly.

The importance of discovering useful insights and improving decision-making saw a decrease from 81% in 2023 to 72% in 2024. While still significant, this drop suggests a relative shift in priorities.The reduction may indicate that while decision-making remains crucial, businesses might have already established AI tools for insights and are now focusing more on application areas like product innovation and customer engagement.

Actionable Insights: Thereis an increased focus on product innovation, sustained emphasis on customer experience, and a slight shift in the prioritization of decision-making insights. These trends highlight the evolving landscape of AI adoption, where businesses are progressively leveraging AI to drive innovation and enhance customer-centric strategies. Organizations should align their AI initiatives with these trends to maximize the benefits and stay competitive in the market. This includes defining KPIs to measure the success of AI initiatives and ensuring alignment with overall business goals.

Organizations should invest in AI-driven customer service tools, such as chatbots and personalized recommendation systems, to enhance customer engagement and loyalty.

Enterprises should utilize AI for product development, market analysis, and innovation. This includes adopting AI for R&D processes, analyzing customer feedback, and exploring new product features driven by AI insights.

Organizations should deploy AI analytics tools to derive insights from their data. This involves integrating AI-driven data analysis platforms that can help identify trends, predict outcomes, and support data-driven decision-making processes.

Adoption of AI, ML by Organizational Functions

Top 3 functions/ departments	Ranking in 2024	Ranking in 2023
IT operations	1 ↔	1
Customer services and engagement	2 ↑	3
Sales and marketing	3 ↑	4

Top 3 Functions by Adoption: IT operations show the highest percentage of high adoption (21%) among the three functions, indicating a more advanced integration of AI. A significant number of organizations (46%) are utilizing AI for specific IT operations. There are still opportunities to expand AI usage in IT operations. (See Figure 2).

Many organizations (41%) are using AI to enhance specific aspects of customer engagement.Similar to sales and marketing, a smaller percentage of organizations have fully integrated AI into their customer services.There is still a notable portion of organizations in the early stages (30%) or not considering AI (9%).

A significant portion of organizations (44%) are using AI in specific cases, showing a moderate level of maturity. The relatively lower percentage of high adoption (18%) indicates that many organizations are still exploring AI's full potential in sales and marketing. There is still a substantial percentage of organizations either in the initial stages of adoption (19%) or not considering AI at all (18%).

Trend and Analysis: There is an overall increase in the wider deployment of AI in IT operations, from

State of Adoption of AI/ML by Functions

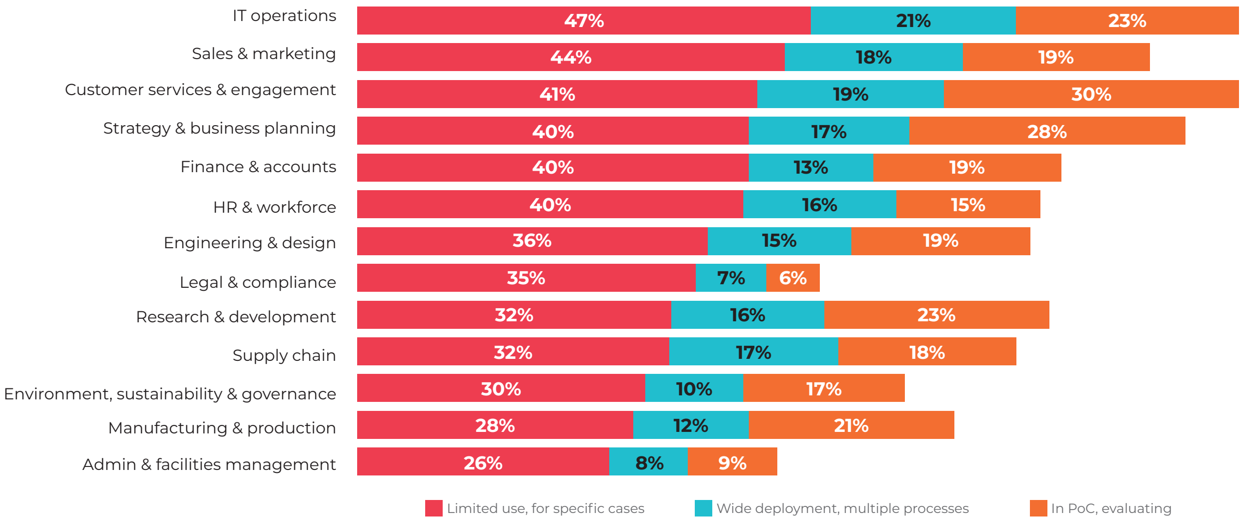


Figure 2: High adoption in IT operations, customer services, and sales and marketing, is indicative of focused integration of AI and ML.

18% in 2023 to 21% in 2024. This trend suggests that organizations are becoming more confident in scaling their AI initiatives beyond pilot phases. The focus is shifting towards integrating AI into everyday operations to drive efficiency and innovation.

The percentage of customer services and engagement in the PoC, evaluating phase increased from 28% in 2023 to 30% in 2024, indicating sustained interest. However, the wider deployment increased significantly from 13% to 19%.This trend indicates a successful transition from evaluation to implementation. Organizations are moving from PoC to practical applications, showing growing confidence in AI's potential to enhance customer engagement.

Limited use of AI remains a significant theme generally, but sales and marketing saw a decrease in limited use from 47% to 44% (while IT operations saw and increase from 41% to 46%). This is suggestive of the fact that while some functions are transitioning to wider deployment, others are still expanding their limited use cases. This indicates a maturing landscape where companies are refining their AI strategies and moving toward broader applications.

Actionable Insights: The comparison reveals a trend towards increased deployment and ongoing evaluations, especially in customer services. Organizations are gradually shifting from limited use cases to broader applications, highlighting the growing maturity of AI initiatives. To capitalize on these trends, companies should focus on scaling successful pilot projects and sharing best practices across functions to ensure comprehensive AI integration.

Organizations should focus on automating routine IT tasks, using AI for predictive maintenance, and enhancing cybersecurity measures through AI-driven threat detection.Other departments can learn from the IT function's approach to AI integration. Sharing best practices and creating cross-functional teams could help other areas, like sales and customer service, achieve similar levels of deployment.

Organizations should prioritize converting PoC projects into full-scale implementations. This can be achieved by focusing on clear metrics for success and ensuring that pilot projects address key pain points in customer engagement.To improve customer engagement, organizations should invest in AI-driven customer support systems, such as chatbots and AI-assisted service agents, which can handle routine inquiries and provide 24/7 support.

Organizations should focus on expanding successful AI pilot projects to broader applications in sales and marketing. This can include using AI for customer segmentation, personalized marketing campaigns, and sales forecasting.

AI and ML Adoption by Business Processes

Top 3 functions/ departments	Ranking in 2024	Ranking in 2023
Customer engagement	1 ↑	3
Cybersecurity operations	2 ↓	1
Systems monitoring and optimization	3 ↑	4

Top 3 Business Processes by AI Adoption: With 34% of organizations using AI moderately and 23% extensively, there is a significant potential for transitioning from moderate to extensive use. Companies that are currently using AI moderately should focus on scaling these initiatives to achieve more widespread AI integration in customer engagement (See Figure 3).

Cybersecurity operations show a robust adoption rate, with 23% extensive and 35% moderate use. With only 6% having no plans for AI adoption, there is minimal resistance to AI in cybersecurity. It will likely be only a matter of time that the remaining low-use and non-adopters as the ROI and effectiveness of AI in preventing breaches and reducing security incidents increase.

A large portion of organizations report moderate use of AI and MLin systems monitoring and optimization (38%), while a notable percentage are planning to adopt AI within 12 months (16%).

Trend and Analysis: The percentage of extensive use in customer engagement remained stable at 23%. This implies that organizations continue to recognize the value of AI in enhancing customer engagement, indicating consistent investment in AI technologies for customer-related processes.

There is an increase in moderate use in cybersecurity operations from 31% to 35%.This indicates a growing recognition of the benefits of AI, with more organizations progressing from initial exploration to active planning and implementation.

Moderate use in systems monitoring and optimization has increased from 29% to 38%, while low use has decreased from 23% to 18% and so has "no plans" from 17% to 8%. This implies that after having tasted initial successes with AI, the organizations are extending the deployments. In other words, many organizations are already leveraging AI but have room for further deployment, which will likely grow with improved integration into existing systems monitoring and optimization apparatus.

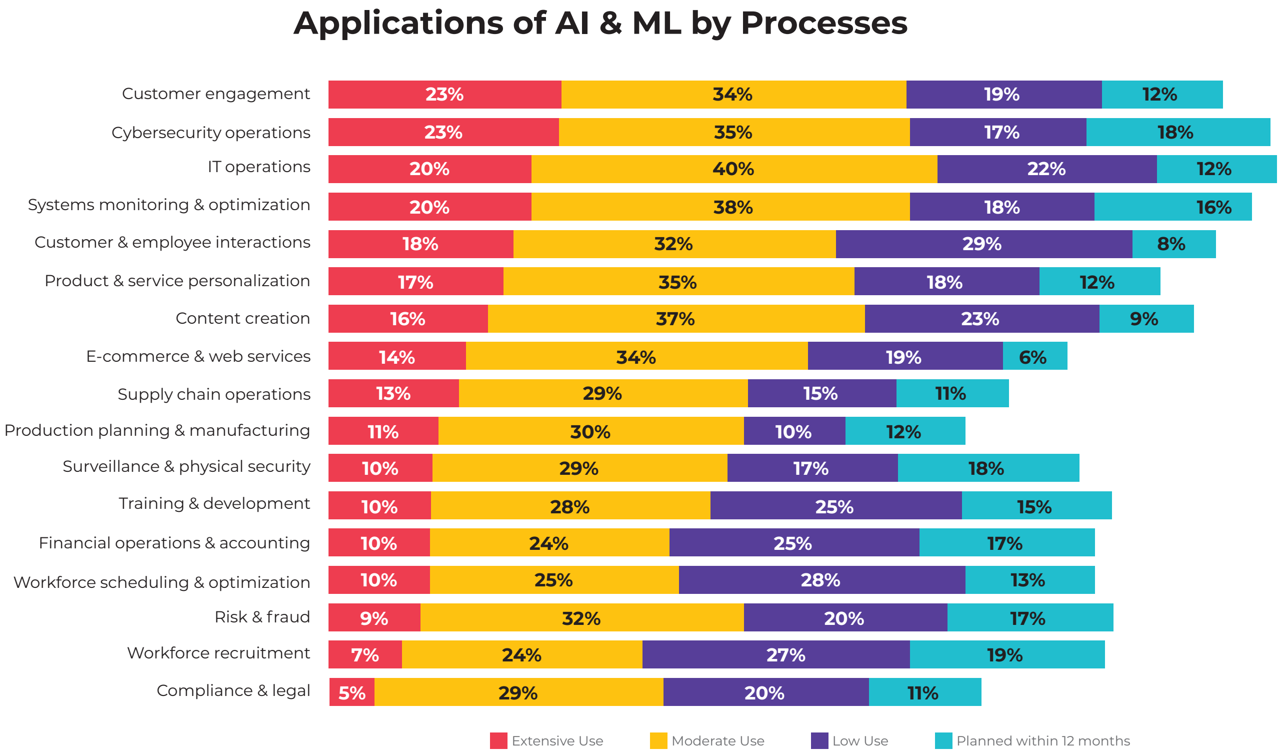


Figure 3: Application of AI/ML in business processes is diverse yet targeted, with customer engagement, cybersecurity operations, and systems monitoring leading in adoption.

Actionable Insights: The comparison reveals a trend towards increased moderate use of AI and ML, reflecting a maturing landscape where organizations are moving beyond initial trials to more comprehensive applications. The stable extensive use in customer engagement highlights the continued importance of AI in enhancing customer interactions. Organizations should focus on scaling successful AI projects and creating clear adoption roadmaps to ensure sustained growth and integration of AI technologies.

The 12% planning to adopt AI within the next 12 months signifies an ongoing trend towards embracing AI. These organizations should prioritize AI applications that directly impact customer satisfaction and retention, such as personalized marketing, automated customer service, and sentiment analysis. Case studies and success stories from similar companies can help highlight the value AI brings in enhancing customer experiences and competitive advantage.

Given the alarmingly sophisticated cyberthreat landscape today, increased AI adoption is crucial for enhancing threat detection, response time, and overall security posture of organizations. Organizations should focus on integrating AI-driven threat intelligence, anomaly detection, and automated response systems to mitigate risks effectively.

Organizations should also prioritize implementing predictive maintenance, performance optimization, and resource allocation tools powered by AI. They should also create clearer roadmaps for AI adoption, focusing on integrating it into existing processes.

Change in AI Spend

In 2024, 37% of enterprises foresee a significant increase in their AI and ML budgets, reflecting a marked rise from 25% in 2023. By comparison, 39% of enterprises plan to somewhat increase their spending versus 43% in the previous year. Further, 14% of respondents expect no change in their spending, a slight decrease from 17% in 2023, which is complemented by the fact that only 9% remain uncertain about their spending plans, which is a significant reduction from 15% last year (See Figure 4).

The 2024 data indicates a continued strong focus on increasing AI and ML investments, with a notable shift towards more significant budget increases. The combined 76% of enterprises in 2024 planning to increase spending (up from 68% in 2023) demonstrates a growing confidence and recognition of the transformative potential of AI and ML technologies.

The analysis of AI and ML spending trends for 2023 and 2024 reveals a clear and increasing commitment among enterprises to invest in these technologies. The shift towards more significant spending increases in 2024 highlights an evolving understanding of AI and ML's critical role in business innovation and growth. Enterprises are steadily moving from exploratory phases to more substantial and strategic investments, signaling a maturation in their AI and ML adoption journey. This trend underscores the importance of AI and ML in driving future business success and competitiveness.

Preferred AI Acquisition Models: Building or developing AI solutions through partners continues to be the most favored approach among enterprises in 2024. With a combined 85% of respondents indicating that this option is either "most likely" or

Change in Spending on AI & ML in Next 12 Months

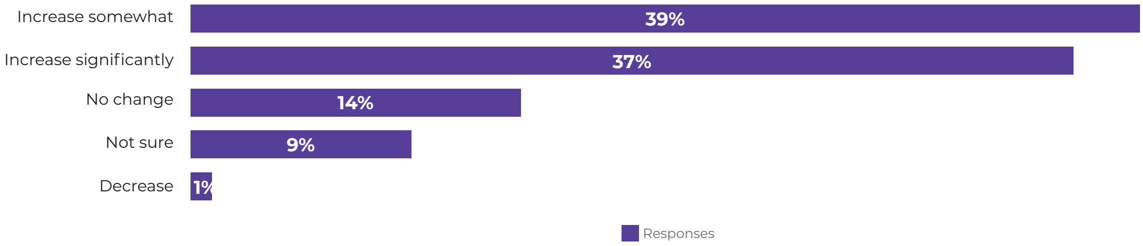


Figure 4: With 76% of the enterprises set to increase their AI/ML spending either significantly or moderately, a strong commitment to AI is firmly in place.

Acquisition of AI Solutions

Preferred acquisition models	Ranking in 2024	Ranking in 2023
Customer engagement Build or develop through partners	1 ↔	1
Use AI-as-a-service	2 ↔	2
Build or develop internally	3 ↓	2
Purchase as packaged solutions	3 ↑	4

“somewhat likely,” it underscores the importance of leveraging external expertise and resources to develop AI capabilities. This strategy can expedite the deployment of AI solutions and provide access to specialized skills and technologies that may not be readily available in-house (See Figure 5).

Using AI-as-a-Service (AIaaS) is a close second, with 78% of enterprises likely (combining most likely and somewhat likely) to consider this model. AIaaS offers a scalable, cost-effective way to access advanced AI capabilities without significant upfront investments in infrastructure and talent. This model is particularly attractive for businesses looking to integrate AI into their operations quickly and flexibly.

Developing AI solutions internally is a strategy that 77% of enterprises find likely to adopt. This approach allows for greater control over AI development and customization to meet specific business needs. However, it requires substantial investment in building internal capabilities, including recruiting skilled personnel and developing the necessary infrastructure.

Purchasing AI solutions as packaged offerings is considered likely by 66% of respondents. While this model may not offer the same level of customization as building internally or through partners, it provides a quicker deployment path and leverages proven solutions in the market. It is an appealing option for enterprises that prioritize speed and reliability over customization.

Trend and Analysis: The trend shows a slight increase in the preference for building or developing AI solutions through partners, with the “most likely” category increasing from 38% to 39%, and “somewhat likely” from 42% to 46%. The percentage of respondents who are “not sure” has significantly decreased from 12% to 4%. This indicates growing confidence and clarity among enterprises in leveraging partnerships to develop AI capabilities.

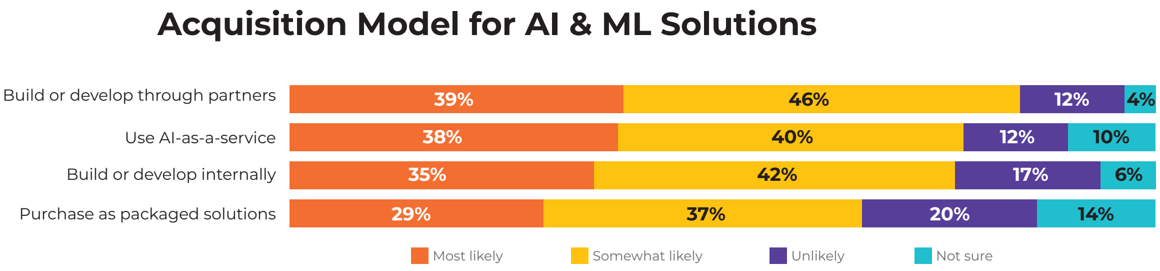


Figure 5: Enterprises are certainly not putting all the AI eggs in one basket and are instead opting for a blend of product, partner-led development, and in-house strategies.

There is a noticeable increase in the likelihood of using AI-as-a-Service. The “most likely” category has increased from 35% to 38%, and “somewhat likely” from 31% to 40%. Additionally, the “unlikely” and “not sure” categories have both decreased, indicating a growing acceptance and adoption of AI-as-a-Service models. The preference for building or developing AI solutions internally remains relatively stable, with a slight decrease in the “most likely” category from 36% to 35%. However, the “unlikely” category has increased from 11% to 17%, suggesting that while internal development remains important, some enterprises might be shifting towards external solutions due to challenges such as skill shortages and resource constraints.

There is an increase in the likelihood of purchasing AI solutions as packaged offerings, with the “most likely” category rising from 25% to 29%. The “unlikely” category has decreased from 27% to 20%, indicating a growing acceptance of ready-made AI solutions that can be quickly integrated into existing systems.

Actionable Insights: Whether choosing to develop internally, partner with external entities, or purchase packaged solutions, the key is to align these efforts with the organization’s strategic goals, customer needs, and market demands.

The trend analysis is indicative of a growing inclination for leveraging external expertise and scalable and flexible AI solutions. Enterprises should actively seek out and form strategic partnerships with AI specialists and technology providers. This approach can accelerate AI development, provide access to cutting-edge technologies, and fill gaps in internal capabilities.

Enterprises may also evaluate and adopt AIaaS offerings to benefit from scalable infrastructure, reduced upfront costs, and the ability to quickly implement AI capabilities.

Packaged AI solutions that can be seamlessly integrated into existing systemscan offer quick deployment, reduced complexity, and proven effectiveness. However, when selecting these solutions, it is important to ensure that the chosen solutions align with business objectives and can be customized to meet specific needs.

By adopting these actionable insights, enterprises can effectively navigate the evolving landscape of AI solution acquisition, leverage the best-suited models for their needs, and drive successful AI integration to achieve their business objectives in 2024 and beyond.

Challenges in Deploying AI & ML Applications

Top 3 challenges of CIOs	Ranking in 2024	Ranking in 2023
Demonstrating business value	1 ↑	4
Integrating AI with existing technologies and systems	2 ↑	9
Identifying right use cases	3 ↓	2

Top 3 Challenges in AI Deployment: Demonstrating the business value of AI and ML systems is the most significant challenge for enterprises in 2024. Nearly half of the respondents (46%) consider it highly important, emphasizing the need to clearly show the return on investment (ROI) and tangible benefits these technologies bring to the organization. This includes showcasing improvements in efficiency, cost savings, enhanced decision-making, and competitive advantage. Without clear evidence of business value, gaining executive buy-in and continued investment can be challenging (See Figure 6).

Identifying the right use cases for AI and ML deployment is another critical challenge. With 44% of respondents rating it as highly important, it’s

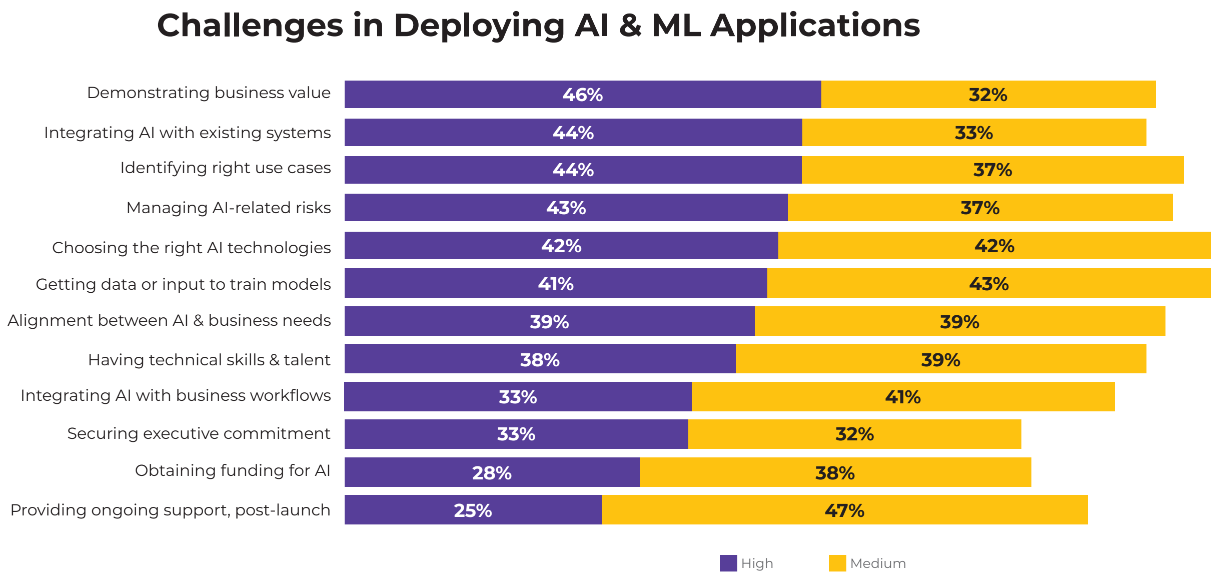


Figure 6: Demonstrating business value, identifying use cases, and integrating with existing IT systems are the key challenges to be overcome for rolling out an AI project.

clear that selecting the most impactful and feasible applications of AI is crucial for success. Organizations often struggle to pinpoint areas where AI can deliver the most value and align with business objectives.

Integrating AI and ML systems with existing technologies and infrastructure is a significant hurdle. With 44% of respondents highlighting it as a high priority, seamless integration is vital to leverage the full potential of AI. Challenges include compatibility issues, data integration, and ensuring that AI solutions work harmoniously with current systems and processes.

Trend and Analysis: There was an increase in the percentage of respondents who viewed demonstrating business value as highly important (from 40% in 2023 to 46% in 2024). The medium importance category saw a decrease from 42% to 32%, suggesting that more organizations are recognizing the critical need to prove business value upfront. The upward trend in the importance of demonstrating business value suggests that CIOs and business leaders are increasingly demanding tangible results from their AI investments.

The challenge of identifying the right use cases has remained consistent in its high importance (44% for both the years). However, there is a slight increase in the medium importance category (from 31% in 2023 to 37% in 2024) and a decrease in the not relevant category, showing that more organizations are actively seeking suitable AI use cases.

There is a notable increase in the importance of integrating AI with existing technologies and systems, with high importance rising from 32% in 2023 to 44% in 2024. The medium importance category decreased, indicating that more organizations are prioritizing integration as a critical challenge.

Actionable Insights: Addressing these challenges requires a strategic approach, involving clear business cases, prioritized use cases, and robust integration plans. By tackling these issues, enterprises can unlock the full potential of AI and ML, driving significant business transformation and innovation.

First of all, organizations will need to focus on creating robust business cases and clear value propositions for their AI projects. The consistency in the importance of identifying the right use cases also highlights the ongoing struggle to pinpoint high-impact and feasible AI applications. This underscores the need for organizations to continuously refine their approach to identifying and evaluating potential AI use cases.

The increase in the perceived importance of integration challenges suggests that as AI adoption grows, organizations face more complexities in ensuring their AI solutions work seamlessly with existing IT infrastructure. This highlights the need for comprehensive integration strategies and robust IT support to facilitate smooth implementation.

Operational Concerns in Deploying AI Systems

Top 3 operational concerns in deploying	Ranking in 2024	Ranking in 2023
Ensuring AI is compliant with applicable regulations	1 ↑	3
Developing relevant AI models/ algorithms	2 ↑	5
Governance of AI systems and processes	3 ↑	7

Top 3 Operational Concerns: Ensuring AI compliance with applicable regulations is the top concern for 2024, with 57% of respondents rating it as highly important. This highlights the growing emphasis on regulatory adherence as AI systems become more integrated into business operations (See Figure 7).

Developing relevant AI models and algorithms is the second most significant concern, with 54% considering it highly important. The development of effective AI models is crucial for achieving desired outcomes and maintaining a competitive edge. This concern reflects the challenges associated with creating models that are accurate, reliable, and aligned with business objectives. Governance of AI systems and processes is another critical concern, with 54% of respondents highlighting its high importance. Effective governance ensures that AI systems are used responsibly, ethically, and in a manner that aligns with organizational policies and objectives. It also involves overseeing the deployment, monitoring, and maintenance of AI systems to ensure they perform as intended.

Trend and Analysis: There is a noticeable increase in the importance placed on ensuring AI compliance with regulations, with the percentage of respondents rating it as a high concern rising from 48% in 2023 to 57% in 2024. This indicates a growing recognition of the complexities and importance of regulatory compliance as AI systems become more prevalent and integrated into core business processes.

The concern regarding the development of relevant AI models and algorithms has grown, with those rating it as highly important increasing from 46% in 2023 to 54% in 2024. This trend underscores the critical role that advanced and accurate AI models play in achieving business goals and staying competitive.

Governance of AI systems has become a more significant concern, with 54% rating it as high in 2024 compared to 44% in 2023. This increase reflects the need for robust frameworks to manage the

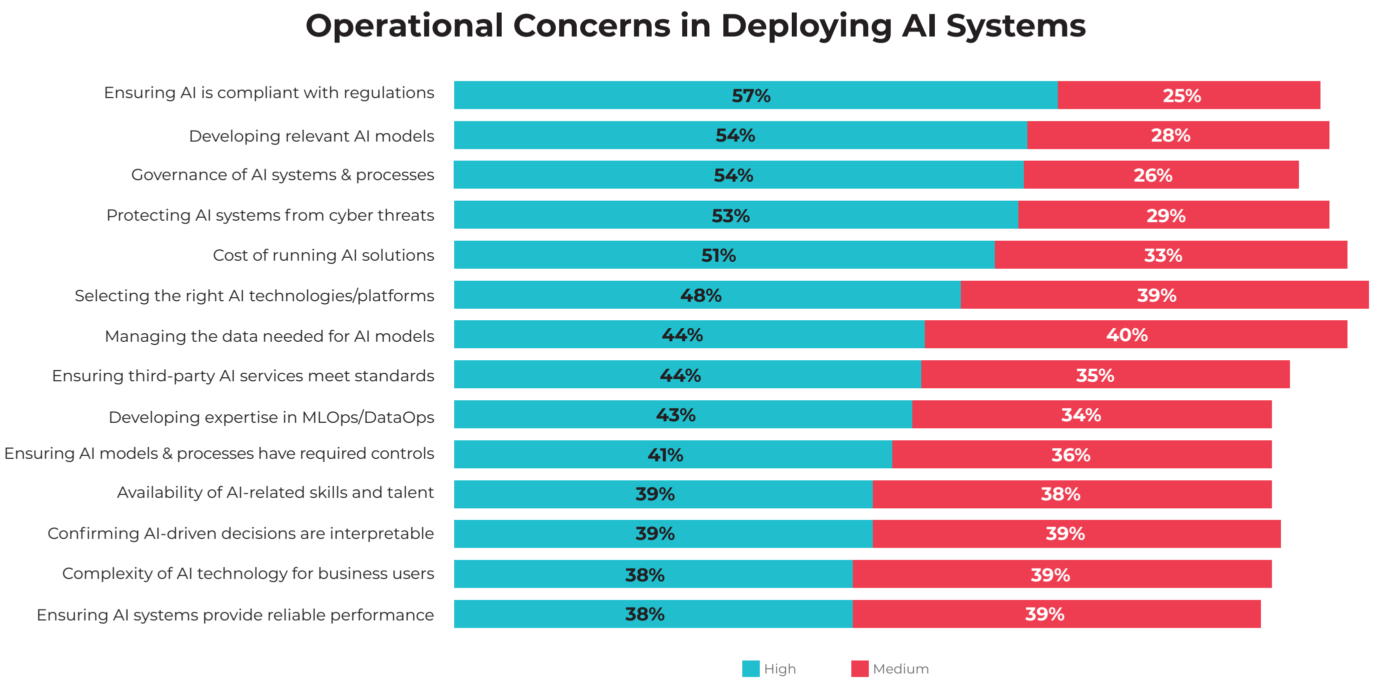


Figure 7: The concerns around regulatory compliance, developing AI models, and governance emphasize the need for robust frameworks and standards.

ethical, legal, and operational aspects of AI deployment.

Actionable Insights: Enterprises should establish dedicated compliance teams and frameworks to ensure that their AI initiatives meet all regulatory requirements. Continuous monitoring and updating of compliance measures are essential as regulations evolve.

It is also important for organizations to invest in research and development to innovate and refine AI models continuously. Collaboration with academic institutions and leveraging open-source platforms can also provide access to cutting-edge algorithms and methodologies.

Implementing robust AI governance frameworks is essential. This includes setting up AI ethics committees, defining clear guidelines for AI use, and establishing transparent processes for monitoring and evaluating AI systems. Regular audits and assessments can help identify and mitigate potential risks.

Top 3 Culture Elements Needed for AI: Executive leadership support is identified as the most critical factor for the success of AI initiatives, with 75% of respondents rating it as very important. This overwhelming majority indicates that top-down endorsement and commitment are vital for driving AI projects forward. Executive leadership ensures that AI initiatives receive the necessary resources,

Role of Cultural Elements in AI's Success

Top 3organizational culture elements	Ranking in 2024	Ranking in 2023
Executive leadership support for AI, ML	1 ↑	3
Change management during AI solution deployment	2 ↑	4
Cross-organization collaboration	3 ↑	6

attention, and strategic alignment with broader business objectives. Leaders play a crucial role in setting the vision, fostering an AI-friendly culture, and mitigating resistance to change within the organization (See Figure 8).

Effective change management is the second most important element, with 63% of respondents considering it very important. AI deployments often lead to significant changes in workflows, roles, and processes, which can face resistance from employees. Proper change management practices help in easing this transition, addressing employee concerns, and ensuring that the workforce is prepared for new ways of working.

Cross-organization collaboration ranks third, with 58% of respondents viewing it as very important. AI projects often require input and cooperation of multiple stakeholders; and by addressing these key cultural elements, organizations can enhance their ability to implement AI solutions effectively, overcome resistance, and achieve their strategic AI objectives.

Trend and Analysis: There is a slight decline in the perceived importance of executive leadership support for AI & ML from 2023 to 2024, with a 4% decrease in those rating it as "very important"(from 79% in 2023 to 75% in 2024) and a corresponding increase in those considering it "somewhat

Organizational Culture for Success of AI & ML

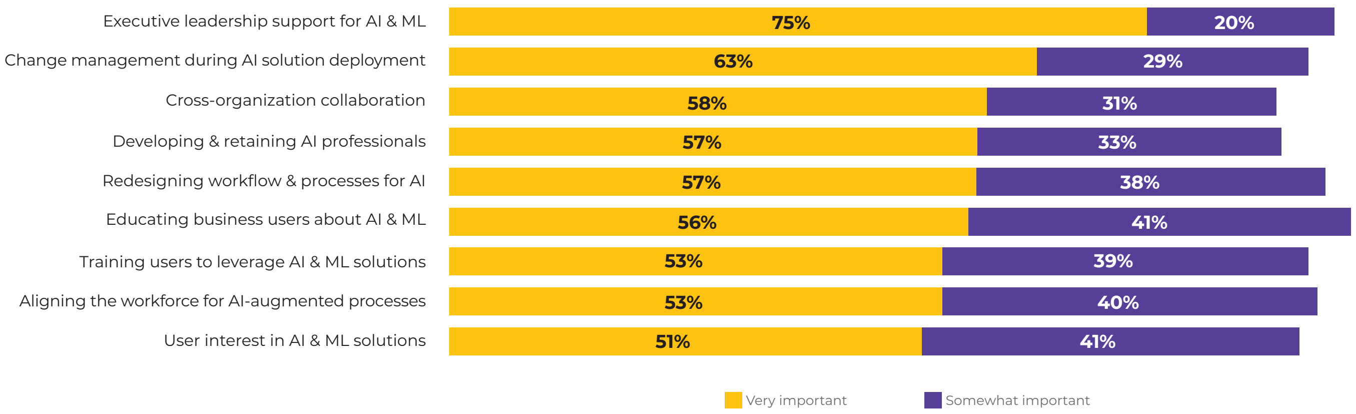


Figure 8: A supportive and integrated organizational culture, especially leadership support, effective change management, and cross-organization collaboration, is the foundation for AI's success.

> "While AI accelerates processes, human oversight is crucial for maintaining quality and accuracy. The goal of AI and ML is to strengthen productivity, allowing humans to concentrate on strategic and complex tasks."

Chitti Babu
Group CIO, Aurobindo Pharma

important" or "not important". However, it remains the top cultural element critical for AI success, indicating ongoing recognition of leadership's role in driving AI initiatives. However, the shifts may also indicate that executive leadership has grown more supportive of AI implementations and therefore getting their go-ahead is now considered easier than a year ago.

There is a slight decline in the perceived importance of executive leadership support for AI & ML from 2023 to 2024, with a 4% decrease in those rating it as "very important" and a corresponding increase in those considering it "somewhat important" or "not important". However, it remains the top cultural element critical for AI success, indicating ongoing recognition of leadership's role in driving AI initiatives. Cross-organization collaboration remains crucial, with a slight increase of 1% in those considering it "very important". However, the rise in the "not important" and "not relevant" categories in 2024 indicates a divergence in opinions about its necessity.

Actionable Insights: Enterprises should ensure that their leadership teams are not only supportive but also actively involved in AI initiatives. This involvement can include setting clear AI goals, regularly reviewing progress, and communicating the strategic importance of AI to the entire organization.

To help employees adapt to AI-driven changes,organizations should invest in robust change management strategies, including clear communication plans, training programs, and support mechanisms. Engaging employees early in the process and involving them in the implementation phase can also reduce resistance and increase buy-in.

To enhancing cross-organization collaboration, leaders should proactively form interdisciplinary teams that include members from different departments such as IT, data science, operations, and business units. These teams can work together to design, develop, and deploy AI solutions. Collaboration tools and platforms may be utilized to facilitate seamless communication and collaboration across departments. Regular meetings, workshops, and collaborative projects can help break down silos and promote knowledge sharing.

AI-ready IT

AI-readiness has become a critical criterion for purchasing decisions across various IT domains.

Data and analytics solutions top the list, with 72% of organizations deeming AI-readiness as very likely to influence their decisions, followed by cloud platforms and solutions at 62%. This reflects the high importance placed on advanced data processing and cloud management capabilities (See Figure 9).

IT security and governance solutions also rank highly (61%), emphasizing the need for robust, AI-driven security frameworks. Enterprise software (ERP, CRM, HRM) and software development tools also show strong AI-readiness demand, at 60% and 56% respectively. Networking devices and IT hardware are somewhat lower on the scale, at 40% and 32%, indicating these areas are still evolving in terms of AI integration. Office productivity software, though vital, has a moderate influence (50%) on AI-readiness for purchase decisions. This data highlights the pivotal role of AI-readiness in driving purchasing decisions, particularly for solutions that directly enhance operational efficiency and security.

AI-readiness Required for IT Solutions

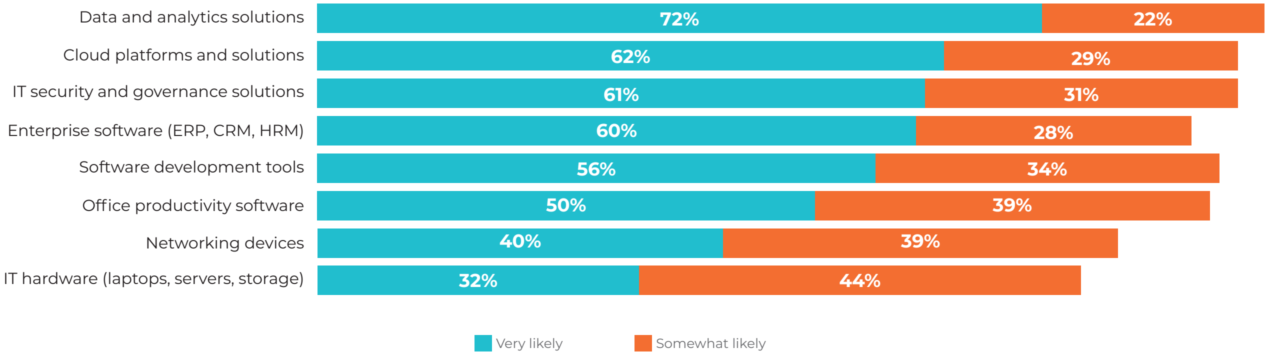


Figure 9: AI-readiness is crucial for purchasing decisions, especially for data solutions and cloud platforms. High importance is placed on AI-driven security and enterprise software.

Cloud and Infrastructure

Leadership Lens: Navigating Challenges and Priorities

Cloud management tools offer a centralized platform for overseeing resources across multiple cloud environments. They feature dashboards and reporting tools that provide real-time insights into resource utilization, performance, and costs, enabling businesses in making informed, data-driven decisions.

To enhance cloud management efficiency and reduce complexity, several areas need improvement:

A. Enhanced interoperability: Tools should better integrate with a wider range of cloud services and APIs to improve functionality and user experience.

B. Advanced analytics and AI integration: Incorporating advanced analytics and AI can offer predictive insights and automate decision-making, optimizing resource use, performance, and security.

C. User-friendly interfaces: Tools need more intuitive interfaces with simplified navigation and customizable dashboards to enhance usability and ease of learning.

D. Comprehensive security features: Tools must advance to include sophisticated threat detection, automated incident response, and continuous compliance monitoring to counter emerging threats.

E. Scalability and flexibility: As cloud environments grow more complex, tools must scale efficiently and adapt to new services and business needs.

"Cloud management tools should integrate widely, leverage AI for insights, offer intuitive interfaces, advance security features, and scale flexibly to manage complex, multi-cloud environments effectively."

Dr Sandip Pradhan
Chief Information Officer,
Exide Industries

Reducing complexity and optimizing cloud usage in multi-cloud environments is challenging but rewarding, when done correctly. To succeed, effective strategies are essential:

1. Choose the right partner: Select a partner with the necessary skills and expertise to support your cloud management needs. This ensures you have the right guidance and support.

2. Centralized unified monitoring: Implement centralized monitoring and orchestration across your multi-cloud environments. This provides a unified view for easier management and optimization.

3. Utilize performance insights: Use tools to gain insights into your cloud infrastructure and application performance to make informed decisions and optimize resource allocation.

4. Optimize resource sizing: Properly size your cloud resources to avoid over-provisioning or under-provisioning, which helps in optimizing costs and improving efficiency.

5. Strong governance: Establish robust governance frameworks to ensure compliance with industry standards and regulations, maintaining control over your cloud operations.

6. Implement robust security policies: Ensure comprehensive security policies and compliance measures are in place to protect your data and infrastructure from potential threats.

"To optimize multi-cloud environments, choose the right partner, use unified monitoring, leverage performance insights, optimize resource sizing, ensure strong governance, and enforce robust security policies."

Apurva Dalal
Chief Information Officer & acting
CISO, Adani Green Energy

AGILITY DRIVERS

To harness cloud solutions optimally for fostering digital transformation, the key is to address security challenges and optimize costs for enhanced business agility.

Priority Actions for CIOs

1. Leverage cloud for disaster recovery and operational flexibility: Prioritize adopting cloud solutions like DRaaS (Disaster Recovery as a Service) to enhance operational flexibility and ensure robust disaster recovery capabilities.

2. Enhance security measures: Address security concerns by implementing comprehensive security strategies and leveraging cloud-based security services (SECaaS) to manage the increasing complexity of enterprise IT environments.

3. Adopt advanced cloud services: Plan to adopt emerging cloud services such as SECaaS, DRaaS, and AaaS (Anything as a Service) within the next 12 months to stay ahead in cloud adoption and improve overall infrastructure resilience.

4. Utilize APIs for IT ecosystem flexibility: Increase the use of APIs to build more flexible and scalable IT ecosystems, ensuring seamless integration and interoperability across various cloud services and applications.

5. Optimize infrastructure and manage Costs: Focus on infrastructure optimization to maximize efficiency and implement cost management strategies to control and reduce operational expenses.

6. Promote SaaS adoption: Continue to lead in SaaS adoption while balancing it with other cloud services to ensure a comprehensive and efficient cloud strategy.

7. Implement robust cost management practices: Establish clear cost management practices and tools to monitor and control cloud expenditures, ensuring cost-effectiveness while leveraging cloud benefits.

8. Ensure compliance and security in cloud adoption: Ensure all cloud services and infrastructure comply with relevant regulations and security standards to mitigate risks and protect organizational data.

Executive Summary

This year, CIOs continue to navigate an evolving landscape where cloud services and IT infrastructure play pivotal roles in driving digital transformation, enhancing business agility, and ensuring operational resilience. The trends and insights culled from the survey provide a comprehensive overview of how organizations are leveraging cloud technologies and addressing associated challenges to stay competitive.

The deployment of cloud services has reached significant maturity, with Software as a Service (SaaS) and Infrastructure as a Service (IaaS) leading the way. SaaS is in production at 69% of organizations, reflecting its crucial role in enabling scalable and accessible software solutions. Similarly, IaaS, with a 68% adoption rate, underscores its importance in providing flexible and robust infrastructure capabilities. These figures highlight the centrality of cloud services in modern IT strategies, where the need for agility, scalability, and cost-effectiveness drives cloud adoption.

CIOs are also prioritizing cloud delivery models that enhance specific business functions. For example, office productivity solutions are predominantly deployed in public cloud environments (56%), facilitating enhanced collaboration and efficiency. Cybersecurity solutions see a balanced deployment across on-premises, private, and public clouds, indicating a strategic approach to safeguarding digital assets across various platforms.

Cloud usage trends in 2024 reveal a strong focus on integrating advanced technologies and practices. SaaS (55%) and APIs (48%) are the most utilized technologies, highlighting the importance of seamless software integration and communication in cloud environments. Furthermore, the emphasis on centralized cloud management (39%) and DevOps/DevSecOps practices (36%) reflects a shift towards more cohesive and secure cloud operations.

The top drivers for using cloud services underscore the strategic priorities of CIOs. Digital transformation and business innovation (83%) remain the primary motivations, followed by infrastructure modernization (61%) and improving speed and agility of infrastructure provisioning (59%). These drivers illustrate the ongoing commitment to leveraging cloud capabilities to foster innovation and operational efficiency.

However, achieving IT security objectives presents significant challenges. The cost and effort to manage security solutions (44%), the evolving threat environment (43%), and the alignment of security with business goals (41%) are top concerns for CIOs. Addressing these challenges requires a robust and adaptive security strategy that integrates seamlessly with business objectives.

Cloud Services Deployed and Planned

Top 3 cloud service categories	Ranking in 2024	Ranking in 2023
Software as a service (SaaS)	1 ↑	2
Infrastructure as a service (IaaS)	2 ↑	9
Application platform as a service (aPaaS)	3 ↓	1

Top 3 Services Deployed: SaaS has the highest current adoption, with 69% of organizations already using it in production (See Figure 1). This reflects the maturity and widespread acceptance of SaaS solutions for various business applications. Also, with 11% planning to adopt SaaS within the next 12 months, the overall adoption is expected to increase further. Only 7% of organizations have no plans for SaaS, indicating a broad recognition of its benefits.

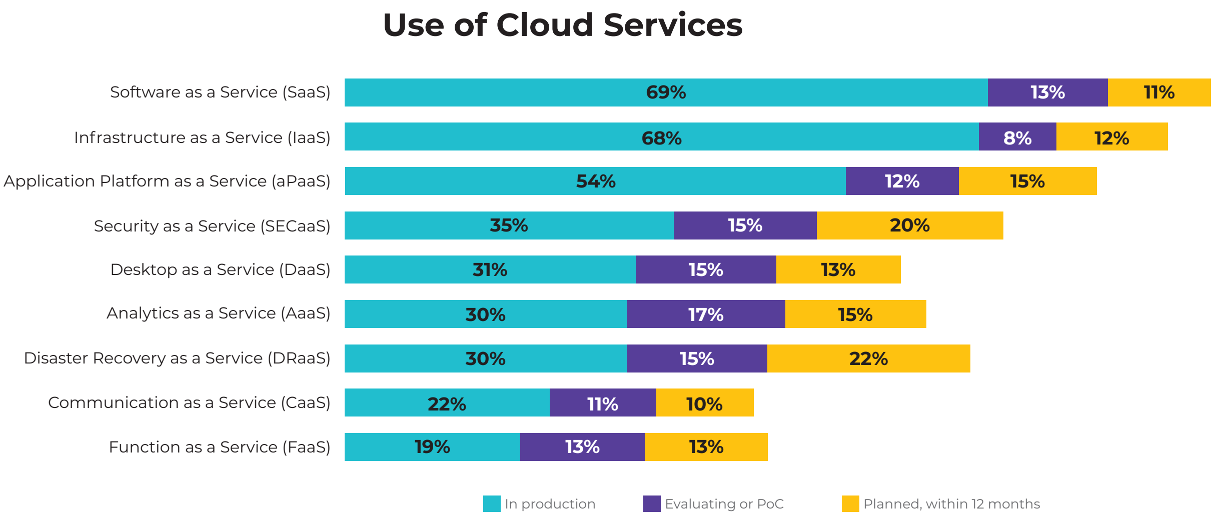


Figure 1: While SaaS and IaaS continue to lead cloud adoption, deployments are significant in other cloud services as well.

Trends and Analysis: For SaaS, the in-production usage decreased from 78% in 2023 to 69% in 2024, indicating a potential shift or re-evaluation in deployments. Also, planned usage for next12 months increased from 3% to 11%, showing renewed interest in future SaaS deployments. For IaaS, in-production usage remained stable at around 68% while planned usage increased from 7% in 2023 to 12% in 2024. For aPaaS too, in-production usage remained stable at around 54-55%, while planned usage for 12 months increased from 8% in 2023 to 15% in 2024.

SaaS continues to be a dominant cloud service, but organizations seem to be re-evaluating their SaaS strategies and planning new implementations. IaaS remains a critical infrastructure service, with stable production use and increased future planning, reflecting its importance in organizational strategies. aPaaS continues to be a key service for application development, with increased planning indicating growing interest in future deployments.

Actionable Insight: Organizations should leverage the widespread acceptance of SaaS to streamline operations and reduce IT overhead. Investing in SaaS applications can provide scalability, cost-efficiency, and ease of management.

The data indicates varying levels of adoption and future plans for different cloud services. SaaS and IaaS have the highest current adoption rates, reflecting their maturity and widespread acceptance. Services like SECaaS, DRaaS, and AaaS show significant growth potential, with many organizations planning to adopt them within the next 12 months. On the other hand, services like CaaS and FaaS face higher resistance, indicating a need for more targeted education and demonstration of their benefits to drive adoption. Organizations should focus on scaling successful cloud initiatives and addressing barriers to adoption to fully leverage the benefits of cloud services.

Prevalent Cloud Models in Use by Application Categories

High Usage Varies by Applications: Backup, DR, and BCP solutions lead with 48% on-prem usage as well as private cloud usage (40%), reflecting the critical need for control and reliability in data protection and recovery processes (See Figure 2). Application Development and Testing follows closely with 46% on-prem usage, which highlights the necessity for secure and stable environments for developing and testing applications. Cyber Security Solutions have a significant on-prem presence at 45%, indicating the need for stringent control over security measures to safeguard against cyber threats and data protection from other external vulnerabilities.

For private cloud usage, AI, analytics, and data solutions have 37% private cloud usage, as a reflection of ensuring data privacy and compliance with data protection laws.Enterprise solutions (ERP, SCM, HR, etc.) at 35% private cloud usage highlights the trend towards leveraging private clouds for mission-critical applications.

Office productivity solutions lead with 56% public cloud usage, underscoring the widespread adoption of cloud-based tools like Google Workspace and Microsoft 365. Collaboration and communication solutions also see 56% public cloud usage, indicating the critical role of cloud platforms such as Slack, Zoom, and Microsoft Teams in modern workplaces. CRM and marketing solutions follow closely with 52% public cloud usage, given that platforms like Salesforce and HubSpot are favored for their ability to integrate seamlessly with other business systems, provide real-time analytics, and support scalable customer relationship management.

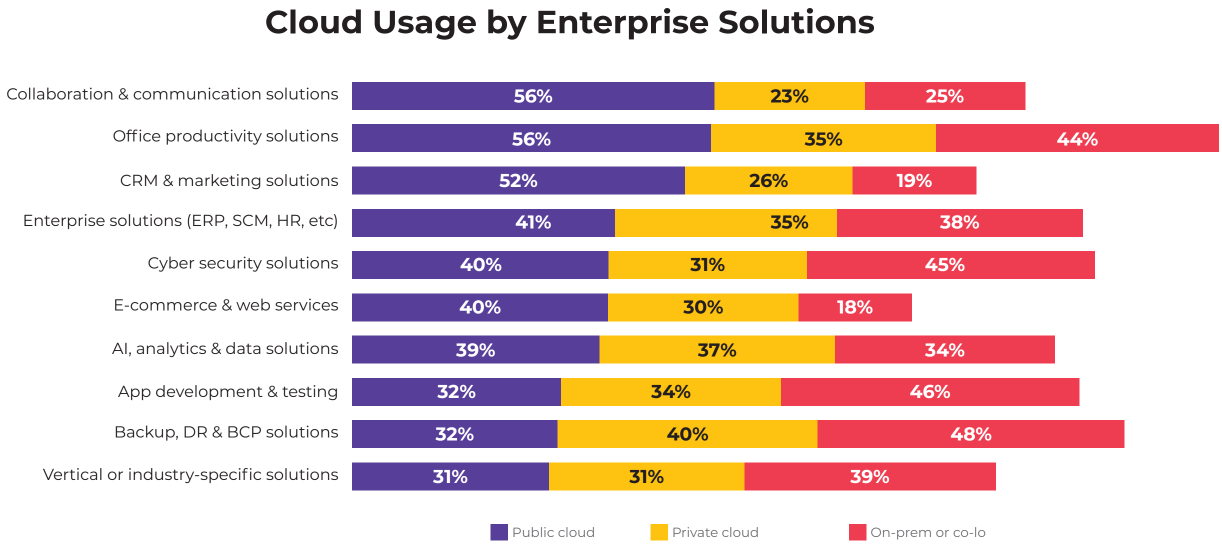


Figure 2: Public cloud dominates for collaboration, communication, and CRM solutions, while private cloud and on-prem solutions are preferred for enterprise and vertical-specific applications.

> "Cloud management tools enhance performance and agility by optimizing costs, automating workloads, and improving security. Future improvements should focus on cost management, asset visibility, and integrated security processes."

Vinod Bhat
Chief Information Officer
& Chief Ethics Counsellor,
Tata SIA Airlines

Trend and Analysis: On-prem usage decreased from 71% in 2023 to 48% in 2024 for backup, DR, and BCP; from 66% to 46% for app development and testing; and from 61% to 45% for cyber security. This significant decrease in on-prem usage across multiple application categories indicates a clear shift towards cloud-based solutions, reflectinga growing confidence in cloud services and their ability to offer superior scalability, flexibility, and cost-efficiency.

For private-cloud, usage by backup, DR, and BCP increased from 36% in 2023 to 40% in 2024; and by AI, analytics, and data it increased from 34% to 37%. However, usage by enterprise solutions (ERP, HR, etc.) decreased from 38% to 35%. These mixed trends show that for critical and sensitive applications, private cloud adoption has increased, reflecting the need for secure, controlled environments. However, the less critical categories have seen slight decreases, partly due to a shift toward public clouds or optimized hybrid models.

For public cloud, usage by office productivity application increased from 42% in 2023 to 56% in 2024; usage by collaboration and communication applications increased from 55% to 56%; and by CRM and marketing application, it increased from 46% to 52%. However, there was a decrease in usage by applications such as AI, analytics, and e-commerce.

This trend of generally increasing usage highlights the growing trust and reliance on public cloud services for their scalability, accessibility, and integration capabilities. The slight decreases in certain categories may indicate a strategic balancing of workloads between private and public clouds for optimizing costs and performance.

The comparative analysis shows a clear trend towards increased adoption of cloud solutions, particularly public cloud, across most application categories. Organizations are moving away from on-prem solutions in favor of the flexibility, scalability, and cost-efficiency offered by cloud services. While private cloud usage has seen mixed trends, it remains essential for applications requiring enhanced security and control. The overall shift reflects the evolving

Cloud Usage by Cloud Practices and Technology Initiatives

Top 3 cloud service categories	Ranking in 2024	Ranking in 2023
SaaS	1 ↔	1
APIs	2 ↑	3
IaaS	3 ↓	2

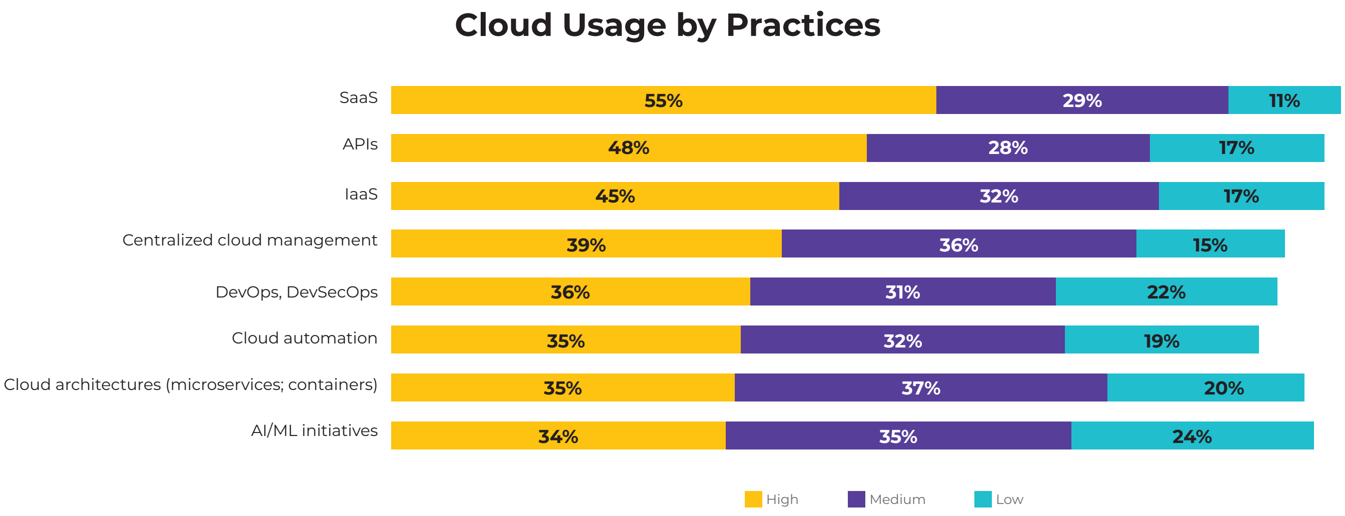


Figure 3: SaaS and APIs are the most utilized practices, while centralized cloud management and DevOps practices are also gaining significant traction.

landscape of IT infrastructure, where hybrid cloud strategies are becoming the norm to leverage the best of both worlds.

Actionable Takeaways: All the three delivery models, i.e., on-prem, private cloud, and public cloud offer differentiated value for different application types. Therefore, there is a need to optimize their usage accordingly. For example, it would be pertinent to upgrade on-prem infrastructure to support hybrid deployments, including adopting technologies like hyperconverged infrastructure (HCI) and software-defined data centers (SDDC). Modernizing on-prem infrastructure would ensure compatibility with cloud services and enhance overall operational efficiency.

Likewise, it would be worth investing in technologies that facilitate seamless integration between private and public clouds, such as hybrid cloud management tools and APIs.Enhanced integration capabilities would allow for better workload distribution and data mobility across cloud environments, thereby optimizing the overall cloud strategy.

When it comes to public cloud, it would pay to invest in cloud-native technologies such as microservices, containerization, and serverless computing to optimize public cloud usage.Cloud-native technologies could enhance the efficiency and agility of applications, allowing organizations to fully leverage the benefits of public cloud platforms.

Top 3 Practices: With 55% of organizations reporting high usage, SaaS is the leading cloud practice, followed by APIs (48%) that are crucial for integrating various cloud services and on-prem systems, enabling seamless data flow, and ensuring interoperability between different applications.IaaS, which provides the essential infrastructure needed for deploying and managing applications in the cloud, has the third-most high usage of 45% (See Figure 3).

Trend and Analysis: SaaS was the leading high-usage cloud category in 2023 (51%) and has remained so in 2024 (55%). APIs have clocked a significant increase in high usage (from 36% in 2023 to 48% in 2024) to become the second-highest category by usage. IaaS comes third with 45% usage in 2024, with a slight decrease from 48% in 2023.

The sustained popularity of SaaS solutions is driven by their scalability, ease of deployment, and cost-efficiency. Organizations can quickly adopt and scale SaaS applications without significant upfront investments in infrastructure.

The jump in high usage of APIs reflects that they are essential for building flexible and scalable IT ecosystems. APIs facilitate the creation of innovative services and applications by allowing developers to access and utilize external functionalities and data.

IaaS has mostly held its ground as it offers scalability and control over computing resources, allowing organizations to scale up or down based on demand. This flexibility is vital for supporting dynamic workloads and optimizing costs.

IT Infrastructure Needs and Concerns by Importance

Top 3 IT infrastructure	Ranking in 2024	Ranking in 2023
Infrastructure security	1 ↔	1
Infrastructure optimization	2 ↑	4
Infrastructure cost management	3 ↑	5

> "Managing multi-cloud environments, though complex, offers flexibility and cost efficiency. Implement cloud management platforms, establish clear governance, right-size deployments, optimize costs, and ensure security and compliance through assessments and analytics."

Harnath Babu
Partner & CIO,
KPMG India

Actionable Insight: Organization should continue to leverage SaaS for its flexibility and ability to support remote and hybrid work environments. Investing in robust SaaS applications can enhance productivity and streamline operations.

It is vital to prioritize API development and management to enhance integration capabilities and foster innovation. Implementing API management platforms can help monitor and secure API usage effectively.

To maximize the benefits of IaaS, organizations should focus on implementing robust infrastructure management practices. This includes leveraging automation tools for provisioning and managing resources, ensuring security and compliance, and optimizing resource utilization to reduce costs.

Concerns about IT Infrastructure

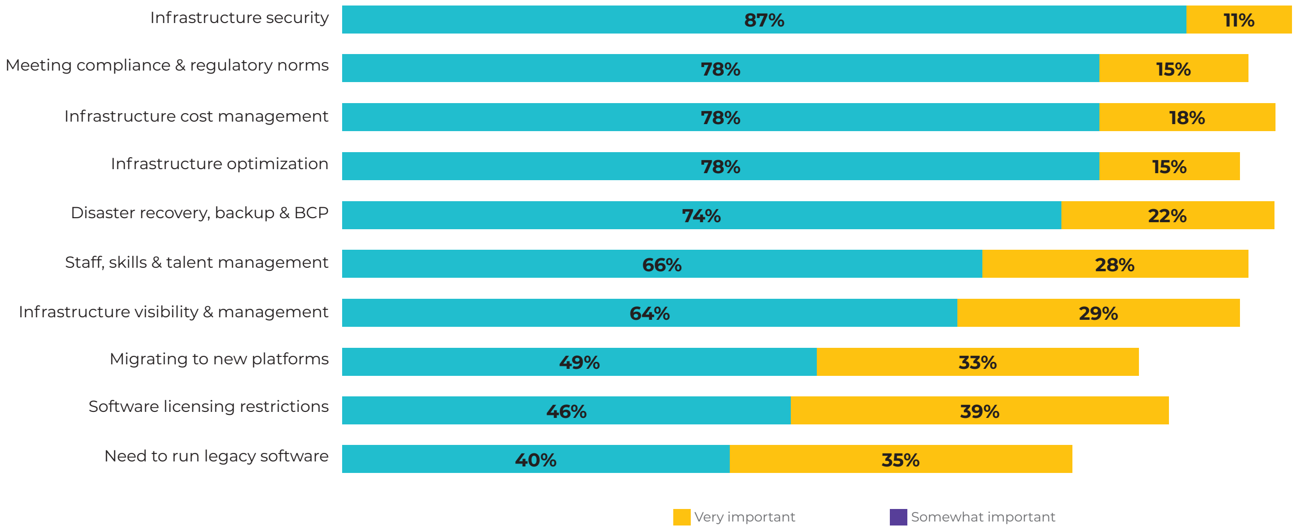


Figure 4: Infrastructure security is paramount, followed by optimization and cost management, but compliance and disaster recovery also remain critical concerns.

Organizations should continue to invest in these cloud practices to enhance their IT capabilities, drive innovation, and maintain competitive advantages.

Top 3 Concerns: Infrastructure security is the top concern, with 87% of respondents considering it very important (See Figure 4). This highlights the critical need for robust security measures to protect against cyber threats, data breaches, and other vulnerabilities. Next, with 78% rating infrastructure optimization as very important, there is a clear preference for ensuring that IT resources are used efficiently while minimizing waste and improving performance. Managing infrastructure costs is of equal priority, with 78% considering it very important. The emphasis on both optimization and cost management highlights the interconnected nature of these concerns, where optimizing infrastructure also helps in managing costs effectively.

Trend and Analysis: The importance of infrastructure security increased from 83% in 2023 to 87% in 2024, highlighting a growing emphasis on protecting IT assets. Organizations continue to enhance their security measures, focusing on advanced threat detection, endpoint security, and regular security audits to mitigate evolving cyber threats.

The importance of infrastructure optimization surged from 63% in 2023 to 78% in 2024. This increase reflects a growing need to maximize the efficiency and performance of IT infrastructure. The decrease in “somewhat important” responses validates that CIOs are viewing optimization as a critical, rather than secondary concern.

The importance of cost management rose significantly from 61% in 2023 to 78% in 2024.

Top Reasons for Using Cloud Services

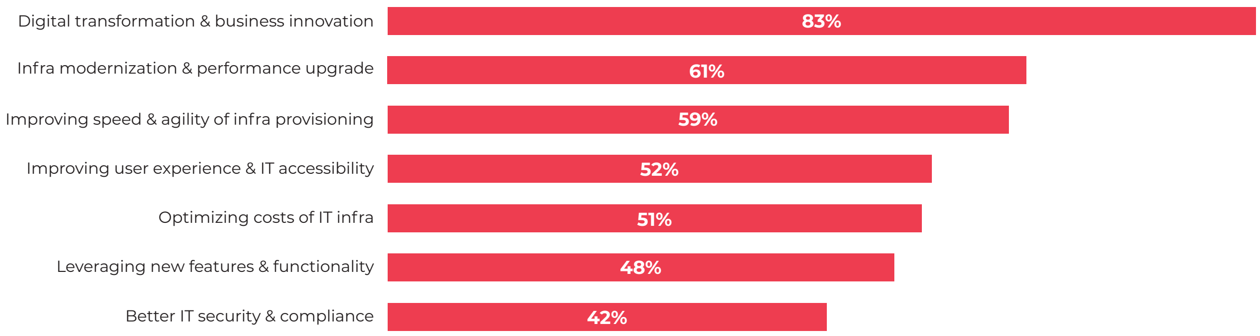


Figure 5: With focus on improving speed, agility, and user experience, digital transformation and infrastructure modernization are key drivers for cloud adoption.

This underscores the increasing pressure on IT departments to control and reduce infrastructure costs. Again, the percentage of "somewhat important"responses decreased significantly, validating that more organizations are now viewing cost management as a top priority.

Actionable Insights: The top three concern areas discussed above highlight the critical aspects of IT infrastructure that organizations need to prioritize. By focusing on these areas, organizations can enhance their security posture, optimize resource usage, manage costs effectively, and ensure compliance with regulatory requirements, thereby supporting sustainable and resilient IT operations.

Organizations could consider prioritizing investments in advanced security technologies, such as intrusion detection systems, firewalls, encryption, and regular security audits. Additionally, implementing comprehensive security policies and employee training programs can enhance overall security posture.

Implementing automation and monitoring tools would enable continuously assessing and improving infrastructural performance. Also, by conducting regular financial audits and optimizing resource allocation could avoid overspending on underutilized resources.

Overall, the comparison between 2023 and 2024 data highlights a clear trend towards prioritizing infrastructure security, optimization, and cost management. The increased emphasis on these areas indicates a growing recognition of their critical role in ensuring the efficiency, security, and financial sustainability of IT operations.

Key Challenges in Using Cloud Services

Top 3 challenges	Ranking in 2024	Ranking in 2023
Cloud security	1 ↔	1
Cost of cloud services	2 ↑	3
Compliance and regulatory issues	3 ↓	2

Drivers for Using Cloud Services Over the Next 12 Months

As per the survey results, the top three drivers for using cloud services in the next 12 months are: digital transformation and business innovation; infrastructure modernization and performance upgrades; and improving speed and agility of infrastructure provisioning (See Figure 5). These highlight the strategic importance of cloud adoption. Organizations focus on leveraging cloud services to drive innovation, modernize their IT infrastructure, and enhance agility to stay competitive in the rapidly evolving business landscape. By prioritizing these areas, businesses aim to fully realize the benefits of cloud technology and achieve their strategic objectives.

Top 3 Challenges: Cloud security is the top challenge, with 80% of respondents identifying it as very important (See Figure 6). This underscores the critical need to protect sensitive data and applications from cyber threats.

The cost of cloud services is equally important, with 80% of respondents viewing it as a very important challenge. This reflects concerns about managing and optimizing cloud expenditures.

Compliance and regulatory issues are identified as very important by 78% of respondents, indicating the significant pressure to adhere to various industry regulations and standards. Non-compliance can lead to severe legal and operational risks, including fines, penalties, and damage to business reputation.

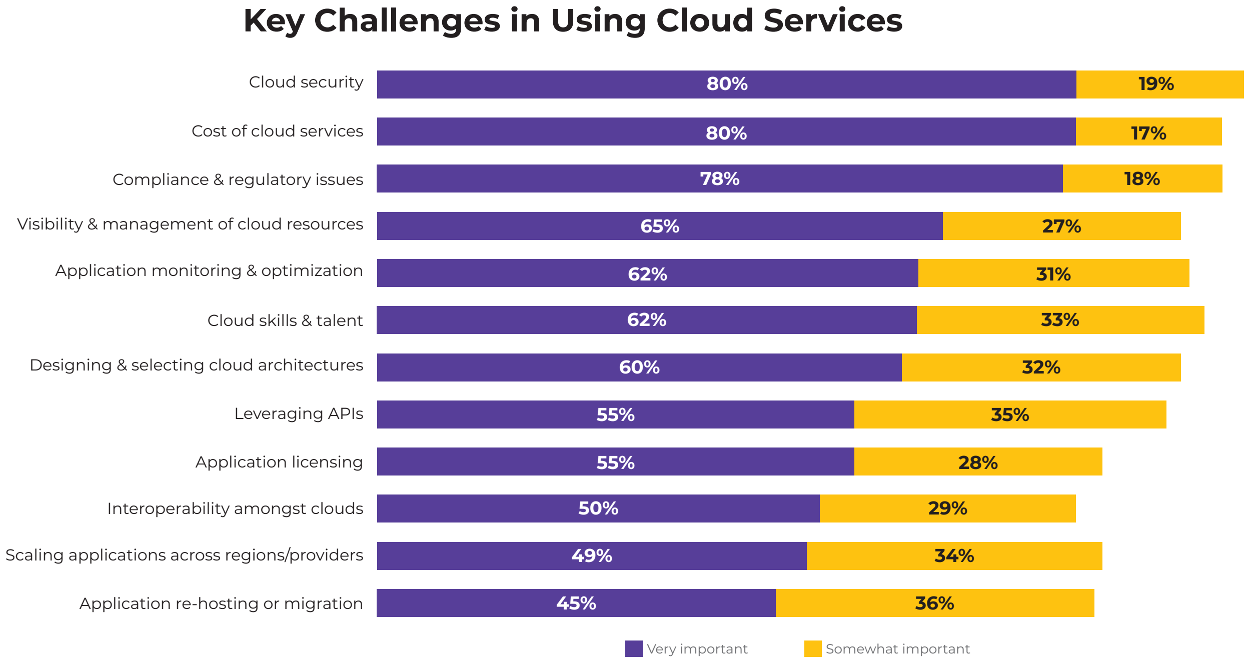


Figure 6: Cloud security and service costs are top challenges, but compliance, resource management, and application monitoring also pose significant concerns.

Trend and Analysis: The perception of cloud security as very important decreased from 88% in 2023 to 80% in 2024. Despite this slight decrease, it remains a top concern. This is validated by the fact that the "somewhat important" responses jumped from 7% to 19%, indicating a broader acknowledgment of cloud security as a significant challenge. So, cloud security remains paramount, and organizations maintain vigilance by continuously updating security protocols, investing in advanced security technologies, and training staff on security best practices.

The importance of managing cloud service costs remains consistently high, albeit there is a slight decrease from 81% in 2023 to 80% in 2024. Moreover, the "somewhat important" responses increased from 14% to 17%, showing a growing concern across more organizations. This underscores the need for cloud cost management tools and conducting regular cost audits to help control cloud spending and optimize resource utilization.

The importance of compliance and regulatory issues also remains high, with only a slight decrease from 79% in 2023 to 78% in 2024. Also, the "somewhat important" responses increased from 14% to 18%, indicating that more organizations are recognizing the significance of compliance issues. This explains the clamor for keeping abreast of changes in regulatory requirements and maintaining comprehensive documentation toward mitigating compliance risks.

Actionable Insights: The key challenges in using cloud services discussed above highlight critical areas where organizations must focus their efforts to ensure successful cloud adoption and operation. By

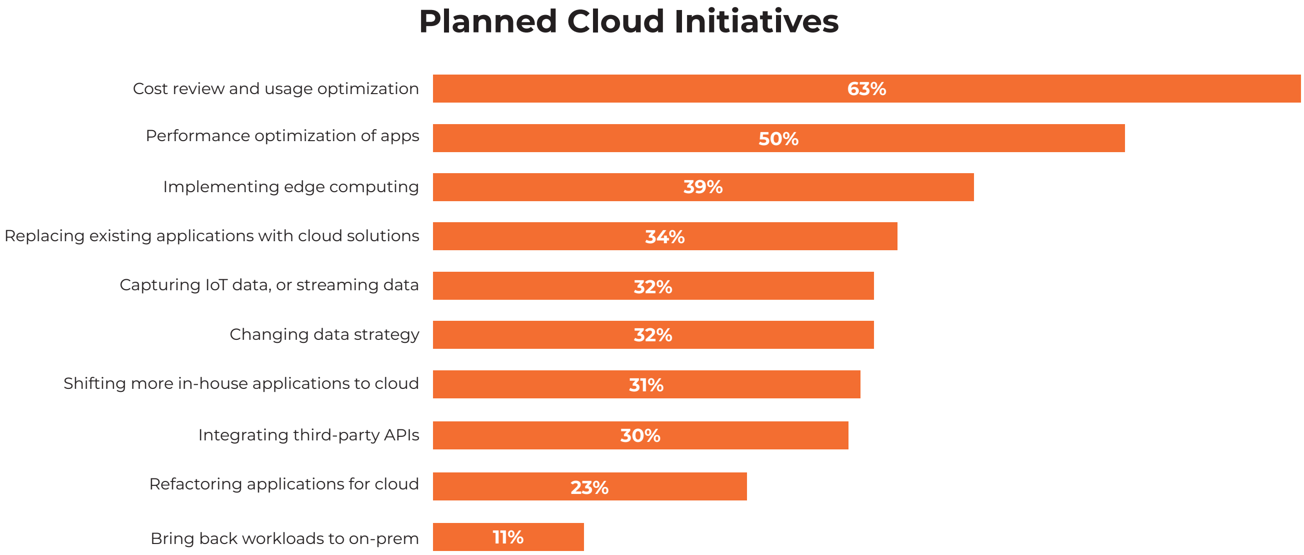


Figure 7: Cost optimization and app performance are the top priorities, with edge computing and shifting in-house applications to cloud are also in focus.

prioritizing robust security measures, implementing effective cost management strategies, and ensuring compliance with regulatory requirements, organizations can address these challenges and fully leverage the benefits of cloud services. Investing in the right tools, processes, and skills will be key to overcoming these challenges and achieving a secure, cost-effective, and compliant cloud environment.

Organizations should prioritize implementing comprehensive security measures, including advanced encryption, multi-factor authentication, continuous monitoring, and regular security audits. Additionally, adopting a zero-trust security model can further enhance the security posture in cloud environments.

To manage cloud costs effectively, organizations should implement cloud cost management tools, adopt reserved or spot instances where appropriate, and regularly review and optimize resource usage. Establishing governance policies to monitor and control cloud spending can help prevent cost overruns.

Organizations should invest in compliance management solutions that help monitor and enforce regulatory requirements. Regular compliance audits, employee training on regulatory standards, and working closely with legal and compliance teams can ensure adherence to relevant regulations and mitigate risks.

High-impact Operational Benefits of Using Cloud Services

Top 3 business benefits	Ranking in 2024	Ranking in 2023
Disaster recovery and business continuity	1 ↑	3
Work from anywhere capability	2 ↑	12
Better data security	3 ↑	15

Top IT Operational Priorities Planned for Cloud

Operationally, the top three priorities for the next 12 months are: cost review and usage optimization; performance optimization of apps; and implementing edge computing (See Figure 7). There has been a considerable shift in the priorities since last year when performance optimization of apps was the top priority, followed by integrating third-party APIs and capturing IoT data or streaming data.

The shift in CIO priorities from 2023 to 2024 highlights a natural progression in cloud adoption and optimization strategies. As organizations mature in their cloud journeys, they are focusing on cost management, maintaining and enhancing application performance, and adopting emerging technologies like edge computing to stay competitive and responsive to market demands. This evolution reflects a deeper understanding of cloud capabilities and a strategic approach to leveraging these technologies for sustainable growth and innovation.

Top 3 Operational Benefits: Disaster recovery and business continuity are considered high-impact benefits by 64% of organizations. This high priority underscores the importance of having robust backup and recovery plans to maintain business operations during disruptions (See Figure 8).

The ability to work from anywhere is a high-impact benefit for 62% of organizations. This reflects the ongoing shift towards remote and hybrid work models.

Better data security is identified as a high-impact benefit by 62% of organizations, which is reflective of

> "Assess each cloud's strengths and weaknesses, select services that fit each cloud’s capabilities, and plan your multi-cloud deployment accordingly. For data synchronization, use IaaS-based services to enhance your strategy."

Atish Bhanushali
Senior Vice President - IT & Head - Cloud COE & DevOps, HDFC Bank

the trust in cloud providers’ ability to offer advanced data security measures.

Trend and Analysis: The importance of disaster recovery and business continuity has increased from 59% in 2023 to 64% in 2024. This indicates a growing recognition of the critical role cloud services play in ensuring resilience against disruptions.

The percentage of respondents rating the impact of work from anywhere capability as “high” increased substantially from 45% in 2023 to 62% in 2024. This sharp rise reflects the ongoing shift toward remote and hybrid work models, accelerated by the COVID-19 pandemic and the need for flexible working arrangements. The perception of better data security as a high-impact benefit jumped significantly from 38% in 2023 to 62% in 2024. This increase highlights the growing trust in cloud providers’ security measures and a heightened focus on protecting data against breaches and cyber threats.

The 2024 survey marks a clear shift in the prioritization of cloud benefits, particularly with “work from anywhere capability” and “better data security” emerging among the top three benefits. This shift reflects the evolving needs of organizations to ensure resilience, flexibility, and security in their operations. By focusing on these high-impact areas, CIOs hope to better leverage cloud services to drive business continuity, support remote work, and protect critical data, ensuring sustained growth and competitiveness in a dynamic business environment.

Actionable Insights: Cloud services offer scalable and reliable solutions for disaster recovery, ensuring minimal downtime and quick recovery times, which are essential for business continuity. Organizations could further leverage cloud-based disaster recovery solutions to ensure resilience against outages and disasters. Regular testing and updating of disaster recovery plans are crucial to ensure effectiveness.

Cloud services facilitate remote work by providing secure access to applications and data from any location, enhancing flexibility and productivity for employees. To maximize this benefit, organizations should ensure that their cloud infrastructure supports secure and efficient remote access. Implementing VPNs, multi-factor authentication, and regular security audits can help maintain secure remote work environments.

Cloud services facilitate remote work by providing secure access to applications and data from any location, enhancing flexibility and productivity for employees. To maximize this benefit, organizations should ensure their cloud infrastructure supports secure and efficient remote access. Implementing

VPNs, multi-factor authentication, and regular security audits can help maintain secure remote work environments.

By focusing on these high-impact areas, organizations can maximize the value of their cloud investments, drive operational efficiency, and maintain their competitive advantages.

In conclusion, the landscape for cloud and IT infrastructure is marked by advanced deployment and strategic utilization of cloud services. CIOs must continue to balance innovation with security, cost management, and regulatory compliance to harness the full potential of cloud technologies. The insights from 2024 are aimed at providing a roadmap for CIOs to optimize their cloud strategies and address the evolving needs of their organizations.

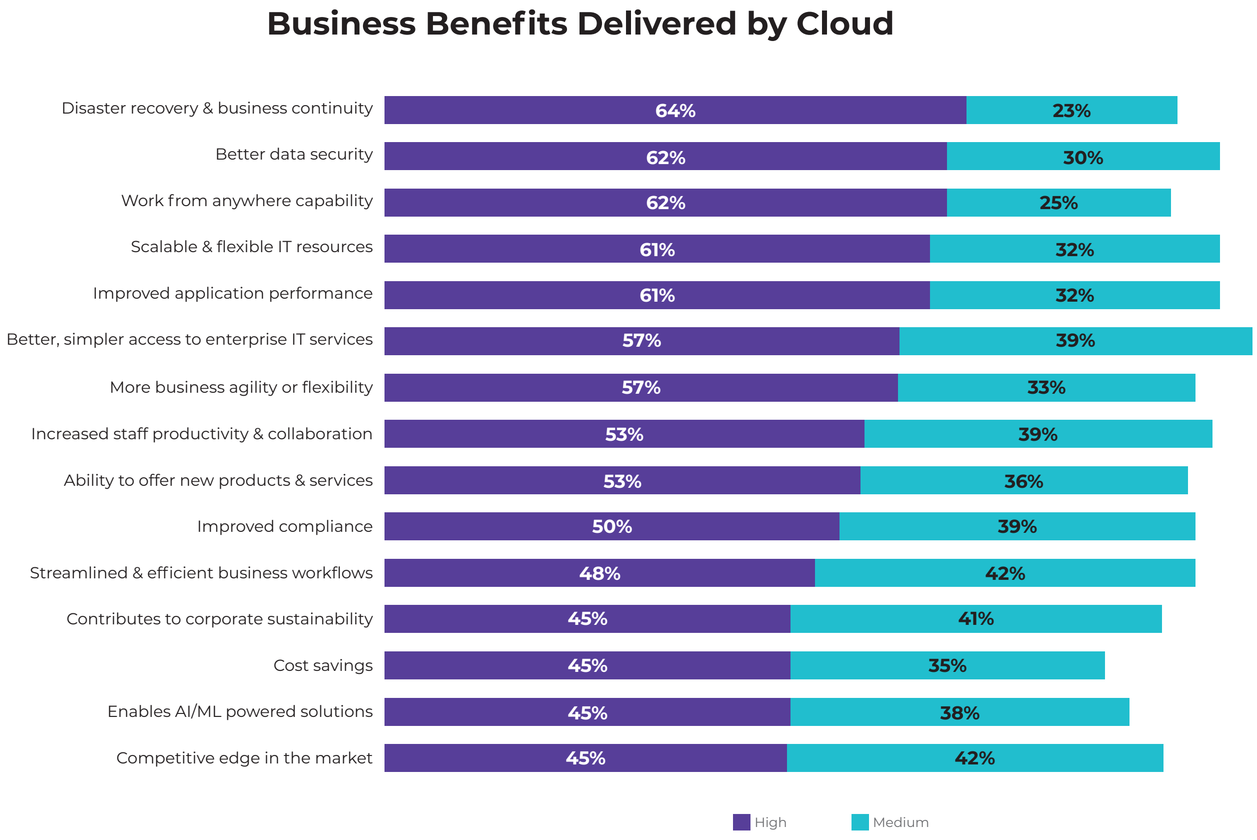


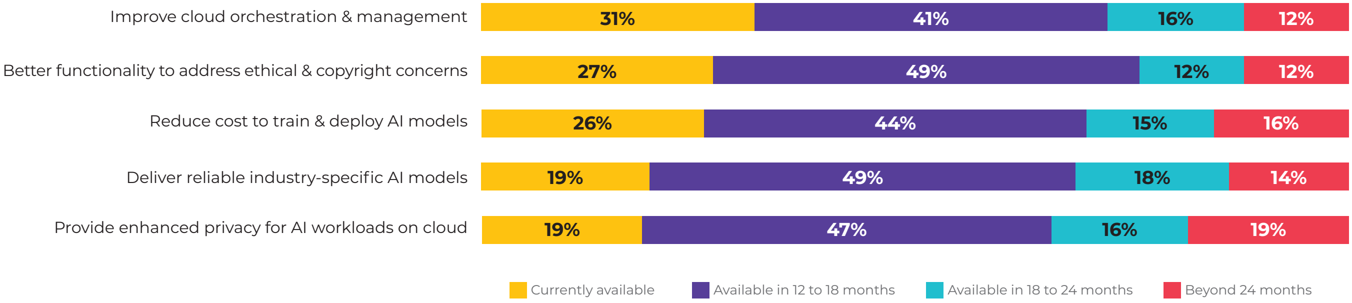
Figure 8: Disaster recovery, business continuity, and work-from-anywhere capabilities are top benefits, along with enhanced data security and improved application performance.

AI and Cloud & Infrastructure

AI's impact on cloud platforms and infrastructure is already significant, with 26% of organizations actively reducing costs to train and deploy AI models (See Figure 9). Enhanced privacy for AI workloads and reliable industry-specific AI models are set to be available within the next 12 to 18 months, at 47% and 49% respectively. This shows a concerted effort to address privacy concerns and deliver tailored AI solutions. Improving cloud orchestration and management is currently being implemented by 31% of organizations, with a further 41% planning to do so within 12 to 18 months. Ethical and copyright concerns are also being addressed, with 27% of organizations already taking steps, and another 49% planning implementations soon. The overall trend indicates a robust push towards integrating AI into cloud infrastructure to enhance functionality, privacy, and cost-efficiency while addressing emerging ethical challenges.

> "To optimize cloud usage, enterprises must align resource sizing with their cloud strategy governance framework. Regular monitoring, licensing audits, and reviews using analytics and FinOps can help reduce idle clusters and decrease cloud sprawl."

Nirupmay Kumar
Executive VP -
Technology, Demand &
Solution Management,
Vodafone Idea



Impact of AI on Cloud Platforms & Infrastructure

Figure 9: AI is transforming cloud platforms, reducing costs, enhancing privacy, and delivering reliable models. Significant advancements are expected within the next 12 to 18 months.

Data & Analytics

Leadership Lens: Navigating Challenges and Priorities

Apart from geo-driven regulatory norms, responsible data retention should ideally be built around the nature of the industry and its specific needs. A one-size-fits-all approach cannot be deployed. As a CxO, one should encourage participation from all internal and external stakeholders in building a robust data retention policy. This policy should cover:

- Categorization of master data based on key aspects like frequency of usage and nature of data.
- Establishing a data mart as a single source of truth for the organization's key data.
- Utilizing data retention to identify patterns and behaviors of the organization's key operational and expenditure parameters.

Beyond the use of effective out-of-the-box data management tools, maintaining data quality requires discipline and a focus on several pillars:

- Dedicated Data Steward to ensure comprehensive, persona-driven data marts.
- Technical Architects to ensure data uniformity, especially for data flow among various systems, and adaptability for elasticity

To embark on a successful analytics and modeling journey, organizations must focus on the following critical aspects:

- **Effective Master Data Management (MDM):** Implement robust controls for data generation, processing, and consumption to ensure high-quality and consistent data.
- **Single source of truth:** Establish a unified source of truth across the IT ecosystem, ensuring timely synchronization and consistency across relevant systems.
- **Data harmonization and cleansing:** Standardize and clean data across systems, functions, and business units. Establish guardrails and controls at data origin points, such as using common codes and definitions for products, customers, and vendors.
- **Data access and timeliness:** Ensure frequent and timely access to data for efficient extraction, transformation, and loading. This facilitates the generation of meaningful and actionable business insights.

Addressing these areas will provide a strong foundation for effective analytics and modeling, enabling better decision-making and strategic planning.

"A one-size-fits-all approach won't work. As a CxO, it's crucial to engage both internal and external stakeholders to collaboratively build a robust data retention policy."

Rajneesh Garg
Chief Information Officer & Senior VP, Allcargo ECU

"To succeed in analytics and modeling, focus on robust data management, a unified source of truth, data harmonization, and timely access for actionable insights."

Vininder Baweja
Chief Digital & Information Officer, Saint-Gobain India

FUELLING INNOVATION AND BUSINESS GROWTH

As new tools and technologies revolutionize businesses, the need to focus on advanced analytics, data integration, and strategic governance will be paramount.

Priority Actions for CIOs

1. Optimize data storage: Implement a balanced approach to data storage, ensuring that frequently accessed data is readily available while optimizing long-term storage solutions.

2. Enhance data architecture and technology: Invest in robust data architecture and technology to support growing data volumes and reach higher maturity in data strategy.

3. Leverage advanced analytics and AI: Mature the processes for aggregating and organizing data to enable the use of advanced analytics and AI, driving deeper insights and innovation.

4. Strengthen data governance and security: Increase focus on the governance of data use and data sharing, ensuring robust security and controls for data stores.

5. Improve data quality: Address the challenge of poor data quality by implementing data cleaning and management practices to ensure reliable inputs for advanced analytics.

6. Secure leadership support for data initiatives: Advocate for the importance of data quality and secure leadership support by demonstrating the ROI and strategic value of investments in data initiatives.

7. Identify impactful use cases: Work with business units to identify and develop high-impact use cases that showcase the value of data and analytics in driving business growth.

8. Enhance data literacy across the organization: Promote data literacy programs to align analytics initiatives with business goals and ensure all stakeholders understand the importance and potential of data-driven decision-making.

Executive Summary

The data and analytics landscape is experiencing significant transformations, driven by the need for organizations to harness data for competitive advantage. As CIOs, the strategic focus has shifted towards leveraging advanced analytics, machine learning, and AI to drive business insights and innovation. In 2024, data integration with third-party sources, data warehouses, and governance policies emerged as top priorities, with 63%, 58%, and 45% of organizations, respectively, having these in production. These trends indicate a strong emphasis on ensuring data accessibility, reliability, and compliance.

One notable trend is the maturation of data strategy elements. For instance, data architecture and technology have seen substantial improvements, with 34% of organizations reaching a reactive or opportunistic level and 29% achieving managed or systematic maturity. This reflects a growing recognition of the importance of robust data infrastructures to support advanced analytics capabilities.

Additionally, the volume of enterprise data continues to soar, necessitating sophisticated data management strategies. In 2024, hot data usage was predominant in organizations with less than 500 TB of data, with 73% in active use. Conversely, larger data volumes, such as those exceeding 100 PB, saw significant portions categorized as cold data, highlighting the need for efficient archival solutions.

Data analytics usage across business functions underscores its integral role in decision-making. Business planning and strategy, sales and marketing, and finance lead in advanced analytics adoption, with 37%, 35%, and 33% respectively, indicating a shift towards data-driven strategies to enhance operational efficiencies and market responsiveness.

Challenges persist, particularly in implementing robust analytics programs. Issues such as data quality, identifying right use cases, and securing business or leadership support are critical hurdles. Addressing these requires CIOs to foster a culture of data literacy, streamline data governance frameworks, and ensure alignment between analytics initiatives and overarching business goals.

Enterprise Data Volume by Storage Tiers

The analysis of enterprise data volumes by storage tiers in 2024 reveals that as data volumes increase, there is a significant shift towards archival (cold data) storage. Smaller volumes see more active (hot) usage, while larger volumes necessitate robust archival solutions to manage costs and performance effectively. There appears to be an acute focus on tailoring storage strategies based on data volumes, for ensuring that organization invest in the right mix of high-performance, warm, and archival storage solutions to optimize both access and cost-efficiency (See Figure 1).

The dataset provides insights into how enterprise data volumes are categorized across different storage tiers in 2024, including hot data (active use), warm data (intermittent use), and cold data (archival). Here's an analysis of the data distribution across various storage tiers:

Less than 500 TB: A significant majority of respondents use hot data in this tier (73%), indicating active usage. This is likely because smaller data volumes are easier to manage and access frequently. A substantial percentage of respondents use warm data also (54%), suggesting that while actively used, some data is accessed less frequently. Only 30% of data is cold, reflecting that with smaller data volumes, there is less need for extensive archival.

Total Volume of Data

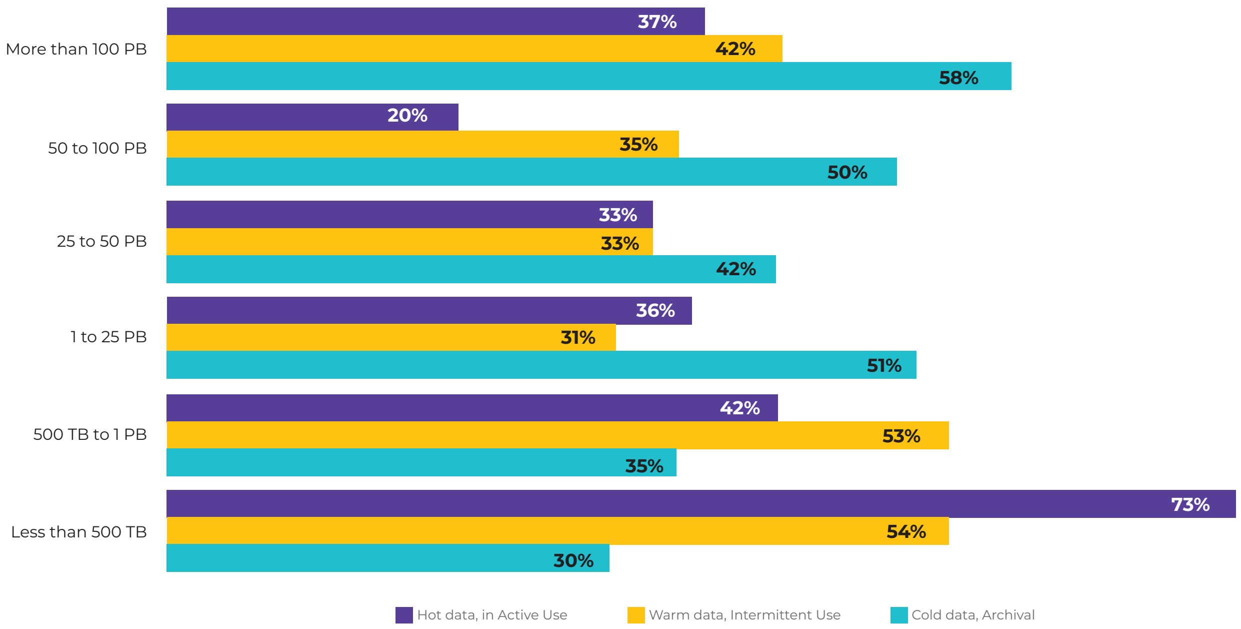


Figure 1: The under-500 TB tier remains dominant, but a declining trend has set in, as some of the higher storage tiers are gaining, albeit slowly.

However, there is a significant decrease in respondents using hot data in this tier (from 82% in 2023 to 73% in 2024), which could be indicating a shift towards more balanced data management. Percentage of respondents using cold data has also decreased from 46% to 30%, which could be suggestive of improved data lifecycle management practices.

Actionable Insight: Organizations with smaller data volumes should focus on optimizing their infrastructure for high-speed access and performance, ensuring that hot data storage is efficient and cost-effective.

500 TB to 1 PB: In this tier, a moderate percentage of respondents are using hot data (42%), which implies active use, but a more significant percentage of respondents are using warm data (53%), indicating intermittent use. The percentage of cold data users (35%) is higher for this tier compared with lower tiers, suggesting a growing need for archival as data volume increases.

Hot data usage remains relatively stable (with slight increase in respondents from 41% in 2023 to 42% in 2024). This is accompanied by decrease in both warm and cold data users in the category, thereby indicating better data classification and management.

Actionable Insight: For medium-sized data volumes, organizations should balance their investments in both high-performance storage for hot data and efficient archival solutions for cold data to optimize costs and performance.

1 to 25 PB: Only 36% of respondents are using hot data in this tier, indicating reduced active usage as data volumes increase in this tier, while 31% data is warm. Over half (51%) of the data is cold, reflecting significant archival requirements.

Hot data usage has remained consistentin 2023 and 2024. Cold data usage has seen some decrease, indicating improved data lifecycle management and archival strategies.

Actionable Insight: Organizations should implement robust archival strategies and storage solutions that can efficiently manage large volumes of cold data, reducing costs associated with maintaining rarely accessed information.

25 to 50 PB: Data usage is evenly split between hot and warm (33% respondents each), with a substantial usage being for cold data (42% respondents). A significant amount of data falls in the cold category, necessitating effective archival solutions.

There has been a significant reduction in hot datausage (from 41% respondents in 2023 to 33% in 2024), indicating more efficient categorization of active versus less frequently used data. Increase in warm data users suggests more intermittent data access requirements.

Actionable Insight: A balanced approach should be taken to manage both active and archival data, ensuring that storage solutions are optimized for both frequent access and long-term storage.

50 to 100 PB: In this tier, only 20% of respondents use hot data, while 50% prefer it for cold data usage, thus showing a significant shift toward archival storage. Warm data usage is by 35% respondents, indicating that a portion of the data is accessed intermittently.

In this category too, significant reduction in hot data (from 33% in 2023 to 20% in 2024) indicates better management of active data. Warm data usage remains consistent, with a slight increase.

Actionable Insight: Organizations should focus on scalable archival storage solutions that can handle large volumes efficiently, while ensuring that warm data storage remains cost-effective and accessible.

More than 100 PB: A relatively high percentage of respondents (37%) use this tier for hot data and 42% use it for warm data, indicating significant active and intermittent use even with very large volumes. A significant percentage of respondents (58%), the highest among all tiers, use these storage solutions for cold data, which reflects their need for extensive archival solutions.

This category has bucked the trend with a substantial increase in hot data users (from 31% in 2023 to 37% in 2024), which is indicativeof more active usagein case of very large data volumes. Warm data user percentage has also jumped significantly, suggesting more balanced data access requirements. For cold data usage, although the user percentage remains high, their numbers have significantly reduced over the previous year, which suggests changes in archival strategies and better utilization of other storage tiers.

Actionable Insight: For very large data volumes, a comprehensive data management strategy is essential, focusing on efficient archival systems, cost-effective warm data storage, and maintaining high performance for hot data.

Enterprise Data Growth by Application Type

When we compare 2024 survey results with 2023 results, three broad trends are discernible. For the first growth bracket (less than 25% growth), almost all media types have seen decreased growth since 2023, even though this bracket has the highest percentage shares. Two media types are exceptions, namely, image and PDF files, and text data (See Figure 2).

To illustrate, in the first growth bracket, the growth rate for audio files declined from 60% in 2023 to 47% in 2024, but this growth bracket still had the highest

Which Data is Growing How

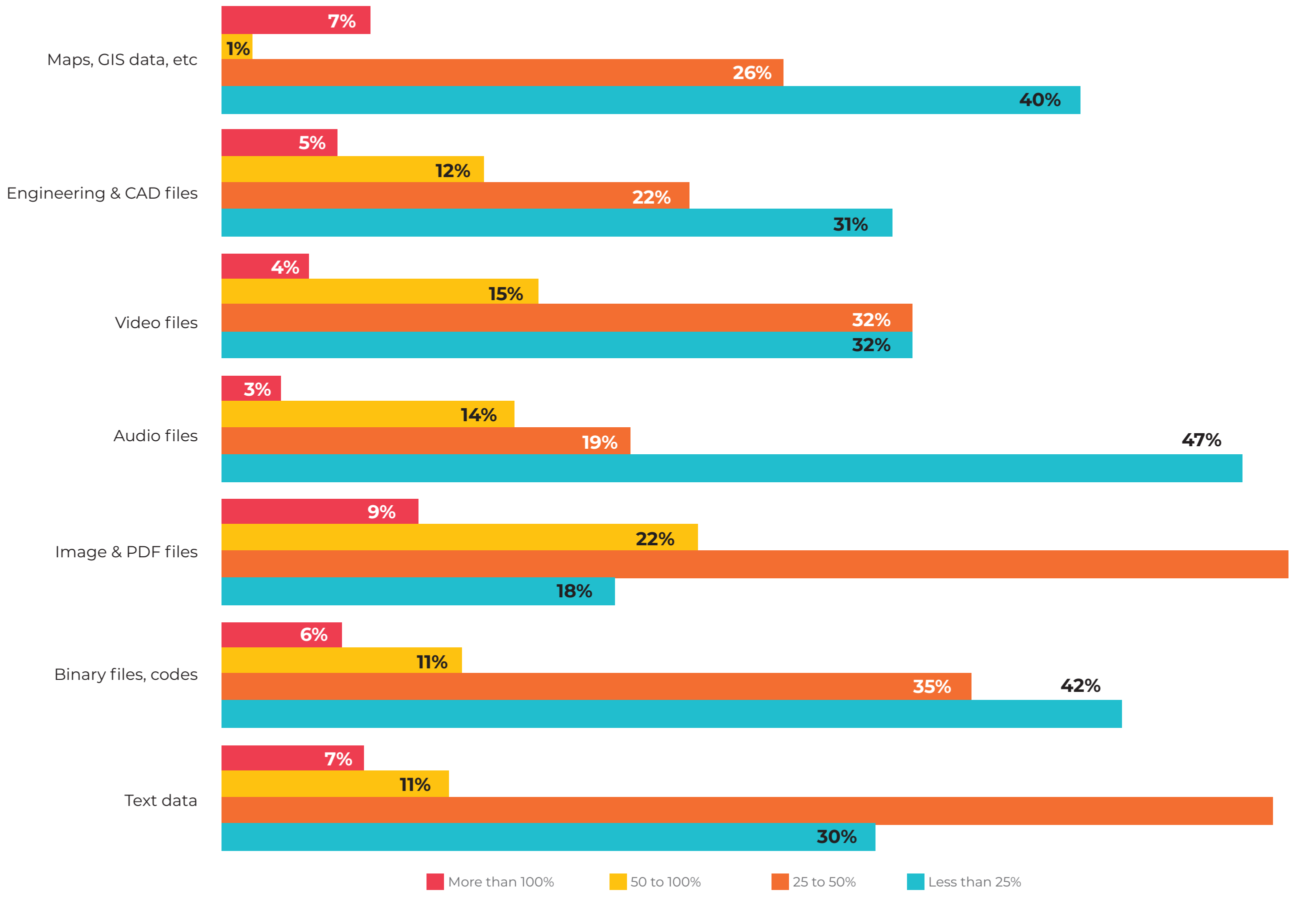


Figure 2: Image and PDF files, text, and videos show higher growths, while slower growth is relatively more prevalent across other data types.

percentage share for audio files. For audio files, 19% growth came in the second growth bracket (25–50% growth); followed by 14% in the third growth bracket (51–100% growth); and 3% in the fourth growth bracket (more than 100% growth).

In this perspective, we assess the data growths of various media types.

Audio Files: The percentage of audio files in the first growth bracket decreased from 60% in 2023 to 47% in 2024; the second growth bracket saw an increase from 7% to 19%; and third growth category remained relatively stable, with a slight increase from 12% to 14%.

There is a shift toward more moderate growth in audio files, with a decrease in the very slow growth bracket. However, while there has been a good increase in share in the second bracket, the distribution is still skewed toward the low-growth bracket.

Binary Files, Codes: The percentage share of binary files in the first bracket decreased from 51% in 2023 to 42% in 2024; thesh are in the second bracket saw a slight increase from 32% to 35%; and the third and fourth growth bracketsalso saw slight increase but with single-digit shares.

There is a trend toward more balanced growth in binary files, with a decrease in the slow growth category and a slight increase in higher growth categories, along with a good distribution of shares in low and higher brackets.

Engineering & CAD Files: The percentage of engineering and CAD files growing less than 25% decreased from 39% in 2023 to 31% in 2024; while the secondgrowth bracket saw an increase from 13% to 22%.

Maturity Levels of Data Strategy Elements

Top 3 data strategy elements	Ranking in 2024	Ranking in 2023
Data architecture and technology	1 ↑	4
Data engineering and DataOps	2 ↑	3
Data analytics and usage	3 ↓	1

It may be inferred that there is a shift toward more moderate growth in engineering and CAD files.

Image & PDF Files: The percentage of image and PDF files growing less than 25% decreased significantly from 33% in 2023 to 18% in 2024. Also, there was a significant increase in the second growth bracket (from 37% to 49%) and a moderate growth in the third growth bracket (from 16% to 22%). Thus, a notable shift toward higher growth rates is discernible for image and PDF files.

Maps, GIS Data, etc.: The percentage of maps and GIS data growing less than 25% decreased from 47% to 40%, while the share in the 25 to 50% growth category increased from 18% to 26%. There is a shift towards moderate growth in maps and GIS data.

Text Data: The percentage of text data growing less than 25% decreased from 52% to 30%, while the 25 to 50% growth category saw a significant increase in share from 22% to 49%. There is a significant shift toward moderate growth in text data.

Video Files: The percentage of video files growing less than 25% decreased from 38% to 32%, while share in the 25 to 50% growth category increased from 22% to 32%. There is a shift towards more balanced growth in video files.

Level of Maturity of Data Strategy

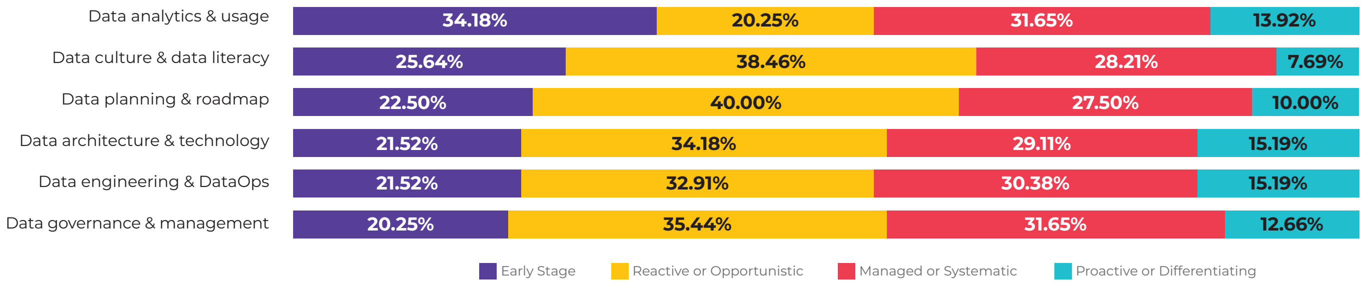


Figure 3: Data architecture and technology, and data engineering and DataOps are maturing relatively faster than other strategies.

Actionable Insights: The comparison between 2023 and 2024 data reveals distinct trends in enterprise data growth by application types. There is a general shift towards moderate growth across various data types, with significant increases observed in image and PDF files, text data, and video files. Organizations should tailor their storage strategies to accommodate these growth patterns, ensuring efficient, scalable, and cost-effective data management solutions to support the evolving needs of their data infrastructure.

We classified the maturity levels of various enterprise data strategy elements into four categories—early stage; reactive or opportunistic; managed or systematic; and proactive or differentiating—and sought responses from IT leaders for various data strategy elements in use.

The survey findings in 2024 show that data architecture and technology strategies of enterprises lead in terms of attaining the proactive or differentiating stage of maturity, showing that 16% of the organizations have fully mature and optimized data architecture and technology strategies in place (See Figure 3). A significant percentage (29%) are in the managed or systematic stage, while the maximum percentage are in reactive or opportunistic stage (34%), indicating that many enterprises are still adapting and responding to immediate needs rather than having a fully established strategy. Nevertheless, the majority of organizations are past the early stage, which harbors only 22% of the organizations.

The maturity level of enterprises for their data engineering and DataOps strategyis almost at par with that of the data architecture strategy, with 15% being in the proactive or differentiating stage; a notable 30% having a managed or systematic approach; and the most significant proportion (33%) being in the reactive or opportunistic stage.

For data analytics and usage strategy, only 14% of the enterprises are in the proactive or differentiating stage, suggesting that advanced analytics practices are less widespread. This is followed by a notable presence (32%) in the managed or systematic stage, reflecting ongoing progress toward structured and strategic data analytics. However, the largest percentage (34%) of organizations are still in the early stages of data analytics and usage, indicating a nascent development in leveraging data for insights.

Trend and Analysis: For data architecture and technology, the share of the proactive or differentiating stage increased substantially from 4% in 2023 to 15% in 2024, complemented by a significant decrease in the share of managed or systematic stage from 52% to 29%. However, there was also an increase in percentage of organizations in the early stage increased from 16% to 22%, along with a comparable increase in the share of reactive or opportunistic stage from 27% to 34%.

The significant increase in the proactive or differentiating stage indicates that some organizations are making substantial advancements and optimizing their data architecture and technology strategies. The survey results also indicate a mixed maturity level in data architecture and technology, with some organizations advancingfrom the managed stage to the proactive stage, along with new organizations entering the early and reactive stages. However, it is also indicated that some organizations may have regressed to the early and reactive stages.

For data engineering and DataOps, the share of the proactive stage saw a significant increase from 6% to 15%, accompanied by decrease in shares across the other stages. The share of early stage decreased from 25% to 22%; the share of the reactive stage decreased slightly from 34% to 33%, and that of the managed stage decreased from 34% to 30%.

There is a clear trend towards higher maturity levels, with a significant increase in proactive maturity indicating advancements in data engineering and DataOps.

Notably, for data analytics and usage, the percentage of organizations in the early stage increased significantly from 21% in 2023 to 34% in 2024. There is also a notable decrease in the reactive or opportunistic stage from 31% to 20%; and the share of managed or systematic stage too saw a slight decrease from 37% to 32%. However, the share of the proactive or differentiating stage increased from 10% to 14%.

Thus, there is a regression towards the early stage, indicating a possible restructuring or re-evaluation of data analytics strategies. However, the increase in proactive maturity shows that some organizations are advancing.

Actionable Insights: Data architecture and technology, data engineering and DataOps, and data analytics and usage are critical areas where enterprises should focus their efforts to enhance maturity, improve efficiency, and gain strategic advantages from their data initiatives. Investing in these areas will enable organizations to achieve higher levels of data strategy maturity and better leverage their data assets for competitive differentiation.

While the notable rise in proactive maturity particularly indicates significant advancements for some organizations, there is a need to strike a balance between improving foundational strategies and investing in advanced, differentiating technologies to

Top 3 Data and Analytics Models and Policies in 2024

Top 3 data and analytics	Ranking in 2024	Ranking in 2023
Data integration with third-party sources	1 ↑	2
Data warehouse	2 ↓	1
Data governance policy	3 ↔	3

achieve a cohesive and efficient data architecture. Focusing on structured growth and systematic improvements will help in moving towards higher maturity levels, ultimately leveraging the various strategies for better organizational outcomes.

Top 3 Data and Analytics Models: With 63% of organizations having data integration with third-party sources in production, this indicates a high level of adoption and maturity in integrating external data sources. Further, 13% are currently evaluating and another 13% are planning to implement within the next 12 months, which shows ongoing interest and development. Only 11% have no plans or see no need for this integration, reflecting the relative importance of this model (See Figure 4).

A substantial 58% of organizations have data warehouses in production, indicating a high adoption rate. Also, 17% are evaluating and 10% are planning to implement within the next 12 months, showing sustained interest in data warehousing. However, 14% have no plans or see no need for data warehouses, suggesting some organizations may be exploring alternative data storage solutions.

With 45% of organizations having data governance policies in production, this reflects a moderate to high level of adoption. Moreover, 26% are in evaluation, and 21% are planning to implement within the next 12 months, indicating robust ongoing development. Only 9% have no plans or see no need for data governance policies, highlighting its importance for data quality, security, and compliance.

Trend and Analysis: The percentage of organizations with data integration in production increased from 57% in 2023 to 63% in 2024, while those in theevaluation stage decreased from 17% to 13%. Also, percentage of organizations in the planning stage slightly decreased from 14% to 13% and so did the percentage of organizations with no plans or need

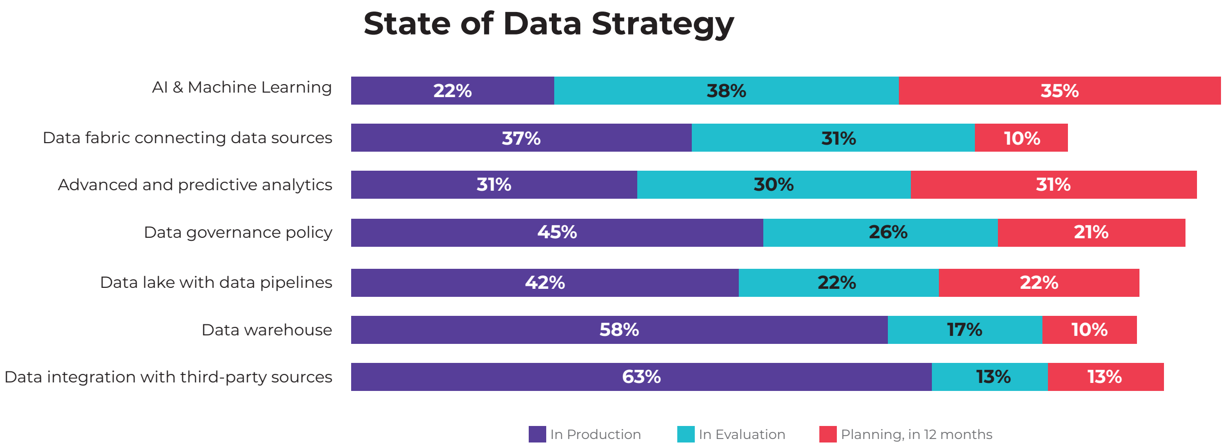


Figure 4: Data integration with third-party sources and data warehouses have high production levels, while AI/ML and advanced analytics are primarily in evaluation or planning stages.

for data integration (from 12% to 11%).The increase in production indicates a growing maturity and widespread adoption of data integration with third-party sources, reflecting its critical role in data strategy.

The percentage of organizations with data warehouses in production increased marginally from 57% in 2023 to 58% in 2024, while the share in the evaluation stage increased from 13% to 17%.The percentage of organizations in the planning stage decreased from 16% to 10%, whilethe percentage of organizations with no plans or need for data warehouses remained unchanged at 14%.The steady production rate and increased evaluation indicate sustained interest and development in data warehousing, which is a time-tested model.

The percentage of organizations with data governance policies in production decreased from 52% in 2023 to 45% in 2024, while those in the evaluation stage increased from 21% to 26% and the share in the planning stage slightly decreased from 23% to 21%. However, the percentage of organizations with no plans or need for data governance policies increased from 5% to 9%. The decrease in production and increase in evaluation and no plans may suggest a shift or reassessment of data governance strategies in favor of some other model.

Actionable Insights: The analysis of the top three data and analytics models and policies by their adoption stages in 2024 shows significant adoption and ongoing interest in data integration with third-party sources, data warehouses, and data governance policies. These elements are crucial for effective data management and utilization. Organizations should continue to optimize these areas, ensuring they support strategic goals and adapt to evolving data needs and regulatory landscapes. For those still in the evaluation or planning stages, prioritizing scalability, integration, and compliance will be key to successful implementation and maturation of these data strategies.

Organizations should focus on optimizing integrations with third parties, to ensure they facilitate seamless data flow and enhance data quality and accessibility from various external sources.

For organizations in the evaluation or planning stages of data warehouses, focus on scalability, integration capabilities, and performance optimization of data warehouses will be crucial. Those with existing implementations should continue to optimize data management and retrieval processes.

Organizations should prioritize establishing and refining robust data governance frameworks to ensure data integrity, security, and regulatory compliance. For those in evaluation or planning stages, aligning governance policies with organizational objectives and regulatory requirements will be essential.

Measures Taken to Ensure Data Integrity

Top 3 data and analytics	Ranking in 2024	Ranking in 2023
Data backup	1 ↔	1
Data security control	2 ↔	2
Data encryption	3 ↑	7

Top 3 Measures: Data backup is the most widely implemented measure, with 70% of organizations having it in place. Another 20% of organizations are in the process of implementing data backups, showing ongoing efforts to enhance data integrity, while a further 8% plan to implement data backups within

Acquisition/deployment model planned for AI, ML solutions.

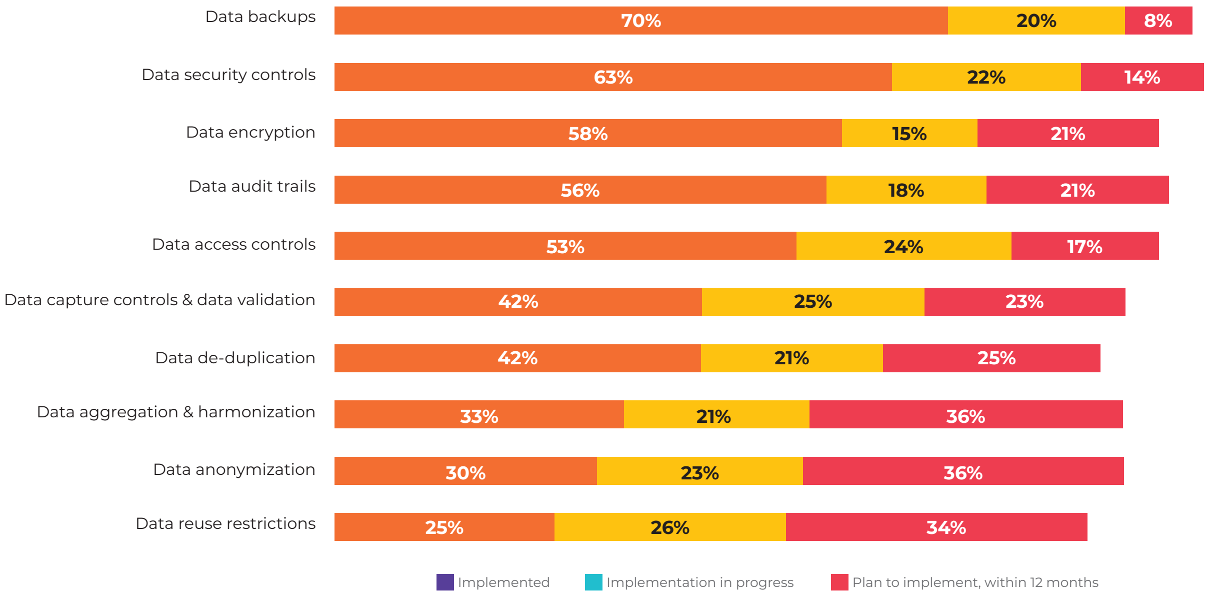


Figure 5: Data backups and security controls are widely implemented, followed by encryption, audit trails, and access control as crucial measures for maintaining data integrity.

the next 12 months, indicating that this measure is the top priority (See Figure 5).

Data security controls are implemented by 63% of organizations, reflecting the measure's critical role in protecting data integrity. Moreover, another 22% are currently implementing these controls, indicating active efforts to bolster data security. Yet another 14% plan to implement data security controls within the next 12 months, highlighting continued focus on enhancing security measures.

Data encryption is implemented by 58% of organizations, indicating a strong emphasis on protecting data privacy and integrity; 15% are in the process of implementing data encryption, showing ongoing efforts to secure data; and 21% plan to implement data encryption within the next 12 months, reflecting a high priority on enhancing data security.

Trend and Analysis: The percentage of organizations with data backup implementations decreased from 82% in 2023 to 70% in 2024; the percentage of data backups in progress increased from 10% to 20%; while those planning to implement data backups within 12 months slightly increased from 7% to 8%. Despite the decrease in implemented backups, the increase in progress and planning indicates continued focus on data backups, though there may be some shift toward alternative data protection strategies.

The percentage of organizations with data security controls implemented decreased from 68% in 2023 to 63% in 2024, while implementation in progress increased from 17% to 22%. The percentage planning to implement within 12 months remained unchanged at 14%. The decrease in implementation but increase in progress suggests ongoing efforts to enhance and update security measures. Stable planning figures indicate consistent prioritization of data security.

The percentage of organizations with data encryption implemented increased from 46% in 2023 to 58% in 2024, while implementation in progress decreased from 31% to 15%. The percentage planning to implement data encryption within 12 months increased from 18% to 21%. The survey results indicate that a good percentage of implementations in progress last year may have got completed, which led to the significant increase in implemented projects. This also reflects a growing emphasis on protecting data privacy and integrity, with increased planning also validating this by showing future focus.

Actionable Insights: Data backups, data security controls, and data encryption are critical focus areas for organizations. These measures have high implementation rates, reflecting their importance in maintaining data integrity and security. Organizations should continue to optimize these measures, ensuring they are comprehensive and uptodate to protect against evolving data threats and ensure data resilience. For those still in the implementation or planning stages, prioritizing these measures will be key to achieving robust data integrity and security.

Ensuring regular and automated data backups should be a fundamental practice for all organizations to safeguard against data loss and enhance data recovery capabilities. Organizations should prioritize the continuous improvement of data security controls to protect against data breaches and unauthorized access, ensuring robust defense mechanisms are in place. Implementing and maintaining robust data encryption protocols is essential for organizations to safeguard sensitive data from unauthorized access and ensure compliance with data protection regulations.

Maturity Levels of Data Analytics Usage by Business Functions

Top 3 business functions	Ranking in 2024	Ranking in 2023
Business planning and strategy	1 ↑	3
Sales and marketing	2 ↓	1
Finance	3 ↓	2

Top 3 Functions by Data Analytics Maturity: For business planning and strategy, 73% of organizations use MIS or reports, indicating a reliance on comprehensive reporting to inform strategic decisions; 65% use dashboards, reflecting the need for real-time insights and performance tracking; and 37% of organizations employ advanced analytics, demonstrating the importance of predictive and prescriptive analytics in strategic planning. Only 6% of organizations find data analytics not relevant for business planning and strategy, underscoring its critical role in this function (See Figure 6).

In sales and marketing, 78% of organizations use dashboards, highlighting the need for real-time tracking of sales metrics and marketing performance; 67% use MIS or reports, reflecting the importance of detailed reporting in tracking sales and marketing outcomes; and 35% use advanced analytics, indicating the growing role of data-driven insights in optimizing sales strategies and marketing campaigns. However, 9% of organizations do not find data analytics relevant for this function, indicating room for increased adoption.

Acquisition/deployment model planned for AI, ML solutions.

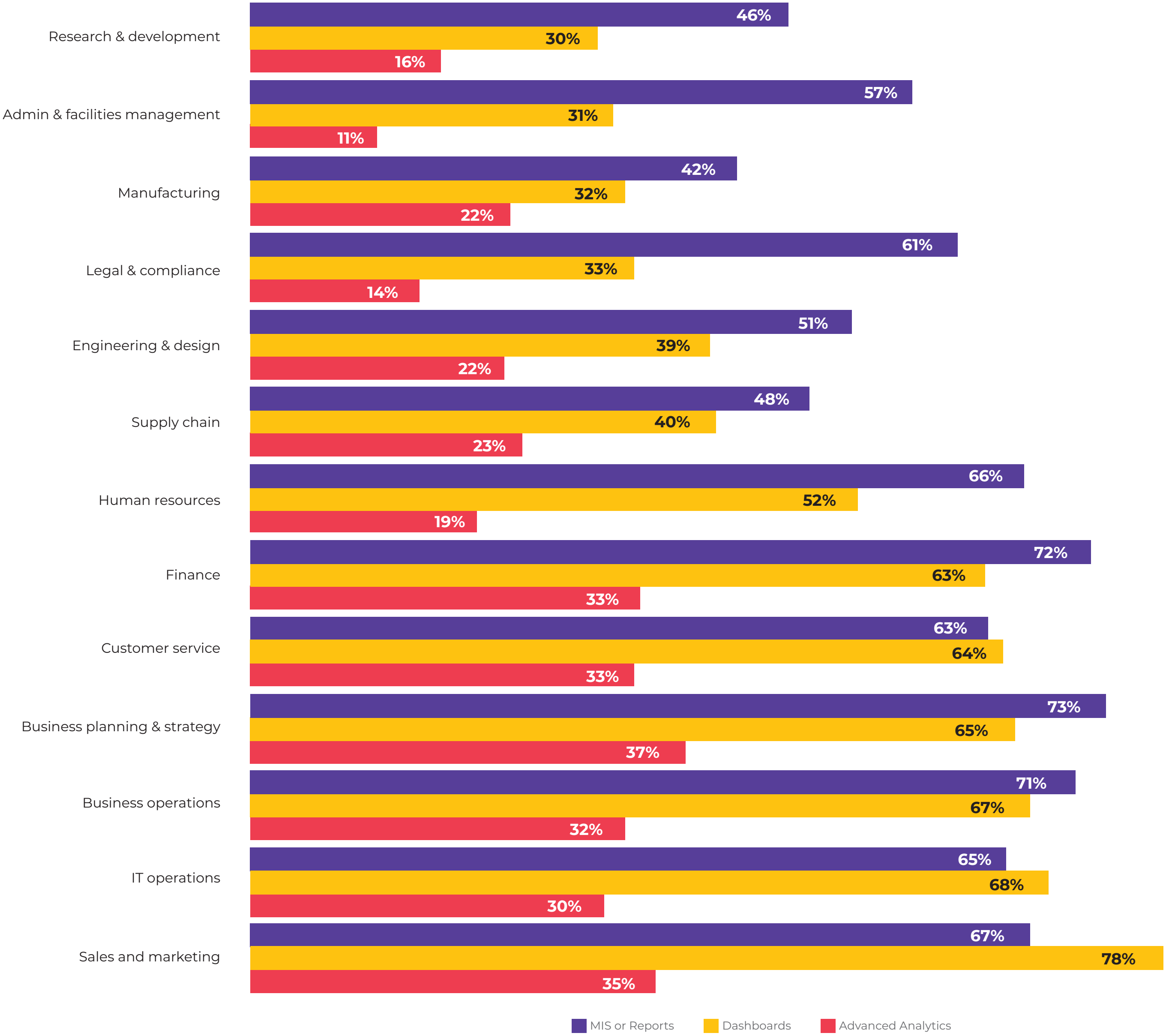


Figure 6: Dashboards and MIS reports are extensively used in like planning, sales, and finance, while advanced analytics is gaining traction in business planning and strategy.

In finance, 72% of organizations use MIS or reports, indicating a strong need for detailed financial reporting and analysis; 63% use dashboards, reflecting the importance of real-time financial monitoring and decision-making; and 33% use advanced analytics, demonstrating the role of predictive analytics in financial planning and risk management. Only 6% find data analytics not relevant for finance, highlighting its critical importance.

Trend and Analysis: For business planning and strategy,a slight decrease from 39% in 2023 to 37% in 2024 indicates a marginal decline in the use of advanced analytics.Dashboards decreased from 69% in 2023 to 65% in 2024, reflecting a small reduction in their reliance. MIS or reports increased significantly from 63% in 2023 to 73% in 2024, showing the growing importance of more detailed and comprehensive reporting for strategic planning.

For sales and marketing, a significantdecrease in use from 46% in 2023 to 35% in 2024, indicating a reduced emphasis on advanced analytics. Use of dashboards increased from 66% in 2023 to 78% in 2024, reflecting a heightened focus on real-time performance tracking. Use of MIS decreased from 79% in 2023 to 67% in 2024, showing a reduced reliance on traditional reports. Thus, there is a shift from advanced analytics and MIS or reports to a greater emphasis on dashboards, which indicates a preference for real-time insights and agile decision-making in sales and marketing.

The use of advanced analytics in finance declined from 42% in 2023 to 33% in 2024, indicating a reduced emphasis on advanced analytics in finance. Dashboards remained stable at 63%, showing their consistent use. Use of MIS decreased from 81% in 2023 to 72% in 2024, reflecting a reduced need for detailed reports. The reduced reliance on advanced analytics and MIS or reports, coupled with stable dashboard usage, suggests a shift towards more streamlined and routine data analytics in finance.

Actionable Insights: The study reveals a strong reliance on data analytics across various maturity levels. These functions extensively use MIS or reports, dashboards, and advanced analytics to drive strategic decisions, optimize performance, and enhance operational efficiency.

Organizations should continue to leverage and enhance advanced analytics capabilities to support strategic planning, ensuring they have access to deep insights and predictive models to drive informed decisions.

Sales and marketing teams should focus on expanding their use of advanced analytics to better understand customer behavior, optimize campaigns, and enhance sales strategies. Finance departments should enhance their use of advanced analytics to improve financial forecasting, risk assessment, and strategic financial planning, ensuring robust financial management and decision-making.

Key Challenges in Implementing Robust Analytics Programs

Top 3 challenges in implementing	Ranking in 2024	Ranking in 2023
Business or leadership support	1 ↔	1
Quality of data	2 ↑	4
Identifying right use cases	3 ↓	2

Top Three Challenges: Business or leadership support stands out as the most critical challenge, with a “very important” score of 85%, followed by “somewhat important” score of 14%. The success of analytics programs heavily relies on strong leadership endorsement. Lack of support can hinder resource allocation, slow down project timelines, and diminish the overall impact of analytics initiatives. This emphasizes the need for leaders to champion data-driven decision-making and ensure that analytics programs receive the necessary backing and investment (See Figure 7).

The quality of data is another significant challenge, underscored by 82% of respondents as very important, followed by 17% as somewhat important. High-quality data is essential for generating accurate insights and making informed decisions. Poor data quality can lead to incorrect conclusions, eroding trust in analytics solutions. Organizations must prioritize data cleansing, validation, and governance to maintain data integrity and reliability.

Identifying the right use cases is crucial for the effective implementation of analytics programs. With 81% of respondents marking it as very important and another 18% as somewhat important, it is clear that organizations need to focus on selecting use cases that align with their strategic goals and offer high value. Misalignment of use cases can result in wasted resources and missed opportunities. Therefore, a thorough assessment of potential analytics

Challenges in Implementing Analytics Programs

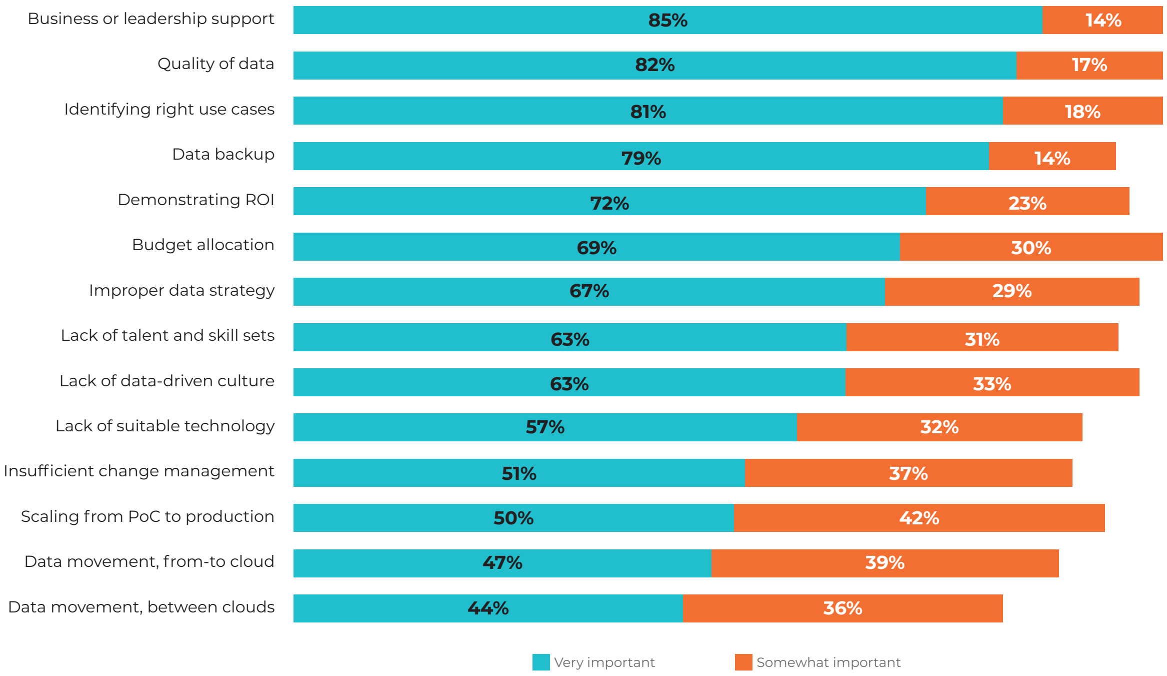


Figure 7: Leadership support, data quality, and identifying use cases are top challenges, as demonstrating is critical for successful implementations.

applications and their impact is vital for maximizing the benefits of analytics initiatives.

Trend and Analysis: Business or leadership support remains the top challenge in both 2023 and 2024. However, there is a slight decrease in the percentage of respondents considering it very important (87% in 2023 to 85% in 2024). This marginal decline suggests that while leadership support is still critical, organizations might be seeing slight improvements in gaining leadership buy-in for analytics programs.

The importance of data quality as a challenge has remained fairly consistent, with around 82% of respondents marking it as very important in both years. The consistency indicates that organizations continue to struggle with ensuring high-quality data, a foundational element for successful analytics.

The challenge of identifying the right use cases has shown only a slight decrease in the percentage of respondents considering it very important, from 82% in 2023 to 81% in 2024. This suggests that while it is still considered a significant challenge, there may be a growing capability or confidence within organizations in identifying impactful use cases for their analytics programs.

Actionable Insights: To successfully implement robust analytics programs, organizations in 2024 must ensure strong leadership support, maintain high data quality, and carefully select the most impactful use cases. Addressing these challenges will enhance the effectiveness and ROI of their analytics efforts, paving the way for more informed and strategic decision-making.

The comparative analysis of the key challenges in implementing robust analytics programs in 2024 versus 2023 shows that business or leadership support, quality of data, and identifying the right use cases remain top concerns. While there are slight variations in the percentages, these challenges consistently highlight the critical areas where organizations need to focus to ensure the success of their analytics initiatives.

In conclusion, the data and analytics landscape in 2024 presents both opportunities and challenges for CIOs. Prioritizing data integration, governance, and advanced analytics, while addressing skill gaps and strategic alignment, will be crucial for organizations aiming to thrive in an increasingly data-centric world.The landscape is marked by significant transformations as tech leaders prioritize leveraging advanced analytics, machine learning, and AI. Key trends include the maturation of data strategy

> "CIOs should ensure data storage and retention strategies include two copies—one in the cloud, and one on-premises or in another cloud. Compliance with DPDP law requires data masking, clear access management, encryption of key customer data, and monitored API interfaces."

Tushar Vagal
CIO & Digital Head - Realty,
Larsen & Toubro

elements and the increasing volume of enterprise data, with a strong focus on data integration, governance, and accessibility. Business functions such as planning, sales, and finance lead in advanced analytics adoption. However, challenges like data quality, identifying use cases, and securing leadership support persist. Addressing these will require enhancing data literacy, streamlining governance frameworks, and aligning analytics initiatives with business goals to thrive in a data-centric world.

AI and Data & Analytics

Enterprises are prioritizing the use of AI to overcome the data gravity trap, focusing on enhancing data processing strategies (48%) and improving data management processes (46%) within the next 12 months. This urgency underscores the critical need to handle vast amounts of data more efficiently (See Figure 8). Over the subsequent 12 to 18 months, efforts will likely continue with a notable emphasis on increasing performance, scalability, and reliability (42%), and enhancing resource utilization (42%). AI's role in enabling edge computing (29%) and reducing risk through predictive analytics (36%) will be pivotal, indicating strategic moves towards optimizing data handling and risk management. However, some enterprises have no immediate plans for AI adoption in areas like enabling edge computing (32%) and improving cost management (18%), highlighting potential areas for growth and focus. The data suggests a comprehensive approach where immediate enhancements in data processing and management are followed by broader, more integrated AI applications in the medium term.

Plans for Using AI to Overcome Data Gravity

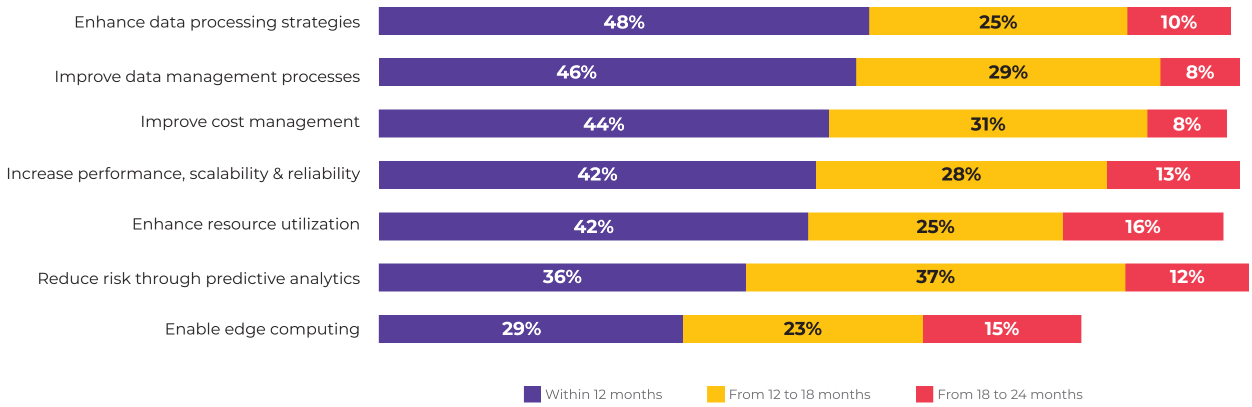


Figure 8: Enterprises focus on enhancing data processing and management strategies with AI, aiming for immediate improvements, while long-term plans include optimizing cost management and edge computing.

IT Security

Leadership Lens: Navigating Challenges and Priorities

Cybersecurity awareness is crucial yet often weak, primarily due to human error, negligence, or a lack of digital knowledge that cybercriminals can exploit. An organization's cybersecurity resilience relies heavily on its employees, which makes robust awareness and training programs essential as the first line of defense against cyber threats. It is important to educate individuals on practices such as multi-factor authentication and creating strong passwords to enhance security.

More than 90% of cyber-attacks involve social engineering, with phishing being the most prevalent. These attacks typically use spoofed emails and malicious links to deceive individuals into revealing sensitive information, such as login credentials, credit card numbers, or other personal details. To counteract these threats, organizations should deploy anti-spam solutions and increase awareness about phishing tactics among their employees. By addressing these issues proactively, organizations can significantly improve their defense mechanisms and reduce the risk of successful attacks.

Using AI in data security allows organizations to analyze data from various sources to identify patterns and detect unusual activities that may indicate malicious behavior. AI enhances threat detection capabilities by providing early warning notifications and automating responses, thus improving the efficiency and effectiveness of cyber defense strategies.

AI adds substantial value across numerous areas of cyber defense and operations, including:

- Identity and Access Management (IAM)
- Vulnerability and Risk Management
- User and Network Behavior Analysis
- Transaction Monitoring for Fraud Management
- Real-Time Monitoring, Reconciliation, and Reporting
- Incident Response
- Threat Intelligence and Threat Modeling

Incorporating AI into these areas helps organizations strengthen their cybersecurity posture, improve efficiency, and respond more effectively to evolving threats.

"An organization's cybersecurity resilience relies heavily on its employees, making robust awareness and training programs essential as the first line of defense against cyber threats."

Dr. Prashant Atreya
Executive Director
(IT&C), NHPC

"Integrating AI into data security enables organizations to analyze data from multiple sources, uncover patterns, and detect anomalies that may signal malicious activity."

Abhijit Chakravarty
Executive Vice President -
Networks & Cyber Security,
Kotak Mahindra Bank

NAVIGATING CHALLENGES IN AN ULTRACOMPLEX LANDSCAPE

Infosec leaders must balance innovation and security while addressing cyber threats, skill gaps, and cloud complexities to achieve organizational resilience and effective IT security.

Priority Actions for CIOs

1. Strengthen Employee Training and Security Culture: Implement comprehensive training programs and foster a culture of vigilance to address the human element as the weakest link in security.

2. Implement Robust Identity Management and MFA: Adopt stronger identity management practices and enforce pervasive multi-factor authentication (MFA) to combat password and identity-based attacks.

3. Focus on Business Continuity and Disaster Recovery: Enhance business continuity planning and disaster recovery (DR) strategies to mitigate the impact of security-related disruptions.

4. Bolster In-House Security Expertise: Invest in building in-house security expertise to ensure greater control and responsiveness to evolving security threats.

5. Align Security with Business Objectives: Ensure that security strategies are aligned with overall business objectives to support organizational goals and resilience.

6. Prioritize Security Investments: Focus on strategic investments in training, comprehensive security frameworks, and advanced security technologies to strengthen defenses.

7. Conduct Regular Penetration Testing and Audits: Proactively conduct regular penetration testing and security audits to identify and address vulnerabilities before they can be exploited.

8. Embrace Security Automation: Leverage automation to enhance security processes, reduce manual efforts, and improve response times to security incidents.

Executive Summary

In the rapidly evolving digital landscape, it has become increasingly pivotal to safeguard organizational data and infrastructure. As digital transformation accelerates, organizations are increasingly reliant on robust IT security measures to protect their assets, data, and operations from ever-evolving threats. The analysis of IT security trends and challenges for 2024 reveals critical insights that can help infosec leaders in fortifying their security postures and addressing emerging risks.

The IT security environment in 2024 is characterized by a heightened focus on managing complex, multi-faceted threats. Among the top challenges identified, cost and effort to manage security solutions, evolving threat environments, and alignment of security with business goals stand out prominently. For instance, 44% of CIOs consider the cost and effort to manage security solutions a high-priority challenge, emphasizing the need for efficient and scalable security strategies. Similarly, 43% of CIOs highlight the evolving threat environment as a significant concern, necessitating continuous adaptation and vigilance.

In response to these challenges, organizations are prioritizing specific measures to address skill gaps and enhance their security capabilities. Providing training for employees is the foremost strategy, with 69% of organizations already implementing comprehensive training programs. This proactive approach ensures that the workforce remains adept at countering new and sophisticated threats. Additionally, re-training technical staff (64%) and partnering with experts or consultants (59%) are critical components of the security enhancement strategy, reflecting a commitment to leveraging both internal and external expertise.

Deployment of IT security processes and operations also sees significant advancements. Penetration testing, adopted by 64% of organizations, remains a cornerstone of proactive security measures. The implementation of security standards and frameworks (58%) and security audits (56%) further underscores the emphasis on establishing rigorous and standardized security protocols. By addressing the key challenges and leveraging robust security processes, modern organizations can ensure that they remain secure, resilient, and positioned for future growth in an increasingly digital world.

IT Security Incidents by Severity in the Last 12 Months

Top 3 security incidents	Ranking in 2024	Ranking in 2023
Phishing attacks	1 ↔	1
Password/identity-based attacks	2 ↔	2
Ransomware attacks	3 ↔	3

Top 3 Incidents by Severity: Phishing attacks top the list as the most severe IT security incident, with 50% of respondents rating them as highly severe. The prevalence and effectiveness of phishing attacks, which often exploit human vulnerabilities, make them a significant concern for organizations. The high percentage of medium severity (33%) further underscores the pervasive nature of these attacks and the necessity for robust training and phishing prevention measures (See Figure 1).

Password and identity-based attacks are the second most severe incident, with 44% of respondents identifying them as highly severe and 27% considering them of medium severity. The continued reliance on password-based authentication and the increasing sophistication of identity theft techniques highlights the critical need for stronger identity

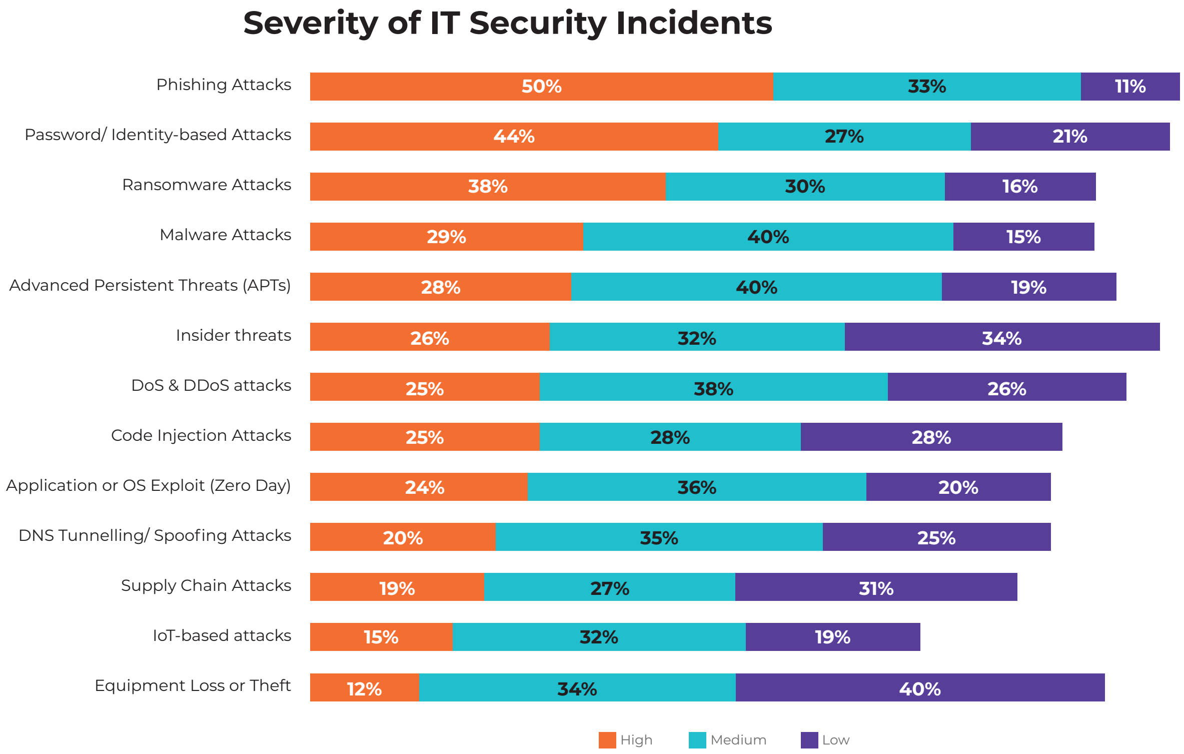


Figure 1: Phishing and identity-based attacks top the list, with ransomware and malware also posing notable threats.

management practices and the adoption of multi-factor authentication (MFA) solutions.

Ransomware attacks remain a significant threat, with 38% of respondents considering them highly severe. The financial and operational impact of ransomware, where attackers encrypt critical data and demand payment for its release, continues to pose a serious risk to organizations. The relatively high percentage of medium severity (30%) indicates that while some organizations may have effective measures in place, the threat remains substantial, necessitating continuous vigilance and investment in ransomware prevention and recovery strategies.

Trend and Analysis: Phishing attacks have increased in severity, with the percentage of respondents rating them as high rising from 40% in 2023 to 50% in 2024. This indicates a growing recognition of the impact of phishing attacks on organizations. The increase in medium severity ratings from 29% to 33% also highlights the continued prevalence of these attacks.

Password and identity-based attacks have seen a significant increase in perceived severity. The percentage of high severity ratings nearly doubled from 23% in 2023 to 44% in 2024. This shift underscores the growing threat posed by identity theft and credential-based attacks. The reduction in low severity ratings from 39% to 21% further emphasizes the escalating concern.

Ransomware attacks have become more severe, with high severity ratings increasing from 23% in 2023 to 38% in 2024. The increase in medium severity ratings from 23% to 30% indicates that more organizations are experiencing significant disruptions due to ransomware. The reduction in low severity ratings from 36% to 16% highlights the growing impact of these attacks.

Actionable Insights: Phishing attacks, password/identity-based attacks, and ransomware attacks have continued to be the top three IT security incidents by severity in 2023 as well as in 2024. These incidents underscore the ongoing challenges organizations face in protecting against sophisticated and evolving cyber threats. Strengthening user awareness, implementing robust authentication mechanisms, and enhancing ransomware defense strategies are critical steps in mitigating these high-severity security incidents.

Specifically, organizations should focus on enhancing their phishing awareness training and implementing advanced phishing detection tools. Implementing multi-factor authentication (MFA) and stronger identity management solutions is critical to mitigating the risk for password/identity-based attacks. Further, organizations should invest in robust backup solutions, regular security assessments, and incident response plans to effectively counter ransomware threats.

Impact of IT Security Incidents on Organizations

Top 3 security incidents	Ranking in 2024	Ranking in 2023
Disruption of business operations	1 ↔	1
Loss of critical data or sensitive data	2 ↔	2
Financial loss	3 ↔	3

Top 3 Impacts of Security Incidents: Disruption of business operations is identified as the most significant impact of IT security incidents, with 24% of respondents indicating a high impact. The equal percentage of medium impact (24%) further highlights the widespread concern about operational disruptions (See Figure 2).

The loss of critical or sensitive data is a close second, with 23% of respondents rating it as a high impact. An additional 26% report a medium impact, making data loss a major concern for more than half of the respondents (49%).

Financial loss is the third most reported impact, with 20% of respondents indicating it has a high impact on their organization. Combined with the 24% who report a medium impact, it is evident that financial implications of security incidents are a significant concern for 44% of respondents.

Trend and Analysis: There has been an increase in the perceived impact of IT security incidents on business operations disruption, with high and medium impact ratings rising from 20% to 24% and 15% to 24%, respectively. This shift indicates that organizations are increasingly recognizing the critical nature of operational disruptions caused by security breaches. The lower percentage of respondents reporting no impact (from 39% in 2023 to 21% in 2024) further underscores the growing concern over this issue.

The impact of data loss has significantly heightened, with high impact ratings increasing from 19% to 23% and medium impact ratings from 13% to 26%. The sharp decrease in the percentage of respondents reporting no impact (from 48% in 2023 to 29% in 2024) suggests that data breaches are becoming more frequent and severe. Organizations need to strengthen their data protection mechanisms and ensure robust response strategies are in place to mitigate these risks.

The financial impact of IT security incidents has grown, with high impact ratings rising from 15% to 20% and medium impact ratings from 15% to 24%. The significant decrease in respondents indicating no financial impact (50% in 2023 to 34% in 2024) points to an increased awareness and reporting of financial losses due to security breaches. This trend highlights the necessity for comprehensive financial risk management strategies and cyber insurance to mitigate the financial repercussions of such incidents.

Actionable Insights: The study findings highlight the critical need for robust security measures, effective incident response plans, and comprehensive risk management strategies to protect against and mitigate the severe consequences of security incidents. Comparing 2024 to 2023, there is a clear upward trend in the severity of the impacts of IT security incidents on organizations. Disruption of business operations, loss of critical or sensitive data, and financial loss have all seen notable increases in high and medium impact ratings. These trends emphasize the critical need for enhanced security measures, robust data protection, and comprehensive risk management strategies to address the escalating threats and their consequences.

Given that nearly half of the respondents (48%) report medium to high impact of security incidents on

Impact of IT Security Incidents

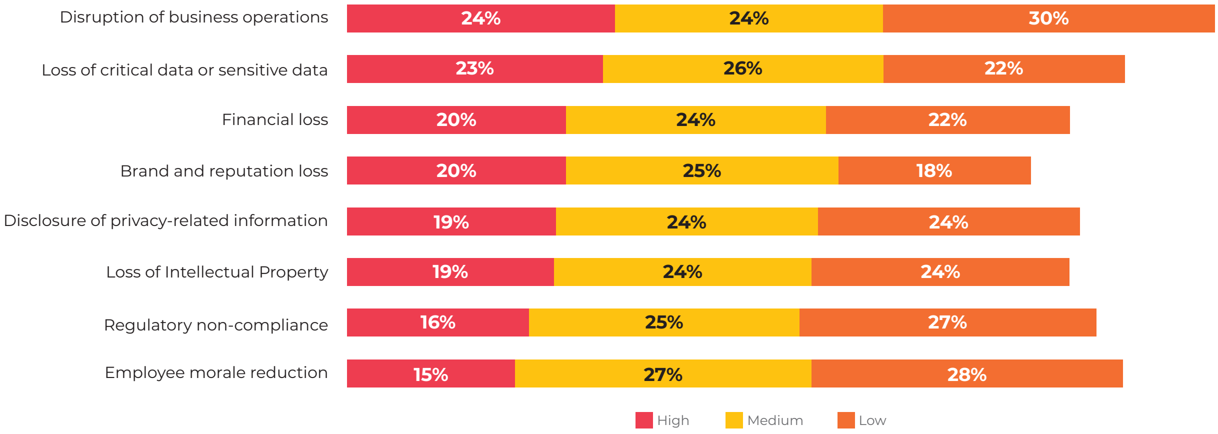


Figure 2: Disruption of business operations, and loss of critical data, financial and reputational losses highlight the need for comprehensive security strategies.

business operations, organizations need to prioritize business continuity planning and disaster recovery strategies to mitigate these disruptions.

To mitigate the loss of critical data, robust data protection measures, including encryption, regular backups, and stringent access controls to safeguard sensitive information and minimize the risk of data breaches, are of paramount importance.

Further, organizations must invest in comprehensive risk management frameworks and cyber insurance policies to mitigate potential financial losses from security breaches.

IT Security Incidents by Frequency

Top 3 security incidents	Ranking in 2024	Ranking in 2023
Human error/mistakes	1 ↔	1
Malware	2 ↑	3
Social engineering	3 ↓	2

Top 3 Security Incidents by Frequency: Human error remains the most frequent cause of IT security incidents, with 15% of respondents indicating it occurs often and 35% occasionally. This underscores the critical need for ongoing training and awareness programs to reduce mistakes and enhance the cybersecurity posture of organizations (See Figure 3).

Malware incidents are the second most frequent, with 11% of organizations experiencing them often and 37% occasionally. This suggests a persistent threat landscape where malware continues to be a significant concern.

Social engineering attacks are also a prevalent issue, with 11% of respondents reporting frequent occurrences and 27% occasional. These attacks exploit human psychology, making them difficult to defend against solely through technical means.

Trend and Analysis: There is a noticeable decrease in the frequency of human errors/mistakes reported as occurring often, from 22% in 2023 to 15% in 2024. The incidents categorized as rare increased from 24% to 41%, indicating improvements in mitigating human error but still showing a significant portion of occasional occurrences. Indeed, human error remains a substantial challenge.

The occurrence of malware incidents reported as often remained stable at 11%. However, there was an increase in occasional occurrences from 33% in 2023 to 37% in 2024, while rare and no occurrences showed a slight improvement. Malware continues to be a prevalent threat, with occasional incidents increasing. This suggests a persistent and evolving threat landscape, requiring organizations to invest in advanced malware detection and response solutions alongside continuous monitoring.

Social engineering incidents categorized as often slightly decreased from 12% to 11%, while occasional occurrences increased from 25% to 27%. Rare occurrences saw a significant rise from 33% to 42%, indicating some improvement in defenses against social engineering attacks. Social engineering remains a critical challenge, exploiting human vulnerabilities. The increase in rare occurrences suggests that awareness and training programs are somewhat effective, but organizations need to bolster these efforts with more sophisticated detection and response mechanisms.

Actionable Insights: Each of the top 3 incidents underscore different aspects of security—human factors, technical vulnerabilities, and psychological manipulation. Addressing these issues requires a multifaceted approach, including continuous education, robust technical defenses, and fostering a

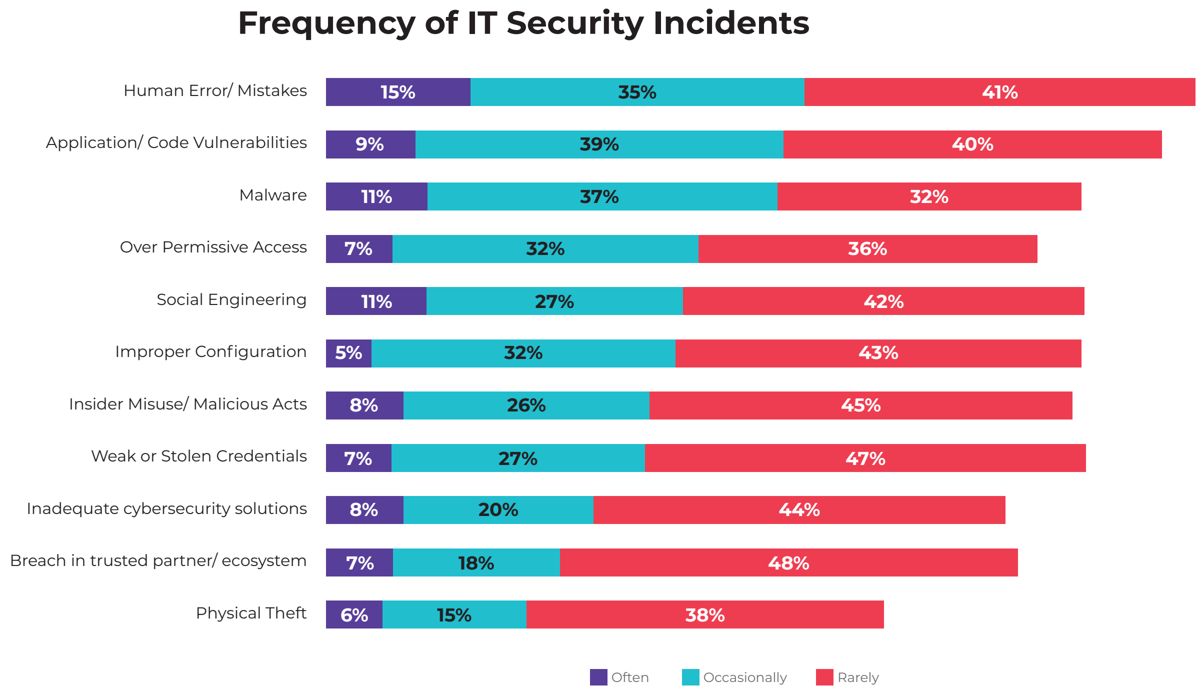


Figure 3: High frequencies of human errors and malware incidents underscore the importance of robust training and cybersecurity measures.

security-conscious organizational culture. By focusing on these areas, organizations can significantly reduce the frequency and impact of these common security incidents. Comparing 2023 and 2024, the data indicates slight improvements in the frequency of high-impact security incidents, but occasional occurrences remain significant.

Particularly, to mitigate human errors, organizations should continue to emphasize training and awareness programs to minimize the likelihood of mistakes.Automating processes and implementing more stringent checks can also help mitigate the risk of human error.

Strengthening endpoint protection, ensuring regular software updates, and deploying advanced threat detection mechanisms are essential measures to combat malware effectively.

Challenges Pertaining to Cloud Security in 2024

Top 3 challenges pertaining	Ranking in 2024	Ranking in 2023
Dependence on platform vendor	1 ↔	1
Integration of multiple cloud services	2 ↑	4
Lack of cloud security expertise	3 ↓	2

Comprehensive security awareness training, phishing simulations, and a culture of vigilance are crucial to minimizing the impact of social engineering tactics.

Top 3 Cloud Security Challenges: Dependence on platform vendors is identified as the most significant challenge, with 26% of respondents rating it as a high concern and another 35% calling it a medium concern. This high dependence can hinder flexibility and innovation, as organizations may find themselves restricted by the capabilities and policies of their vendors (See Figure 4).

Integration of multiple cloud services is another critical challenge, with 26% of respondents viewing it as highly important and a further 29% rating it as having medium importance. As businesses increasingly adopt multi-cloud environments, seamless integration becomes vital to ensure efficient operations and data flow.

A lack of cloud security expertise is a significant concern, with 24% rating it as highly important and a significant 33% considering it to be of medium importance. This challenge highlights the growing need for specialized skills and knowledge in cloud security as threats become more sophisticated.

Trend and Analysis: Dependence on platform vendors remains a top concern, though the percentage considering it to be highly important has decreased from 32% in 2023 to 26% in 2024. This shift indicates that organizations are possibly becoming more adept at managing vendor dependencies or diversifying their cloud service providers.Despite the decrease, the concern remains significant,

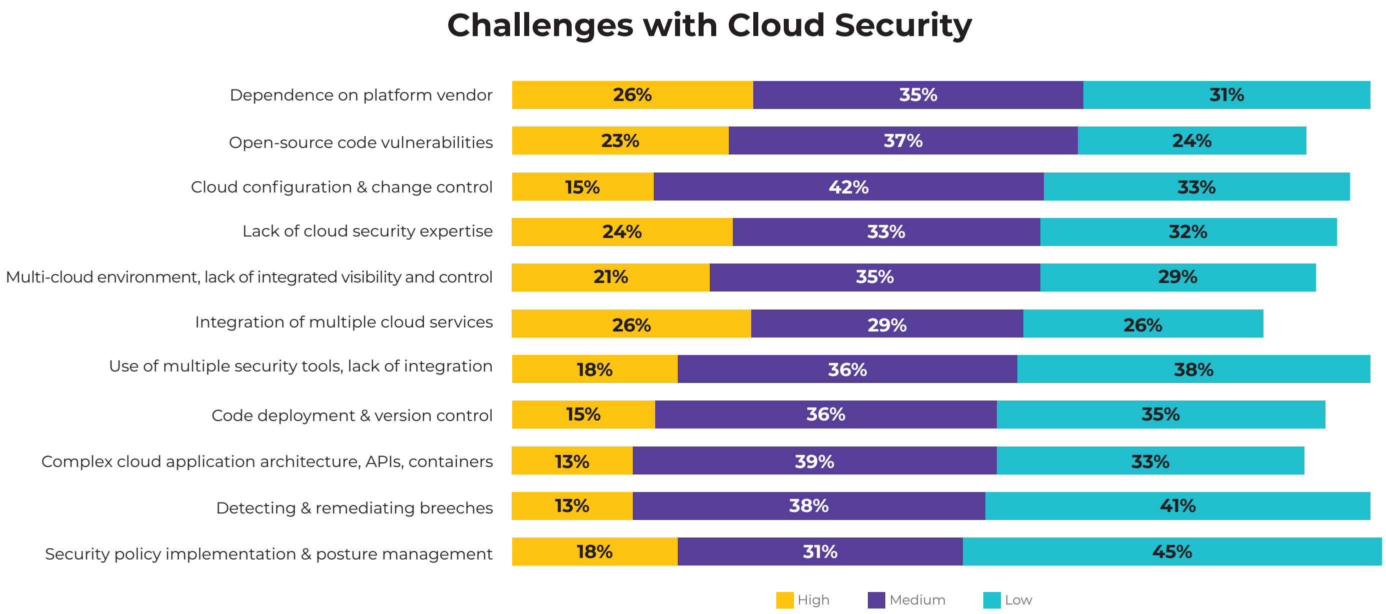

Challenges with Cloud Security

Figure 4: Dependence on platform vendors and integration of multiple cloud services pose challenges, which are compounded by lack of cloud security expertise and open-source vulnerabilities.

highlighting the importance of strategies to mitigate vendor lock-in.

The importance of integrating multiple cloud services has risen sharply, with 26% rating it as highly important in 2024 compared to 16% in 2023. This increase reflects the growing complexity and necessity of multi-cloud environments. This implies that organizations are increasingly recognizing the need for seamless integration of various cloud services to ensure smooth operations.

While the concern about the lack of cloud security expertise has remained relatively stable (25% in 2023 to 24% in 2024), there is a notable increase in those who find it medium important (33% in 2024 compared to 30% in 2023). The persistent challenge of lacking cloud security expertise underscores the need for continuous training and development.

Actionable Insights: By adopting multi-cloud strategies, investing in integration tools, and focusing on skill development, organizations can enhance their cloud security and operational efficiency.

To mitigate the challenge of depending on platform vendors, organizations should consider multi-cloud strategies, diversify their vendor base, and invest in internal capabilities to reduce reliance on a single platform. To improve the integration of multiple cloud services, organizations need to invest in robust integration tools and platforms, develop comprehensive integration strategies, and ensure their teams have the necessary skills to manage complex multi-cloud environments effectively.

To overcome the lack of cloud security expertise, organizations should focus on upskilling their current workforce, hiring experienced professionals, and investing in continuous learning and development programs to build a robust security posture.

State of Deployment of IT Security Processes and Operations

Top 3 IT security processes	Ranking in 2024	Ranking in 2023
Penetration testing	1 ↔	1
Security standards and frameworks	2 ↑	4
Security audits	3 ↓	2

Top 3 IT Security Processes by Deployment: Penetration testing leads the list with 64% of organizations having already implemented this security measure (See Figure 5). This high rate ofits implementation underscores the importance of regularly testing the security posture to identify and mitigate vulnerabilities. With an additional 23% working on implementing, it and 9% planning to do so within six months, penetration testing is recognized as a critical component of a robust security strategy.

Security standards and frameworks are implemented by 58% of organizations, highlighting the significance of adhering to established guidelines to ensure comprehensive security coverage. Another 26% currently working on it indicate ongoing efforts to standardize security practices, and the 14% planning to prioritize it within six months further emphasizes its importance. This structured approach helps organizations stay compliant and resilient against emerging threats.

Security audits, implemented by 56% of organizations, are crucial for assessing and improving security measures. The ongoing work by 28% and plans for 13% to prioritize audits within six months show a strong commitment to continuously reviewing and enhancing security practices. Regular audits help identify weaknesses and

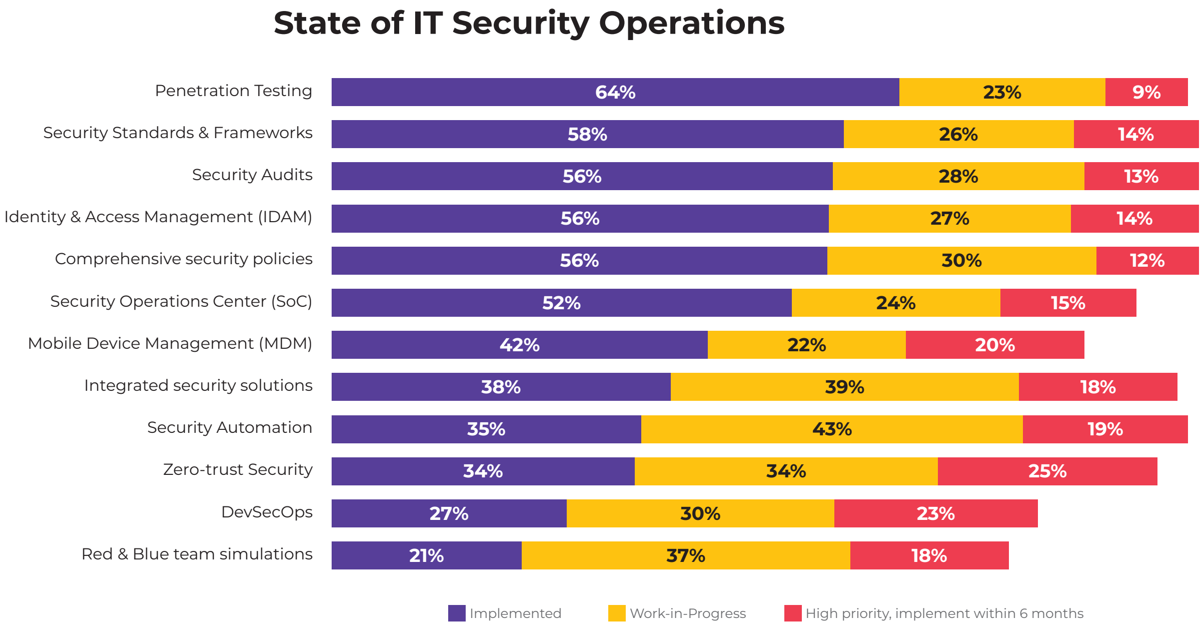


Figure 5: Prioritization of penetration testing and security standards, along with active implementation of security automation and comprehensive policies comprise a proactive approach to security.

ensure compliance with regulatory requirements, reinforcing overall security.

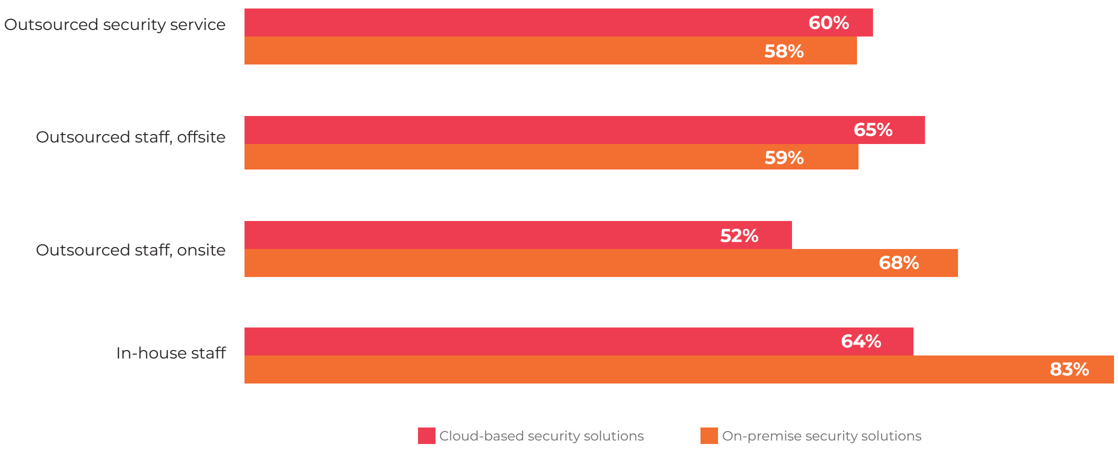
Trend and Analysis: Overall, the trend analysis for 2024 shows a stable or slightly increasing emphasis on key IT security processes and operations. Penetration testing remains a top priority, with implementation rates almost identical (65% in 2023 vs. 64% in 2024). The consistent priority placed on penetration testing reflects its critical role in identifying and mitigating vulnerabilities.

The implementation of security standards and frameworks increased from 51% in 2023 to 58% in 2024. This upward trend indicates a growing recognition of the importance of adhering to established security guidelines to ensure comprehensive protection and compliance.

Security audits have seen a slight decrease in implementation (from 57% in 2023 to 56% in 2024), but they remain a critical focus area. The minor decrease might reflect a shift toward integrating continuous monitoring solutions rather than periodic audits.

Actionable Insights: Penetration testing continues to be a critical security measure with high implementation rates in both 2023 and 2024. To maximize its effectiveness, organizations should ensure penetration tests are conducted regularly and not just as a one-time or annual activity. It may be a good idea to employ both internal teams and external third-party experts to conduct penetration tests. This dual approach ensures a comprehensive evaluation from different perspectives.

IT Security Management



Regarding security standards and frameworks, it is important to implement a culture of continuous improvement by regularly reviewing and updating security policies to align with new threats and regulatory requirements. This could include periodic audits and gap analyses.

Security audits are essential for identifying vulnerabilities and ensuring compliance. To enhance the effectiveness of these audits, organization should invest in automation tools that can streamline the audit process, making it more efficient and less resourceintensive. They should ensure that audit reports are actionable, with clear recommendations and timelines for remediation. This helps in translating audit findings into tangible improvements in the security posture.

On-prem and Cloud-based Deployment and Management

A Balanced Mix: In 2024, the deployment and management of IT security solutions exhibit a strong reliance on in-house staff for on-premise security, with 83% of organizations utilizing internal resources. This indicates a significant emphasis on leveraging internal expertise and control over on-premise security measures. Conversely, cloud-based security solutions also see considerable involvement of in-house staff at 64%, highlighting a balanced approach to managing cloud security within the organization. Outsourced staff, both onsite and offsite, play a crucial role in on-premise security, with 68% and 59% engagement respectively. For cloud-based security, outsourced staff offsite (65%) slightly surpasses outsourced security services (60%). These distributions suggest a strategic blend of in-house and outsourced capabilities to manage the complexities and demands of both on-premise and cloud security environments effectively.

Trend and Analysis: Comparing 2024 survey results with those of 2023, there is a notable increase in the utilization of in-house staff for on-premise security solutions, rising from 75% to 83%. This indicates a growing preference for leveraging internal expertise to manage on-premise security challenges.

For cloud-based security, in-house staff engagement remains relatively stable, with a slight increase from 63% to 64%. Interestingly, there is a decrease in the reliance on outsourced security services for cloud-based solutions, dropping from 70% in 2023 to 60% in 2024. Similarly, the use of outsourced staff, offsite, for cloud-based security solutions has decreased from 74% to 65%.

These shifts suggest a trend toward internalizing cloud security management and reducing dependence on external service providers. The slight increase in the use of outsourced staff, onsite, for on-premise solutions (from 62% to 68%) and for cloud-based solutions (from 63% to 52%) indicates a strategic adjustment in how organizations are deploying their security resources.

Actionable Insights: Organizations should consider the growing trend toward internalizing IT security management, particularly for on-premise solutions. Investing in building and retaining in-house expertise can provide greater control and responsiveness to security threats.

For cloud-based security, while there is a move toward reducing reliance on external service providers, maintaining a balance by leveraging both in-house and outsourced capabilities can ensure comprehensive coverage and expertise. Organizations should continue to invest in training and development programs for their internal teams to handle advanced security challenges.

Additionally, reviewing and optimizing the use of outsourced staff, both onsite and offsite, can help in addressing specific security needs without over-reliance on any single resource type. Strategic partnerships with security service providers can also be beneficial in filling expertise gaps and providing scalable solutions as security demands evolve.

Key Challenges in Achieving IT Security Objectives

Top 3 challenges in achieving	Ranking in 2024	Ranking in 2023
Cost and effort to manage security solutions	1 ↑	3
Evolving threat environment	2 ↓	1
Alignment of security and business goals	3 ↑	5

Top 3 Challenges in Achieving IT Security Objectives: Managing security solutions due to the high cost and effort involved emerged as the top challenge in this year's survey. It was rated high as a challenge by 44% of the respondents; medium by 39%; and low by just 12%, considering that financial burden of implementing, maintaining, and upgrading security measures can strain IT budgets, particularly as the complexity and sophistication of threats increase (See Figure 6).

The rapidly evolving threat landscape poses a constant challenge for IT security teams. It was rated high by 43% respondents; medium by 44% respondents; and low by only 9% respondents, given that new vulnerabilities and attack vectors emerge regularly, requiring continuous adaptation and vigilance.

Security measures must support and not hinder business operations, requiring a delicate balance between protection and productivity. As such, aligning IT security initiatives with overall business goals is crucial but often challenging. This challenge was considered high by 41% survey respondents this year; medium by 38%; and low by 16% of the respondents.

Trend and Analysis: The "high" concern regarding the cost and effort to manage security solutions

> "The stringent provisions of the DPDP Act underscore the need for personal accountability in the event of anomalies. Enforcing these provisions will foster a stronger security culture within organizations."

Ananth Subramanian
Executive VP & Head - IT,
Kotak Mahindra Asset
Management Company

has increased from 39% in 2023 to 44% in 2024. There is a slight decrease in the 'medium'rating and a decrease in the 'low'rating. The increasing concern suggests that organizations are finding it increasingly challenging to manage the costs and efforts associated with maintaining robust security measures. This could be due to the rising complexity of threats and the need for more sophisticated solutions.

The concern about the evolving threat environment has slightly decreased from 47% in 2023 to 43% in 2024 for the 'high'rating. There is an increase in the 'medium'rating and a decrease in the 'low'rating. The slight decrease in the 'high' concern suggests that while the threat landscape remains a significant issue, organizations might be feeling more prepared or have adjusted their strategies to handle evolving threats.

The alignment of security and business goals has increased significantly from 34% in 2023 to 41% in 2024 for the 'high' category. There is a decrease in the 'medium' category and a slight decrease in the 'low' category. The increasing concern highlights the growing recognition of the importance of aligning security strategies with overall business objectives. This could be driven by the need to demonstrate the value of security investments to executive leadership.

Actionable Insights: The trend analysis reveals a growing concern over the cost and effort required to manage security solutions and the alignment of security with business goals. While the concern over the evolving threat environment has slightly decreased, it remains a significant issue.

When it comes to managing security solution cost effectively, the first step could be to prioritize spending on essential security solutions and seek cost-effective alternatives. It may also be worth leveraging automation to reduce manual effort and streamline security processes. Also, by engaging managed security service providers (MSSPs) to handle routine security tasks, internal teams can focus on strategic initiatives.

In view of the evolving threat environment, it would be a must to implement advanced threat detection and monitoring systems to identify and respond to threats in realtime.Investing in threat intelligence services to stay informed about emerging threats and vulnerabilities could be quite pertinent. And of course, to conduct ongoing security training for

Measures Taken to Address the Skill Gaps in IT Security

Top 3 measures taken to address skill gaps	Ranking in 2024	Ranking in 2023
Providing training for employees	1 ↑	2
Re-training technical staff	2 ↑	3
Partnering with experts/ consultants	3 ↓	2

employees to recognize and respond to new types of attacks is a no brainer.

In order to achieve better alignment between security and business goals, it would be crucial to integrate security planning with business strategy development to ensure that security initiatives support business goals. In this regard, it will be important to engage top management in security discussions to ensure their support and understanding of the importance of security investments. This can be done by developing and presenting clear metrics to demonstrate the value of security investments in terms of business outcomes, such as risk reduction and compliance.

Top 3 Measures on Skill Gaps: The majority of organizations are already focusing on providing training for employees (69%), while 20% are planning to do it within six months and 7% are planning withing 12 months. This measure shows a high level of immediate engagement, indicating that organizations recognize the importance of continuous learning and skill enhancement for their existing workforce. The low percentage of those planning or having no requirement (4%) suggests that this is a critical ongoing activity.

Re-training technical staff is another key measure, with a significant portion of organizations actively involved (64%), followed by those planning within six months (21%) and those planning within 12 months (8%). This measure ensures that technical staff remain updated with the latest security practices and technologies. The considerable percentage planning re-training within the next 6 months shows a proactive approach toward maintaining a skilled technical workforce (See Figure 7).

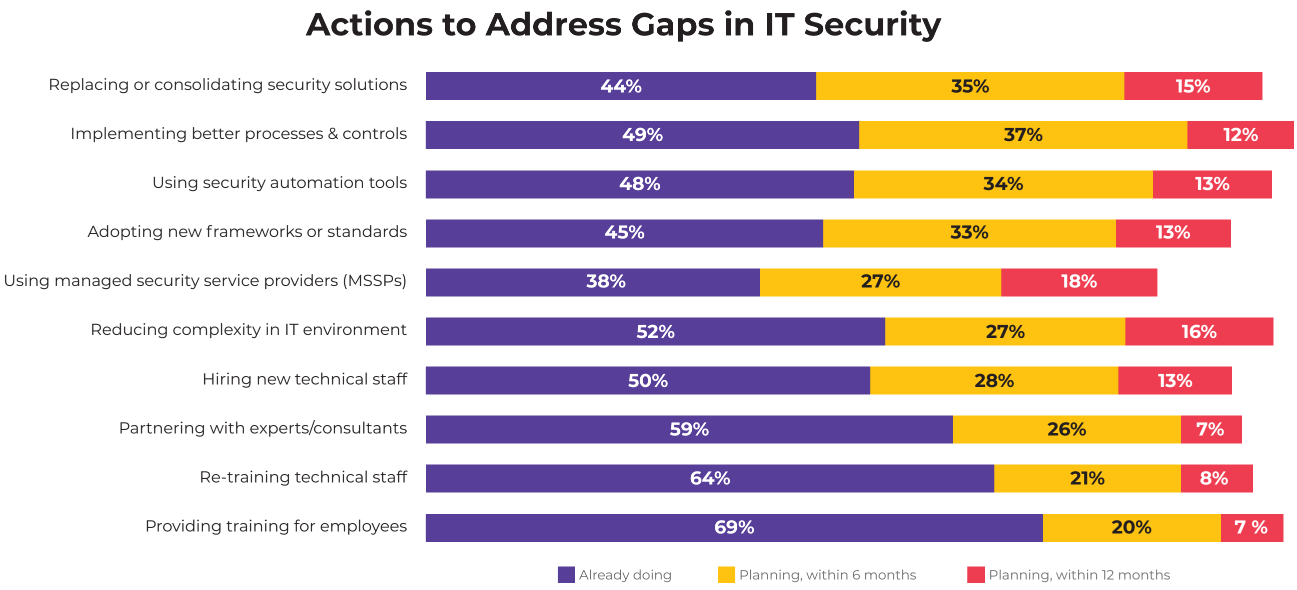


Figure 7: Training and re-training the staff, while partnering with experts and reducing IT complexity help bridge skill gaps, ensuring a robust security posture.

> "As cyber attacks grow more sophisticated, AI's predictive capabilities become crucial for preempting threats. Combining AI with human insight strengthens cybersecurity defenses significantly."

Sunil Gandhi
CIO - Treasury Technology,
Deutsche Bank

Partnering with experts and consultants is a prevalent measure, with many organizations already engaging external expertise (59%). This approach helps bring in specialized knowledge and experience that may not be available internally. With 26% planning within six months and another 7% planning within 12 months, a strong future intent to continue or start these partnerships is indicated.

Trend and Analysis: Providing training for employees remains the top measure in both years. There is a slight decrease in organizations already doing this (from 75% in 2023 to 69% in 2024), but a higher percentage of organizations are planning to implement training within the next six months. The focus on training reflects a continuous need to upskill employees to keep pace with evolving security threats. The increase in short-term planning indicates an urgency to address current skill gaps. The measure of retraining technical staff shows stability in the already implemented (64%) and six-month planning (21%) categories. These figures remain consistent between 2023 and 2024. This consistency highlights the ongoing need to refresh the technical skills of the IT workforce regularly. The similar percentages in both years suggest that organizations recognize the continuous need for technical re-training to address new security challenges.

There is a decrease in the percentage of organizations already partnering with experts or consultants from 70% in 2023 to 59% in 2024. However, there is an increase in those planning to do so within the next six months (from 19% in 2023 to 26% in 2024) as well as in the next 12 months (from 5% to 7%).The decrease in immediate partnerships could be due to a higher level of internal capability development. The increase in short-term planning indicates that organizations still see value in external expertise but might be focusing on internal resources first.

Actionable Insights: The analysis highlights a strong focus on internal training and upskilling, as well as leveraging external expertise to address IT security skill gaps. Organizations should continue to invest in these areas to maintain a robust security posture. By providing regular training, re-training technical staff, and partnering with experts, companies can effectively bridge the skill gaps and enhance their overall security capabilities.

Develop comprehensive training programs that cover current and emerging security threats. Leverage online learning platforms and in-house training sessions. Measure the effectiveness of training programs through regular assessments and feedback. Identify skill gaps through regular performance reviews and skill assessments.Create tailored re-training programs focused on specific technical skills required by the organization. Encourage continuous professional development through certifications and advanced training courses. Identify areas where external expertise can add the most value, such as threat intelligence, risk management, or compliance. Establish long-term partnerships with reputable security consultants and firms. Ensure knowledge transfer from external experts to internal teams to build in-house capabilities over time.

To conclude, the analysis of IT security challenges and measures reveals critical areas requiring CIOs'and CISOs' attention. The evolving threat landscape, alignment of security and business goals, and skill gaps highlight the need for strategic focus. Tech leaders should prioritize investing in training, adopting comprehensive security frameworks, and leveraging advanced technologies. Proactive measures such as regular penetration testing, security audits, and embracing automation can fortify defenses. Ensuring top management support and fostering a security-conscious culture are essential for robust IT security. By addressing these key areas, organizations can enhance resilience and achieve their security objectives in an increasingly complex digital environment.

AI and IT Security

AI's integration into IT security is advancing rapidly, with several areas already benefiting significantly. Currently, AI is highly influential in IT and network asset management (54%) and monitoring and vulnerability management (48%), showcasing its critical role in maintaining security infrastructure. Other key areas like incident response and remediation (47%) and behavioral analysis and threat hunting (44%) also see substantial AI impact (See Figure 8).

Over the next 12 to 18 months, substantial growth is expected, particularly in identity and authentication management (56%) and governance and risk management (49%). This indicates a shift towards more sophisticated, AI-driven security protocols. The projection for the next 18 to 24 months and beyond suggests a slower but steady increase in AI adoption, with specific areas like incident response and governance gradually catching up. Despite the advancements, some aspects like monitoring and vulnerability management will continue to develop beyond 24 months, reflecting ongoing enhancements in AI capabilities. Overall, the trajectory shows a balanced blend of immediate AI implementation and long-term strategic planning to bolster IT security.

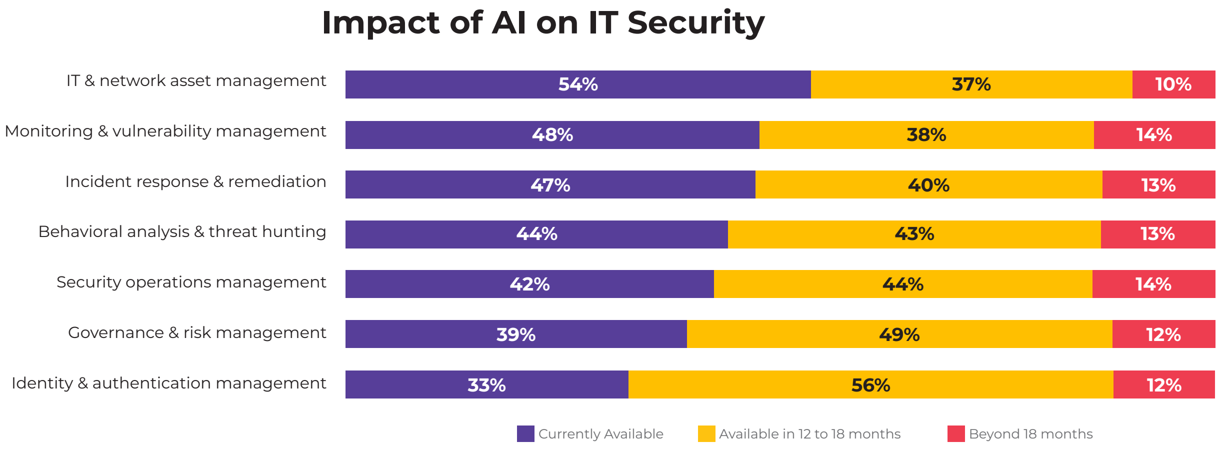


Figure 8: AI is revolutionizing IT security, enhancing asset management, threat hunting, and incident response. Key areas show significant AI adoption within 12 to 18 months.

Key Contributors

Giridhar has more than 30 years of experience in areas spanning media, consulting and digital technology, working with leading B2B and B2C media organizations across the Asia-Pacific region. He has been actively involved with professional communities in developing content-driven engagements and platforms, and people recognition programs.

R. Giridhar
Group Editor
9.9 Group

Deepak is an analyst, columnist, and speaker with more than 25 years of experience in various market research, advisory, and editorial roles spanning domains such as IT, telecom, and sustainability. His focus areas include market and trend analysis, strategic communications, and internal and external sales enablement.

Deepak Kumar
Founder Analyst & Chief Research Officer
BM Nxt

With over 17 years of experience in research, consulting, media, and communication, Jatinder Singh currently serves as the Executive Editor at CIO&Leader. He is responsible for shaping the editorial strategy and direction of the publication. He specializes in writing about cutting-edge topics such as analytics, artificial intelligence, cloud computing, the Metaverse, and cybersecurity.

Jatinder Singh
Executive Editor - CIO&Leader
9.9 Group

Praneeta is a Correspondent with CIO&Leader. She is an experienced content writer and editor with expertise in B2B and print media. In her current role, she covers trends and developments in Artificial Intelligence, IoT, Cloud, Data and analytics, and Cybersecurity. She believes in the power of storytelling and shaping the next generation of askers.

Praneeta
Correspondent-CIO&Leader
9.9 Group

25th ANNIVERSARY CIO&LEADER
TRACK TECHNOLOGY • BUILD BUSINESS • SHAPE SELF

CIO&Leader is India's leading platform for enterprise technology leaders and decision-makers. It serves as a catalyst for the exchange of well-informed perspectives and insights, and fosters discussions on cutting-edge trends, technology implementations and use cases, IT business strategies, leadership, and innovation between CIOs and other key stakeholders.

bmnxt
business & market advisory

BM Nxt specializes in meeting research-based information, communication, and marketing needs of decision-makers and planners in the technology sector. It serves both suppliers and users of technology products and services by providing comprehensive insights and strategies that drive informed decisions and effective planning.

9.9 GROUP