CII-TATA COMMUNICATIONS CENTRE FOR DIGITAL TRANSFORMATION

protiviti®
Global Business Consulting

CII
Confederation of Indian Industry

STATE OF DATA PRIVACY IN INDIA

SURVEY REPORT 2024

CONTENTS

Foreword

As India advances in its digital journey, the protection of personal data becomes increasingly important. The proliferation of digital services, expansion of internet connectivity, and growing adoption of technologies like AI and IoT have all contributed to a massive increase in data generation.

With the introduction of the Digital Personal Data Protection Act, 2023, India has taken significant strides towards establishing a robust data privacy framework. The law aims to protect individual privacy while ensuring that the data economy can thrive. Key aspects include the rights of data principals (individuals), obligations of data fiduciaries (entities processing data), and penalties for non-compliance. The act reflects India's commitment to balancing the benefits of digital innovation with the need to protect personal data.

This evolving legal landscape is crucial not only for safeguarding personal information but also for fostering trust in digital services, which is essential for the continued growth of India's digital economy.

This report on "State of Data Privacy in India" highlights the findings of a joint survey conducted with Protiviti Global, focusing on important aspects of data privacy. This report provides a comprehensive overview of the current state of data privacy in India, based on one of the first detailed studies of its kind conducted across various organizations.

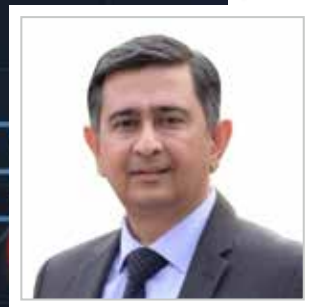
The survey aimed to encapsulate the present landscape of data privacy practices, challenges and perceptions within Indian organizations.

The report stands as an invaluable resource for stakeholders — policymakers, researchers, industry leaders, and civil society organizations—committed to shaping India's digital future.

CII has been a proponent of good governance practices and continues to focus on driving various initiatives with an aim to promoting these among Indian industry. CII considers compliance with applicable laws and regulations of the country as an imperative for all business entities. CII also encourages its members to focus on long-term value creation by adopting sound governance practices which ensure the continued success of businesses.

I express my sincere appreciation to the contributors of the report for their dedicated efforts to distil significant insights into this report. I believe this publication will enable industry and all stakeholders to take proactive steps and informed decisions in terms of building a privacy program within their organizations.

Chandrajit Banerjee
Director General
Confederation of Indian Industry (CII)



Preface

In an era where data has emerged as the new oil, its protection is paramount to safeguarding the rights and freedom of individuals. The rapid digital transformation across sectors has led to an unprecedented generation and utilization of personal data. While this has unlocked immense potential for innovation and growth, it has also heightened the risks associated with data breaches, privacy violations, and unauthorized exploitation of personal information.

India, with its vast and diverse population, is at the forefront of this digital revolution. The need for robust data protection mechanisms is more critical than ever, as the country embraces the benefits of digital technologies across its socio-economic fabric. The Digital Personal Data Protection framework in India represents a significant stride towards ensuring that the digital rights of its citizens are preserved, while ensuring a secure and transparent environment for data processing activities.

CII Tata Communications Centre for Digital Transformation had partnered with Protiviti Global last year to create awareness through several roundtables on data privacy amongst Industry and also undertook a Survey to seek feedback on the State of Data Privacy in India.

Our roundtables witnessed eminent CIOs/CDOs/ Privacy officers deliberate on pertinent points related to data privacy regulations for businesses operating in India, as they would need to undergo substantial changes to align their data processing practices with the new requirements. The Act emphasizes on data localization and cross-border data transfers which may lead to increased investments in data infrastructure within the country, as companies will have to store and process Indian users' personal data within India's borders. This could create opportunities for data center providers and technology companies specializing in data security and privacy compliance.

Some of the findings of our survey report reveal as under:

- 56% of Industry is confident about the privacy related initiatives of GOI and the DPDP Act.
- 52% have experienced a privacy breach in the last 5 years.
- 63% have fully documented privacy policy and procedures
- 24% feel prepared to manage privacy concerns associated with Emerging Technologies

The findings of the Survey reveal that the journey toward a secure digital future is a collective responsibility, and it begins with a comprehensive understanding of the principles and practices that underpin data protection in the modern age.

As we present this report and delve into the nuances of the Digital Personal Data Protection framework, it is crucial to recognize that the success of this endeavor lies in the collaborative efforts of government, industry, and civil society. Together, we can build a digital ecosystem that not only drives economic growth but also respects and upholds the privacy rights of every individual.

Sumeet Walia
Chairman - CII – Tata Communications Centre for Digital Transformation (CDT) &
Executive Vice President & Chief Sales and Marketing Officer, Tata Communications Ltd

Introduction

The landscape of data privacy in India is experiencing a profound transformation as digital technology becomes increasingly prevalent and accessible. With rapid digitization, new opportunities and significant challenges in safeguarding data have emerged. In this context, Protiviti is proud to partner with organizations to assess their privacy needs, implement compliance measures, and respond to both new and evolving regulations.

We are pleased to present this comprehensive report on the State of Data Privacy In India, developed in collaboration with the Confederation of Indian Industry (CII). This report represents a significant milestone in understanding the current state of data privacy in India, as organizations across the country navigate an increasingly complex regulatory landscape.

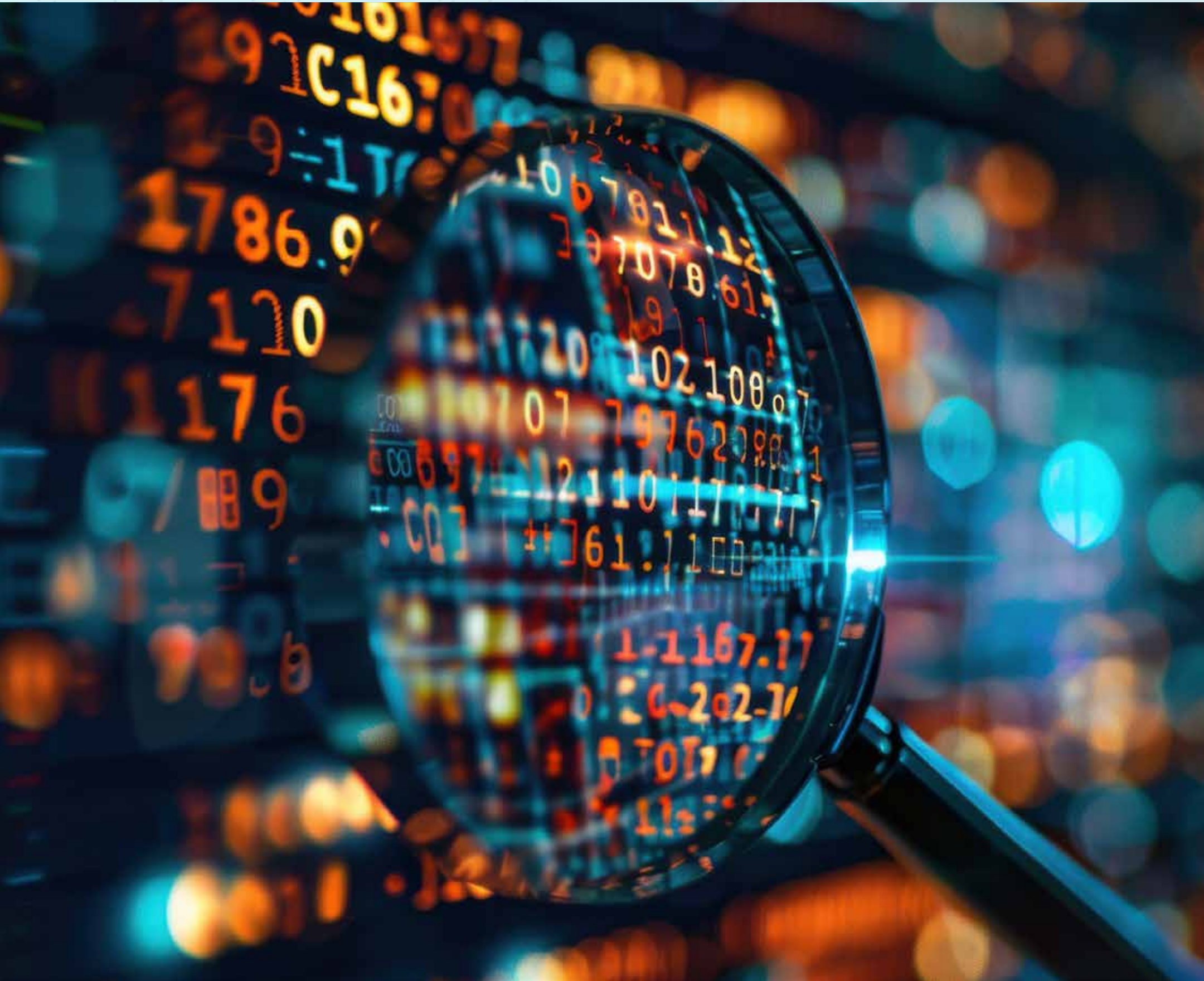
The findings of this survey are crucial for Indian businesses as they adapt to the evolving requirements of the Digital Personal Data Protection (DPDP) Act, 2023 and other emerging data privacy regulations. The insights gathered provide a clear picture of the challenges and opportunities that lie ahead, offering actionable guidance to help organizations strengthen their data protection strategies, ensure compliance, and build trust with their stakeholders.

Our survey encompassed a wide range of participants from diverse industries and roles, including senior management, middle management, and operational staff. The report delves into key aspects of data privacy, including perception and awareness, key drivers impacting privacy, privacy governance, privacy program maturity, and the adoption of technology.

We extend our deep appreciation to CII for their invaluable partnership in this initiative. Their support has been instrumental in reaching a broad spectrum of industries, ensuring that this report accurately reflects the diverse perspectives and realities of Indian businesses. Together, we are committed to fostering a robust and secure digital ecosystem in India, where data privacy is not just a regulatory requirement but a strategic imperative.

We trust that this report will serve as a vital resource for industry leaders, policymakers, and all stakeholders invested in the future of data privacy in India. We encourage you to engage with the findings, consider the recommendations, and join us in our ongoing efforts to shape a secure and compliant digital landscape.

Sandeep Gupta
Managing Director
Protiviti Member Firm for India



Executive Summary

The Digital Personal Data Protection Act, 2023 has been a pivotal initiative by the government to enhance privacy protections in the digital age.

Confederation of Indian Industry (CII) and Protiviti partnered on conducting a comprehensive survey on the preparedness of Indian industries for data privacy and the Digital Personal Data Protection (DPDP) Act. This collaboration was aimed at assessing compliance readiness, identify challenges, and highlight best practices across sectors. The results offer strategic insights and guidance to help businesses navigate the evolving data privacy landscape and align with the DPDP Act.

Our survey aimed to capture the views of executives on the extent to which the measures, as outlined in the Act, have addressed significant privacy concerns and challenges. By analyzing the responses, we sought to gain insights into the overall effectiveness of the Act in safeguarding personal data and privacy rights. This involved examining broader aspects around the state of Data Privacy across organization of India, highlighting the following areas:

- Perception and Awareness
- Key Drivers impacting Privacy
- Privacy Governance
- Privacy Program Maturity
- Embracing Technology

The respondents spanned a diverse range of industries, including BFSI, Information Technology, Hospitality, Manufacturing, Media & Telecom and others, ranging from mid-level to executive management positions.

The findings of this survey will contribute to ongoing discussions on data privacy and inform future policy decisions, ensuring the legislative framework remains robust and adaptive to evolving technological and societal changes.

A summary of the survey results along with the comprehensive analysis is detailed in the subsequent pages.

PERCEPTION AND AWARENESS

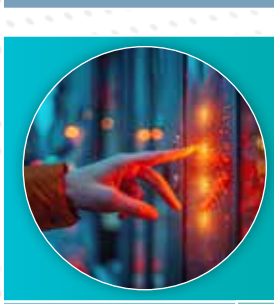
56%
have confidence on Government of India's privacy focused initiatives such as DPDPA

52%
have experienced a privacy breach in the last 5 years

Perception on Transparency in Data Handling Process

82%
perceive that companies are not transparent or partially transparent

61%
Companies take part in practices that are deemed problematic from privacy perspective



KEY DRIVERS IMPACTING PRIVACY

51%
are establishing privacy programs to meet mounting regulatory and contractual demands

Major Privacy Concerns

1. Consent Management & Data Principal Access Request
2. Visibility of Personal data
3. Data Retention & Disposal
4. Data Breaches & Cross-Border Transfer

Key Privacy initiatives

- Improving Overall Privacy Governance, Risk and Compliance
- Establishing a Data Protection Office
- Implementation of solutions for Consent Management and Data Principal Access Rights

PRIVACY GOVERNANCE

Investments allocated for privacy program

High-Revenue Organizations	Lower-Revenue Organizations
37% invest over ₹ 5 crore	**4%** invest over ₹ 5 crore
5% have no budget allocated	**26%** have no budget allocated

Responsibility for Governing and managing Data Privacy Programs

High-Revenue Organizations

44% rely on IT-IS team

39% have dedicated Data Privacy Office

Lower-Revenue Organizations

37% rely on IT-IS team

33% depend on Legal/ Compliance

Dedicated Privacy Focused Steering Committee has been established

High-Revenue Organizations	Lower-Revenue Organizations
43%	**22%**

63%
have fully documented privacy policies and procedures

Top privacy assurance mechanism

1. Privacy Assessments
2. Reliance on standards such as ISO27001, ISO27701
3. Independent third party reviews

High-Revenue Organizations: Above ₹ 1000 Crore Revenue
Lower-Revenue Organizations: Below ₹ 1000 Crore Revenue

PRIVACY PROGRAM MATURITY

Organizational Maturity in Privacy Programs

26% privacy program is implemented

42% privacy program is defined

32% privacy program is not established or in planning stage

Data Retention and Disposal Processes

48% have their data retention & disposal process fully defined and implemented

Privacy Risk from Third Parties

38% address privacy concerns with third parties through both contractual agreements and risk assessments

Preparedness or Incident Response

44% remain at lower maturity levels, with non-proactive approaches for incident response processes

Privacy Focused Skilled Resources

	High-Revenue Organizations	Lower-Revenue Organizations
In house privacy skill	58%	30%
Support from third party organization	36%	41%
Resourcing not planned	6%	29%

Managing cross border transfer

62% Through data localization and legal agreements

20% Yet to define appropriate measures

Readiness for Managing Privacy in Emerging Technologies

24% feel prepared to manage privacy concerns associated with Emerging Technologies

EMBRACING TECHNOLOGY

Top Automation Initiatives in Privacy

- Privacy Rights and Consent Management
- PIA/DPIA/TPRM
- Data Governance (Data discovery / inventory)

Enhancing Privacy Through Digital Identity

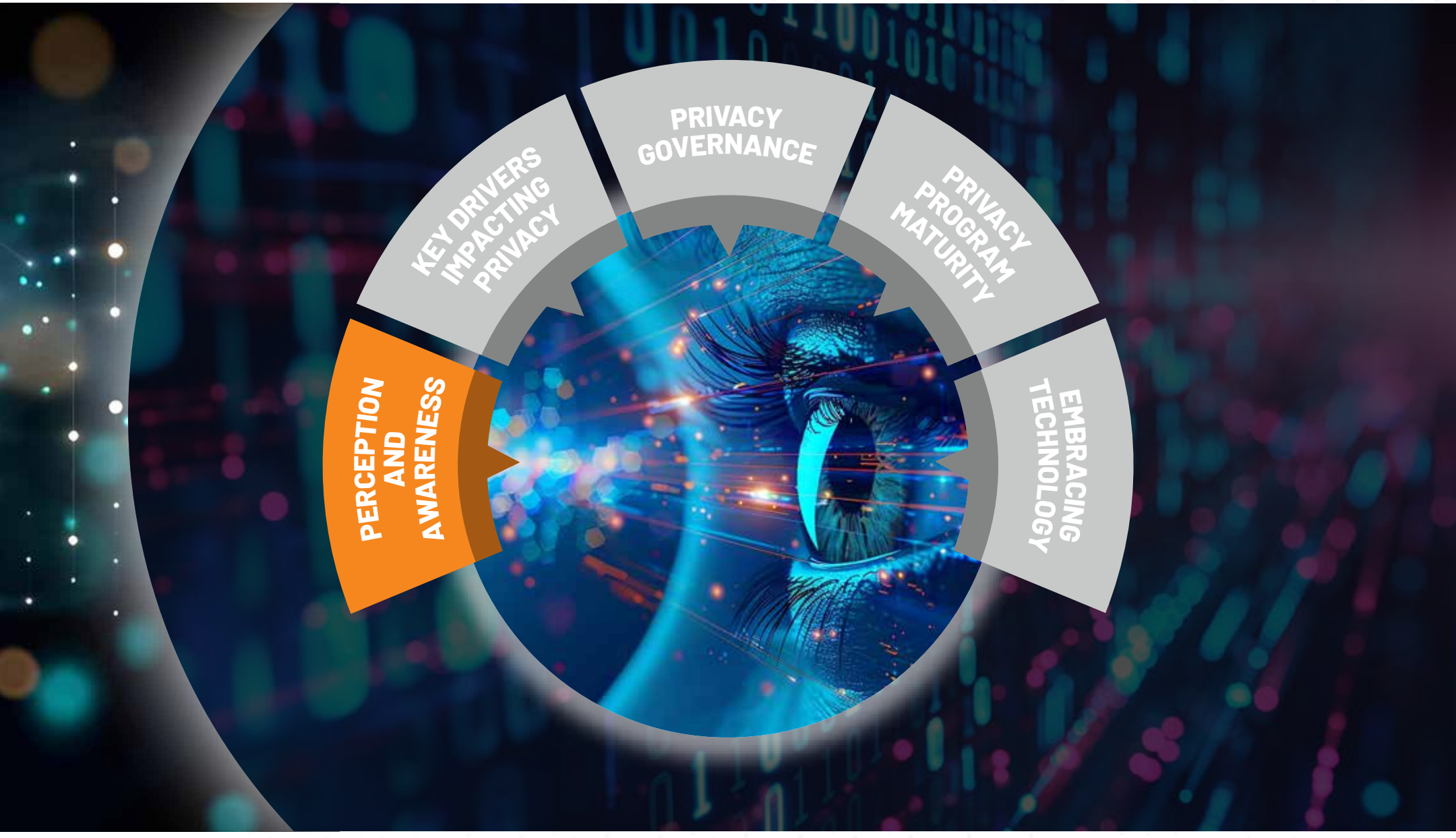
39% Manage privilege access via PAM

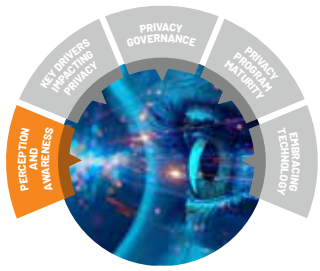
27% utilize PAM for privilege users & enterprise IAM for managing end users

22% Not planned or in planning stages

High-Revenue Organizations: Above ₹ 1000 Crore Revenue
Lower-Revenue Organizations: Below ₹ 1000 Crore Revenue

protiviti®


KEY DRIVERS IMPACTING PRIVACY
PRIVACY GOVERNANCE
PRIVACY PROGRAM MATURITY
EMBRACING TECHNOLOGY
PERCEPTION AND AWARENESS



Perception and Awareness

Understanding Perceptions of the DPDP Act

The survey responses reveal a generally positive perception towards the Digital Personal Data Protection Act 2023, with most respondents endorsing its effectiveness. This confidence likely arises from the Act's extensive coverage, its orientation for businesses, and effective communication of its benefits.

However, a notable portion of respondents exhibit only partial support for the Act or express skepticism about its effectiveness.

This points towards the critical importance of clear and transparent communication, along with meticulous and strategic implementation of regulations, to address privacy challenges effectively. The disparity in viewpoints reflects the complex nature of privacy issues in the country and the legislative challenge of creating laws that meet the diverse needs and expectations of stakeholders.

Do you feel that the government's initiatives on protecting privacy such as the DPDPA 2023 would address key privacy concerns and challenges?

56% Demonstrated confidence in the efficacy of the Digital Personal Data Protection Act 2023

30% Demonstrated partial confidence in the Act's capability to address privacy concerns

14% Expressed clear skepticism or admitted uncertainty regarding the effectiveness of the Act

The concerns and uncertainties voiced by some participants highlights a broader issue regarding the potentially raw privacy culture in India.

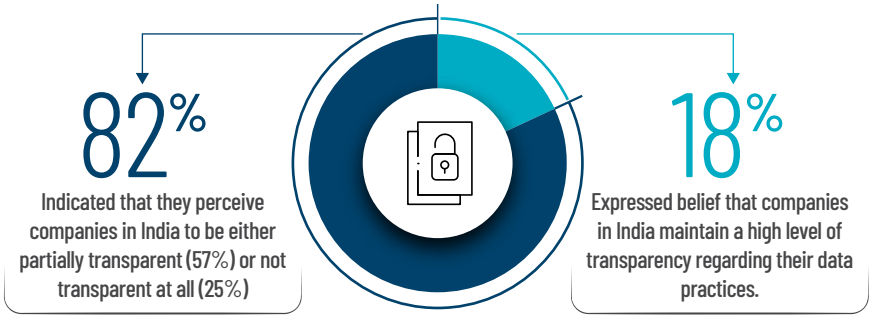
Transparent Data Handling Practices For Building Trust

Navigating the complexities of data collection requires a deep dive into how trust, accountability, and ethical practices are perceived and enacted within corporations. Understanding the nuances of data handling practices is essential for assessing trust and accountability among organizations from the perspective of privacy.

In this survey, we aimed to explore current data collection and processing practices among companies to uncover ' views on trust and accountability in data privacy.

We sought responses on, how transparent companies in India are perceived to be regarding their use, processing, and sharing of personal data and whether they are believed to engage in any concerning practices such as excessive data collection or processing/secondary processing without consent.

How transparent do you feel are the companies in India regarding the use, processing and sharing of personal data?



Majority of respondents experience a sense of uncertainty regarding the handling of their personal data by companies. Despite companies' efforts to reassure users of their commitment to transparency, skepticism persists among a significant portion of the population.

Some recent instances exacerbated this lack of confidence, triggering widespread criticism and casting doubts on the company's transparency and intentions in data handling.

Most organizations (82%) are yet to establish transparent practices for the use, processing, and sharing of personal data within their systems.

DPDPA, 2023 REQUIREMENT

Data fiduciaries are required to provide a detailed notice to the data principal, clearly stating the itemized list of personal data they intend to collect and the purpose for its processing.

Similarly a majority remains uncertain about the practices being followed while processing personal data across their ecosystem. The skepticism may be partly due to public incidents on privacy breaches which had undermined public trust.

Do you believe that corporates follow practices such as excessive data collection, secondary processing without consent etc. Which may be deemed as problematic?

Majority of participants felt that companies take part in activities that can be deemed problematic

61%

Limited number of respondents trust that they're not involved in problematic data practices.

12%

27%

Participants either were not sure if companies follow these practices.

A significant majority (61%) signals a red flag, calling for stricter regulatory oversight and corporate accountability.

Further, an alarmingly low (12%) confidence levels calls for a pressing need for companies to fortify trust through transparency and robust ethical standards.

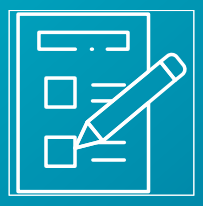
The response echoes a pivotal message of the necessity for Indian Companies to abide DPDPA 2023 in order to prevent data mishandling, protect user privacy, and promote responsible data management practices across ecosystem creating transparency.

Stringent data privacy controls and informed public dialogue about corporate data practices, will be entrusted as a strategic shift towards establishing robust rules for compliance and trust-building in the digital age.

protiviti

Data Breaches and Unauthorized Access to Personal Information

Data breaches have always been a critical concern for organizations globally. In recent years, both the frequency and severity of these breaches have increased, driven by cybercriminals who continuously develop sophisticated methods to exploit vulnerabilities in organizational systems. Malware based cyberattacks, phishing scams, and insider threats are just a few of the tactics employed by malicious actors to compromise sensitive data. As technology advances and data becomes increasingly digitized, the risk of data breaches grows, presenting significant challenges for organizations across various industries.



In response to these challenges, the survey delved to understand whether organizations ever experienced a personal data breach or unauthorized access to personal information.

48% reported no data breaches in the last 5 years

15% experienced a breach within the last 1 year

17% faced breaches within the last 3 years

20% encountered breaches within the last 5 years

52%

organizations have experienced at least one data breach or unauthorized access incident in the last 5 years

The statistics reveal that more that half of the organizations surveyed experienced personal data breach within the last 5 years highlighting the pervasive nature of cybersecurity threats leading to significant privacy invasion.

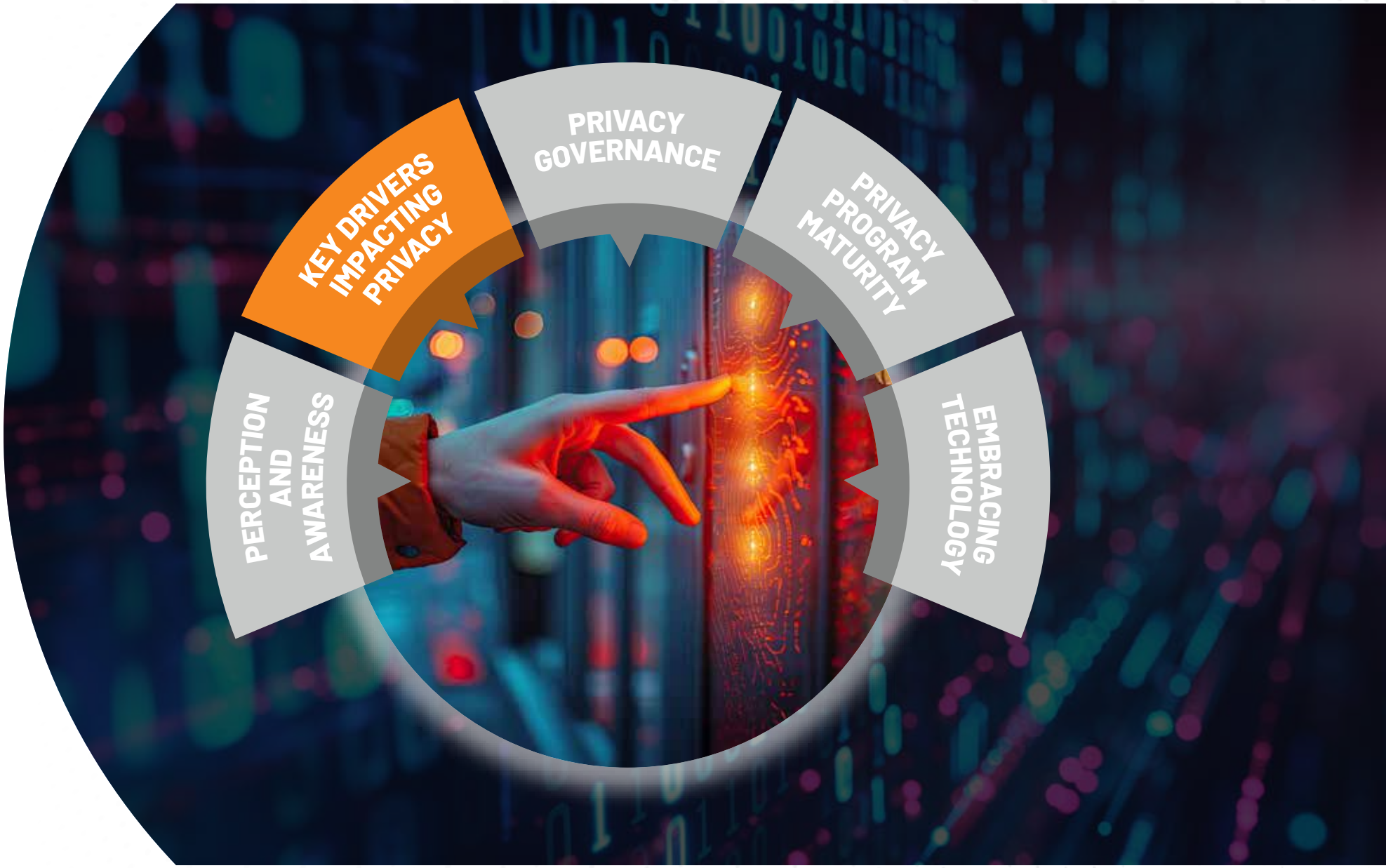
These breaches can lead to significant consequences for organizations, including financial losses, reputational damage, regulatory penalties, and legal liabilities.

Despite advancements in cybersecurity technologies, detecting and responding to personal data breach remains a daunting challenge for many organizations.

This serves as a stark reminder of the persistent and widespread nature of privacy risks. It is imperative for organizations to remain vigilant and proactive in their efforts to prevent, detect, and respond to incidents by adopting a comprehensive approach to develop a resilient infrastructure for data protection.

DPDPA, 2023 REQUIREMENT

Following a data breach, the data fiduciary must alert the Data Protection Board and each impacted Data Principal.


KEY DRIVERS IMPACTING PRIVACY
PRIVACY GOVERNANCE
PRIVACY PROGRAM MATURITY
EMBRACING TECHNOLOGY
PERCEPTION AND AWARENESS

protiviti

DPDPA, 2023 REQUIREMENT

The Act requires consent management, data principal access rights, data retention, and data breach reporting to ensure comprehensive data protection and transparency.

Key Drivers Impacting Privacy

Understanding and Addressing Top Privacy Concerns

Organizations continually assess and respond to the challenges that impede the effectiveness of their data privacy programs and compliance. In doing so, organizations can tailor the privacy practices to address the most pressing challenges.

According to the respondents, the following are the key concerns regarding the privacy program and compliance.

Management of Consent & Data Principal Access Request: The most significant concern, highlighting the complexity of obtaining and managing user consent (including consent for children), reflects the operational difficulties in adapting to stringent regulatory requirements and evolving expectations of transparency from data principals. Additionally, organizations are finding the processing of individuals' requests to access their data to be a challenge. This suggests a need for streamlined processes, skilled resources and better technology usage to handle these requests in a timely and compliant manner.

Visibility of Personal Data: This concern indicates that a lack of clear visibility into where personal data is stored and how it is being used within an organization. This draws the attention towards enhancing process related data flow analysis, data mapping and data inventorization.

Data Retention & Disposal: Effective data retention and disposal are critical components of a robust privacy strategy, as they ensure data is retained only for as long as necessary and is securely disposed off. The complexity arises from varying regulatory requirements, which may mandate different retention periods and disposal methods, making it essential to navigate these intricacies to maintain compliance and minimize the risk of data breaches.

Data Breaches or Security Incidents: The concern for incidents or breaches is indicative of the constant threat landscape and the ongoing effort to secure personal data against unauthorized access or exposure.

Cross Border Data Transfer: Organizations are dependent on the regulator for the application of restriction of data flow to blacklisted countries.

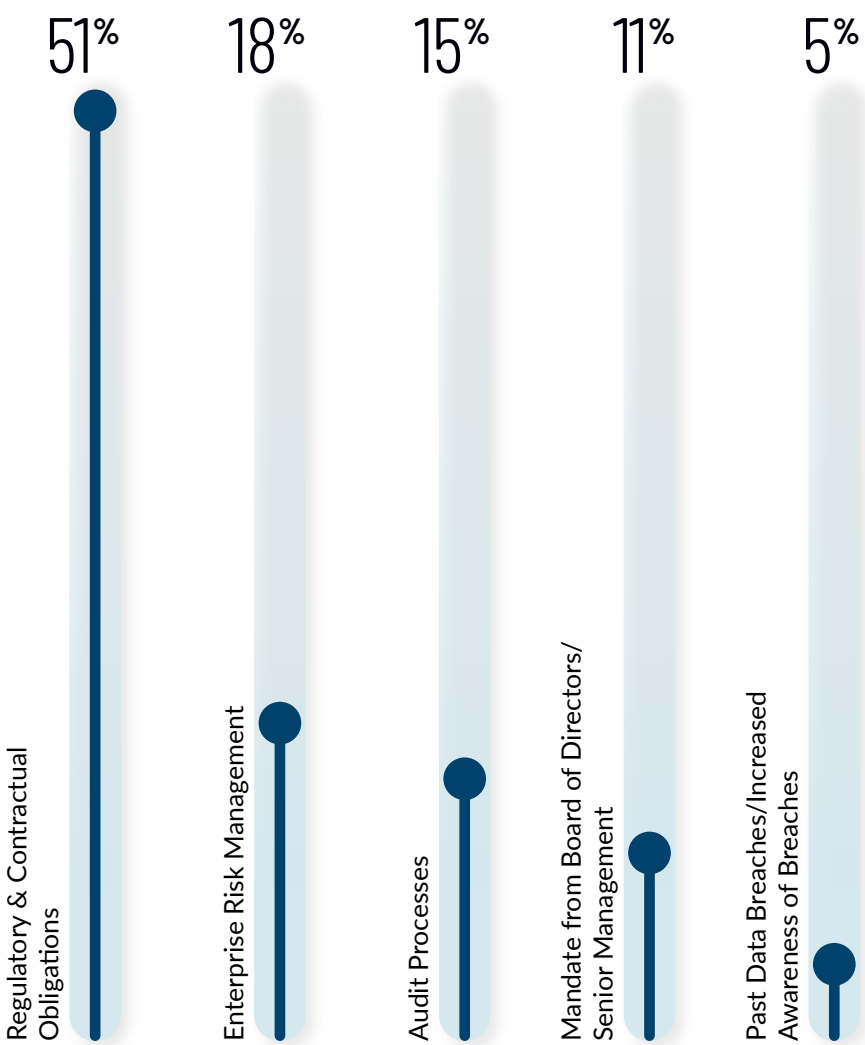
The results highlight proactive awareness and management of key data privacy challenges among organizations.

A significant focus on consent management and data principal access requests demonstrates a commitment to upholding stringent regulatory standards and ensuring transparency with data principals. Furthermore, the emphasis on visibility of personal data and strategic data retention indicates a robust approach to data governance. These efforts are essential for building trust and maintaining the integrity of data privacy programs in a complex digital landscape.

Motivators for Data Privacy Program

Our aim was to delve into the key drivers organizations face—from effective enterprise risk management and regulatory compliance to stakeholder accountability and the growing threat of data breaches. We sought to uncover the key factors that shape an organization's Data Privacy program.

What are the key motivators driving the establishment of a data privacy program?



Confederation of Indian Industry

HERE ARE THE ORGANIZATIONS' MOTIVATIONS FOR PRIORITIZING PRIVACY

Contractual & Regulatory Obligations are the primary motivators

The substantial emphasis on contractual obligations highlights the focus on meeting customer requirements, thereby enhancing customer trust, while close attention to regulatory obligations reflects a strong commitment to upholding legal and compliance standards.

Risk Management is essential

Respondents find Enterprise Risk Management as an essential motivator for organizational commitment to identifying and addressing risks related to data privacy.

Audit Processes Strengthens Foundation

Organizations acknowledge the significance of conducting regular assessments and evaluations to validate the efficacy of their Data Privacy program and focus on areas for enhancement.

Top-level Support is Crucial

The inclusion of a mandate from the Board of Directors/Senior Management suggests that senior executives play an active role in shaping the agenda for Data Privacy initiatives and allocating resources to facilitate their implementation.

Past Incidents Drive Awareness

This implies that organizations draw lessons from past breaches and utilize them as catalysts to fortify their Data Privacy program, aiming to prevent future occurrences.

Organizational Priorities and Practices in Data Privacy Initiatives

Transitioning from conceptualization to the practical implementation of a Data Privacy program poses a significant challenge for many organizations. Prioritizing and focusing on the most crucial privacy tasks is essential. To gain insights into the prevailing privacy management practices across organizations, our survey aimed to understand their key privacy initiatives.

Top 5 Privacy Initiatives

Privacy Governance, Risk, and Compliance (GRC) emerged as one of the prioritized initiative among organizations, highlighting a widespread acknowledgement of the necessity to establish comprehensive frameworks for privacy governance.

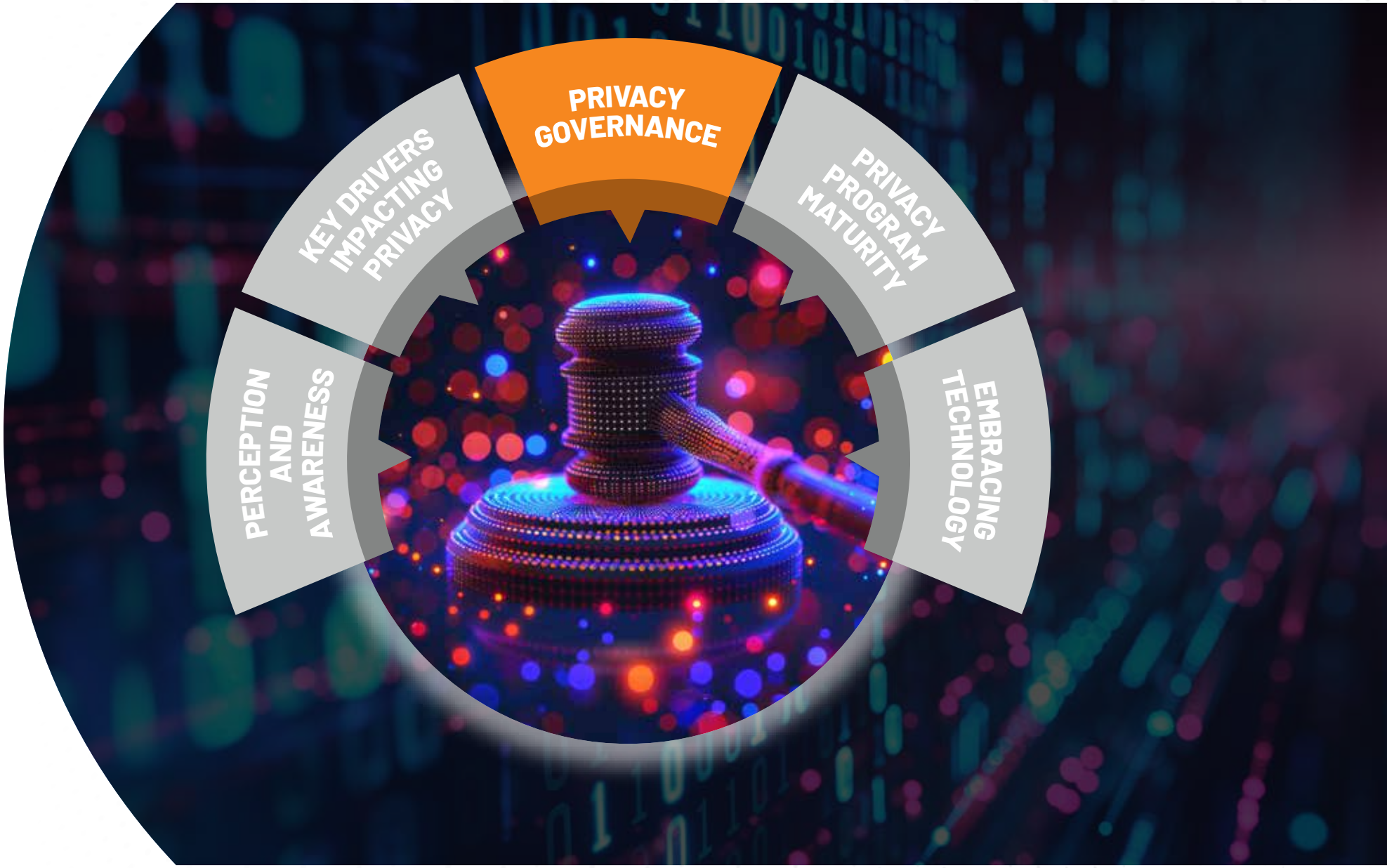
Establishment of DPO and focus on privacy awareness reflects the importance of dedicated leadership in managing privacy-related responsibilities.

Solution Implementation for Consent Management/Data Principal Access rights emphasized that recognition of the importance of privacy management solutions are essential to managing compliance as well as elevating customer trust.

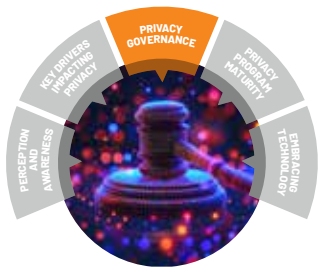
Implementation of Data Classification/ Data Discovery/DLP/DAM/IRM Solutions entails the focus on leveraging technology for developing a secure internal landscape.

Third-Party Security & Privacy Risk Management emphasizes the importance of extending privacy controls lies beyond organizational boundaries.

This reflects that organizations are strategically prioritizing a range of privacy initiatives, including regulatory compliance, governance structure, technology deployment, and risk mitigation approach. Despite potential variations in specific priorities, the overarching objective remains consistent to ensure their readiness to the requirement of DPDPA 2023 and enhance customer trust.


PRIVACY GOVERNANCE
PRIVACY PROGRAM MATURITY
EMBRACING TECHNOLOGY
KEY DRIVERS IMPACTING PRIVACY
PERCEPTION AND AWARENESS

protiviti

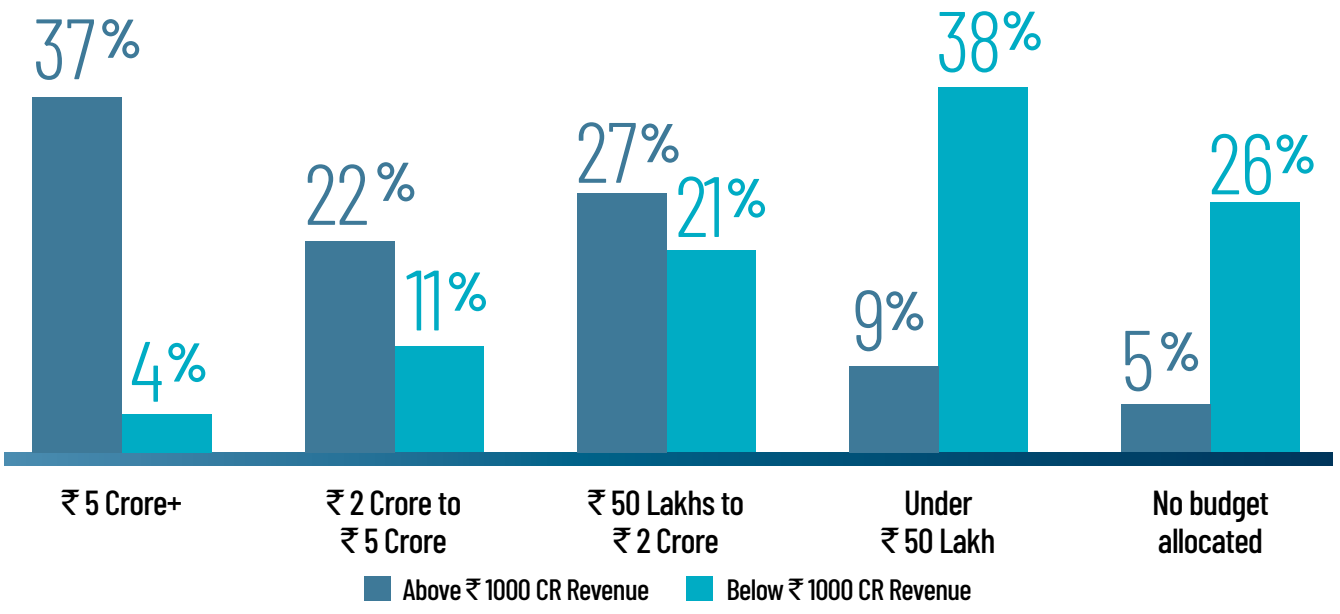


Privacy Governance

Budgetary Allocations for Privacy Programs

As organizations increasingly recognize the importance of data privacy, the allocation of budgets towards these initiatives becomes a pivotal aspect of their strategic planning. This section delves into the various levels of financial commitment made by organizations for managing privacy programs and comply with regulatory standards. Our analysis provides a snapshot of how businesses are prioritizing and investing in their data privacy programs, revealing a broad spectrum of budgetary dedications that reflect differing levels of engagement and readiness.

How much budget or investment is allocated for your Data Privacy Program?

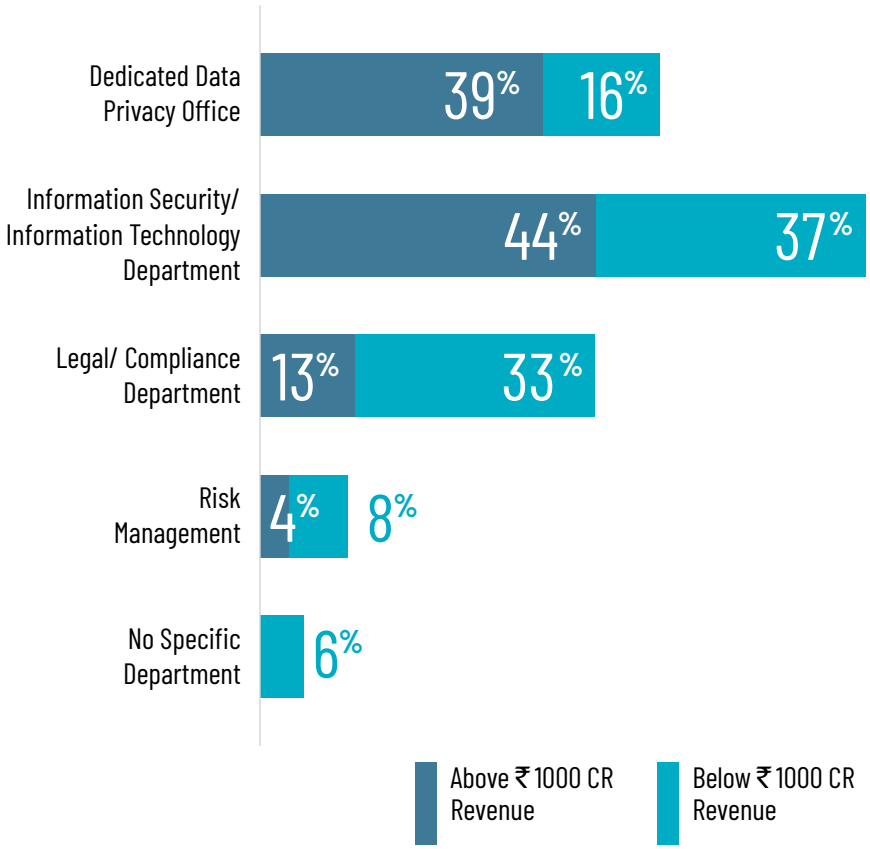


Larger organizations, such as well-established higher revenue companies, tend to allocate substantial budgets for data privacy, often exceeding ₹ 5 crore. In contrast, smaller organizations like MSMEs, startups, and similar classes of data fiduciaries are generally more conservative, typically investing less than ₹ 50 lakhs. Moreover, a significant number of these smaller organizations have yet to allocate any budget for data privacy, suggesting potential opportunities to strengthen their privacy practices. This trend highlights the varying levels of focus on data privacy across different business scales and suggests that without regulatory pressure or direct experience with privacy breaches, smaller organizations may prioritize immediate operational need over long-term privacy investments.

Departmental Oversight Influenced by Organizational Size

We gathered insights from survey respondents regarding the specific departments tasked with the governance and management of data privacy programs within their organizations. The objective was to identify the primary departments responsible for driving and overseeing privacy initiatives and to analyze the variations in these structures across different organizations of different size.

Who is responsible for governing and managing data privacy programs and initiatives in your organization?



Confederation of Indian Industry

Above ₹ 1000 CR Revenue

In organizations with revenues over ₹ 1000 Crore, **44%** predominantly depend on their IT-IS departments for data privacy, making it the most common approach among those surveyed. Meanwhile, **39%** have formed specialized data privacy teams, and **13%** rely on their legal or compliance departments. This trend indicates the significant role IT-IS departments continue to play in data privacy efforts within high-revenue organizations, while also highlighting an increasing shift towards establishing dedicated privacy departments.

Below ₹ 1000 CR Revenue

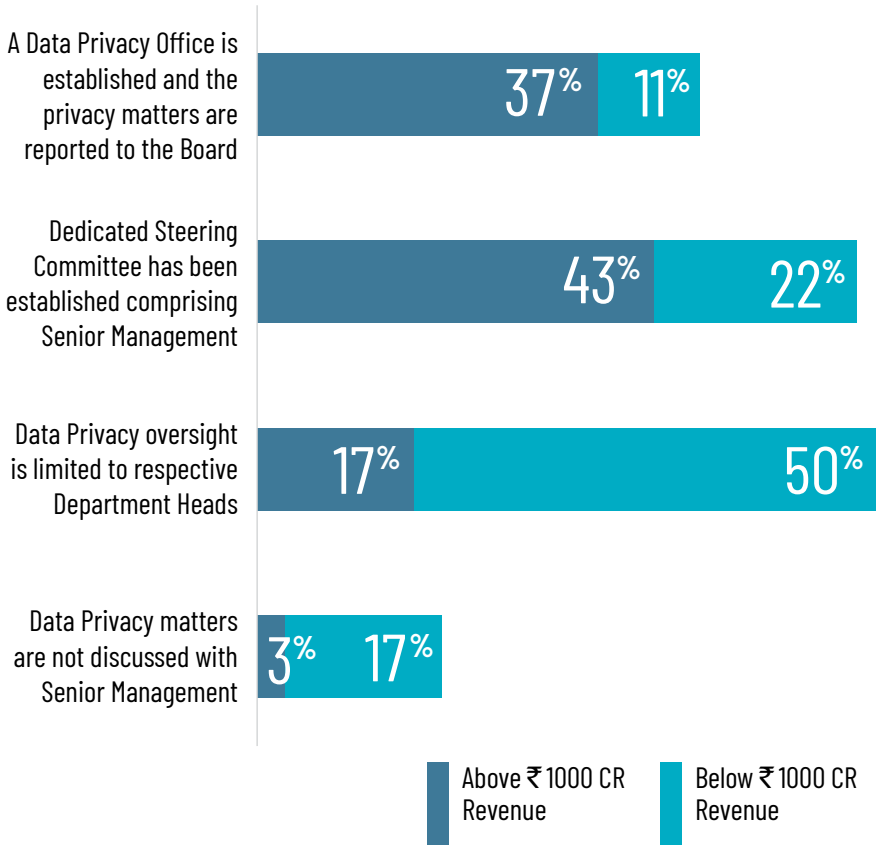
In organizations with annual revenues under ₹ 1000 Crore, **37%** utilize their IT-IS departments for data privacy initiatives, while **33%** rely on their Legal/Compliance Departments, and **16%** maintain dedicated data privacy teams. Additionally, **6%** of these organizations lack a designated department for data privacy, and **8%** assign responsibilities to their Risk Management teams. This illustrates that these companies often spread data privacy duties across various departments instead of forming a specialized unit. This varied approach indicates a more adaptive strategy driven by resource limitations and operational needs.

The results suggest that larger organizations are more likely to have a dedicated data privacy office in addition to relying on IT-IS teams and legal team. In contrast, smaller organizations depend more on IT-IS and Legal/Compliance departments. A small portion of these smaller entities lack a specific privacy department, emphasizing the need for improved privacy governance.

protiviti

Executive Involvement and Oversight in Data Privacy Programs

What is the level of senior management engagement/oversight in your Data Privacy program?



DPDPA, 2023 REQUIREMENT

Significant Data Fiduciaries are obligated to appoint a Data Protection Officer based in India who shall be responsible to the Board of Directors or significant governing body.

FORMAL REPORTING STRUCTURES IN DATA PRIVACY

In organizations with revenues exceeding ₹ 1000 Crore, 37% have established a Data Privacy Office and periodically report data privacy issues to the board. By contrast, only 11% of organizations with revenues below ₹ 1000 Crore have implemented similar practices. This trend suggests that larger organizations are more likely to develop formal structures for managing and communicating data privacy issues to senior management or the board, likely due to increased resources and regulatory demands.

ESTABLISHMENT OF DEDICATED STEERING COMMITTEES

Companies with revenues exceeding ₹ 1000 Crore have established senior management-led Steering Committees for Data Privacy oversight at a rate of 43%. In contrast, smaller firms with revenues below ₹ 1000 Crore have a 22% adoption rate for such committees. Although these committees are less prevalent in smaller companies, their existence still demonstrates a significant commitment to data privacy management. However, the formation of these committees in smaller organizations may be hindered by resource limitations.

LIMITED OVERSIGHT AND AD-HOC REPORTING

50% of organizations with revenues below ₹ 1000 Crore restrict data privacy oversight to department heads, briefing senior management on an ad-hoc basis, as opposed to 17% of larger companies with revenues exceeding ₹ 1000 Crore. This approach is more common in smaller organizations and highlights the need for a more consistent and structured engagement from senior management in data privacy across all organizational sizes.

ABSENCE OF DISCUSSION WITH SENIOR MANAGEMENT

A small fraction of organizations, including 3% of companies with revenues over ₹ 1000 Crore and 17% of organizations with revenues below ₹ 1000 Crore, report that they do not discuss data privacy matters with senior management at all. The relatively low percentages in both categories indicate a generally positive trend toward integrating data privacy discussions into the broader organizational communication and decision-making processes.

Documented Data Privacy Policies in the Organization

DPDPA, 2023 REQUIREMENT

Define and document privacy policies and notices.

Adhering to data protection regulations involves maintaining privacy documents, which fosters compliance, builds trust, mitigates risks, and promotes transparent privacy management practices. Through documented policies and processes, organizations showcase their dedication to safeguarding individuals' privacy rights and upholding regulatory standards

Are there documented data privacy policies and procedures in place within your organization?

VIEW ACROSS SECTORS

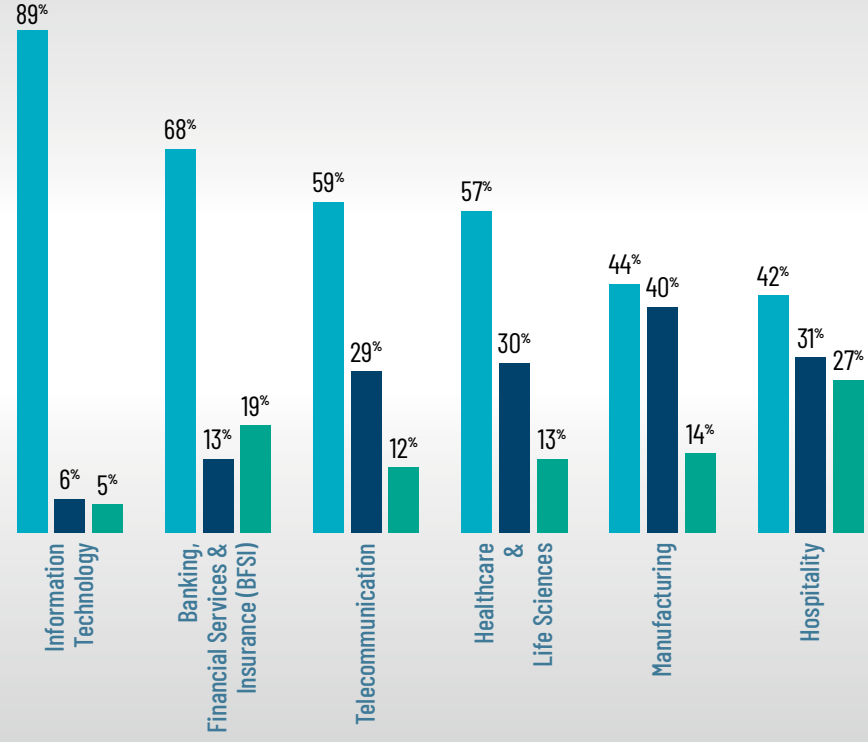
63% Reported having documented data privacy policies and procedures in place

25% Indicated partial documentation of data privacy policies and procedures

12% Admitted to not having such documentation

INDUSTRY SECTORAL VIEW

Further analysis of the responses reveals a sectoral perspective as well. The details are as follows:



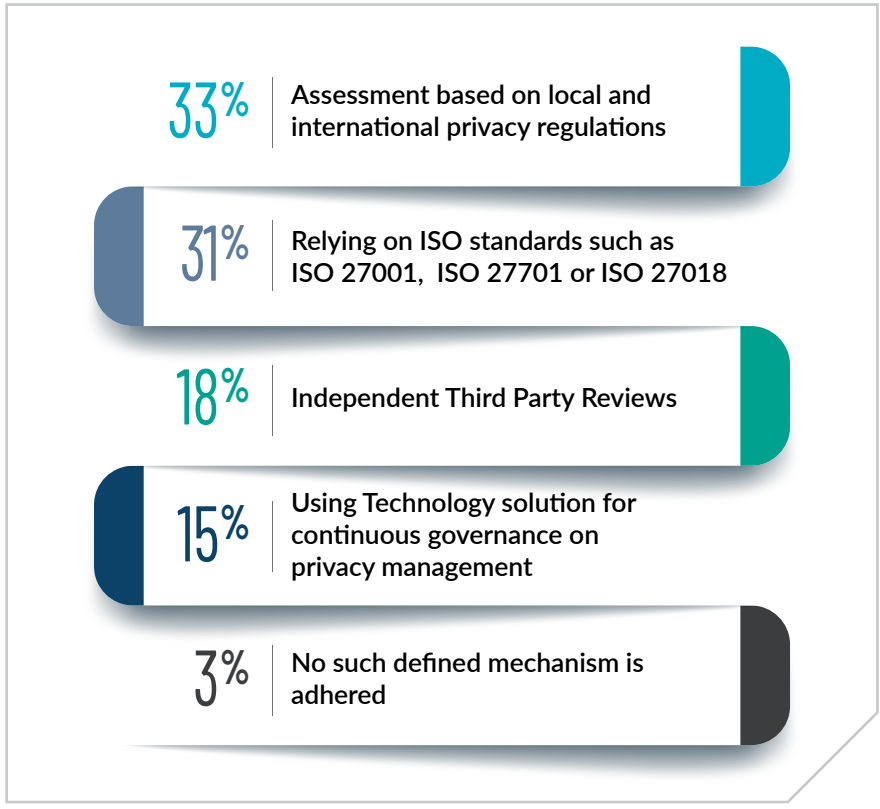
The Information Technology and BFSI sector in India leads in documented data privacy policies and procedures followed by Telecommunication and Healthcare & Life Sciences and are better prepared to adhere DPDPA, 2023 and other sectors particularly Manufacturing & Hospitality need to put significant efforts in order to be ready for the new regulation compliance by developing documented policies and procedure.

Privacy Assurance Mechanisms for Organizational Maturity

Undoubtedly, Privacy Assurance Mechanisms are instrumental in demonstrating adherence to both local and global privacy standards.

To understand the strategies employed by organizations, we asked:

What assurance mechanisms do you intend to utilize to demonstrate compliance and/or maturity within your data privacy program?



DPDPA, 2023 REQUIREMENT

Perform Data Protection Impact Assessments (DPIA) and independent Data Audits

Local Laws, Global Impact Embracing the Digital Personal Data Protection Act reflects a commitment to legal alignment and jurisdiction-specific requirements and suggests a strong focus on regulatory compliance.

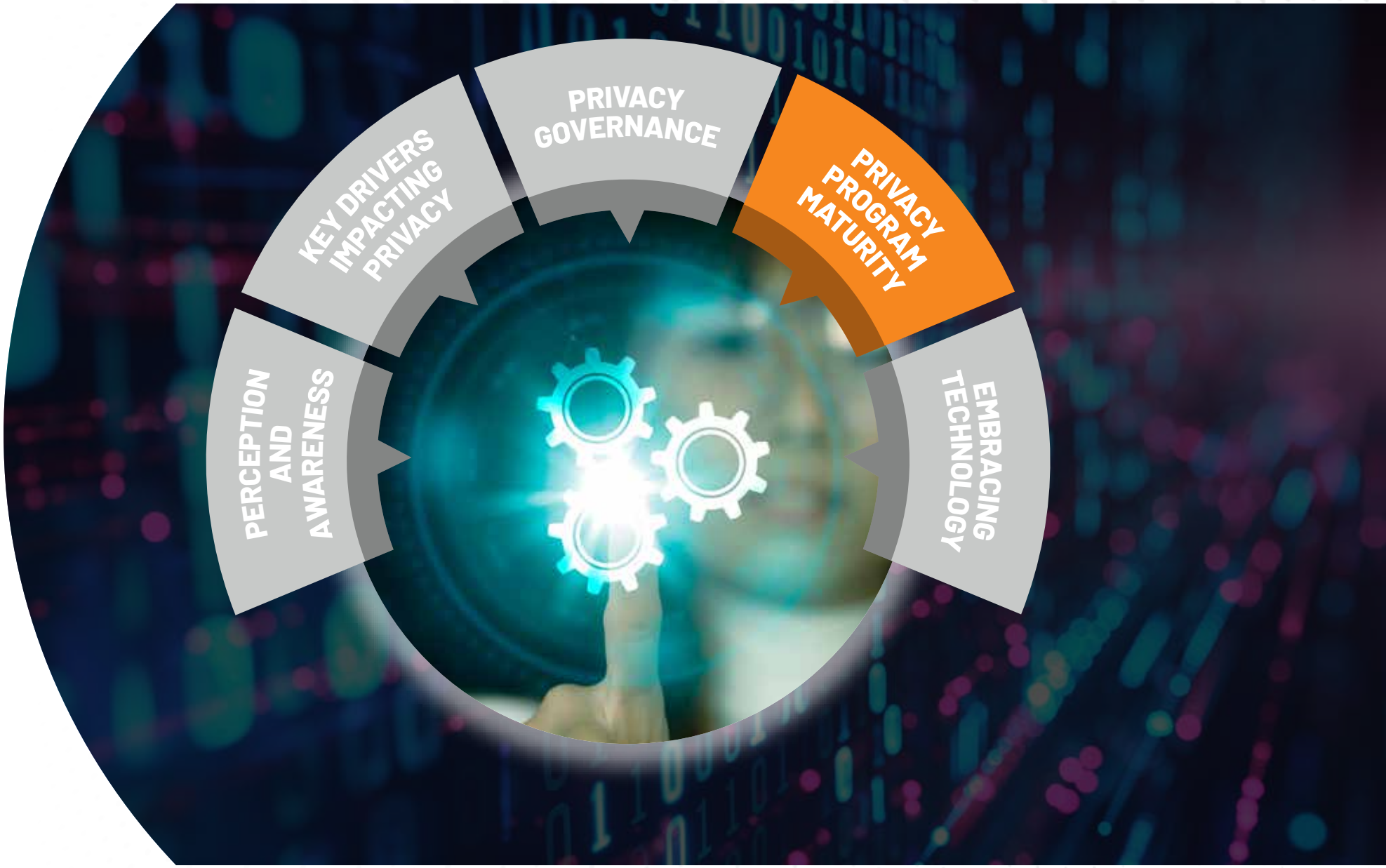
Fortifying ISO 27001 along with Privacy specific standards demonstrate a commitment towards the approach of readiness of organizations aligning it with proven privacy standards and ensuring robust data protection measures.

Navigating Regulations with Privacy Management Tools suggests that implementing privacy management tools isn't merely about adopting technology; it's a strategic approach to streamline compliance efforts and proactively address regulatory challenges.

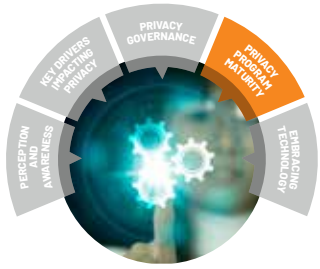
Third-Party Audits for Transparency indicate a strong emphasis on external validation and trust-building.

Yet to Define a standard mechanism of Assurance signifies that some organizations are still navigating through the complexity prior to implementing Assurance Mechanism in the organization.

The survey highlights a focus on compliance, with 64% of organizations relying on privacy standards and regulations. However, gaps remain, as 3% have no formal privacy assurance mechanisms, despite the use of technology and third-party reviews by others.


PRIVACY GOVERNANCE
PRIVACY PROGRAM MATURITY
EMBRACING TECHNOLOGY
KEY DRIVERS IMPACTING PRIVACY
PERCEPTION AND AWARENESS

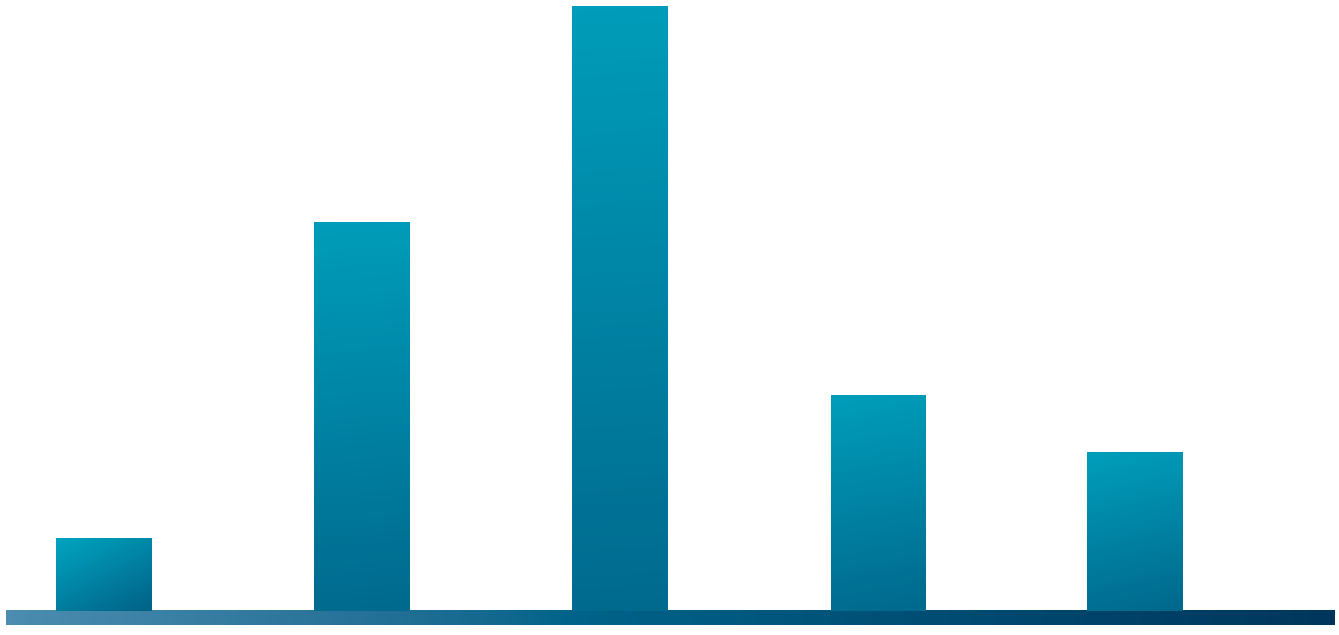
protiviti



Privacy Program Maturity

Organizational Maturity in Privacy Programs

What is the current status of your Data Privacy program?



5%
Data Privacy program is not established and is currently not in the plan

27%
Data Privacy program is in the planning stages

42%
Data Privacy program is defined

15%
Data Privacy program is implemented

11%
Data Privacy program is implemented and at optimized stage

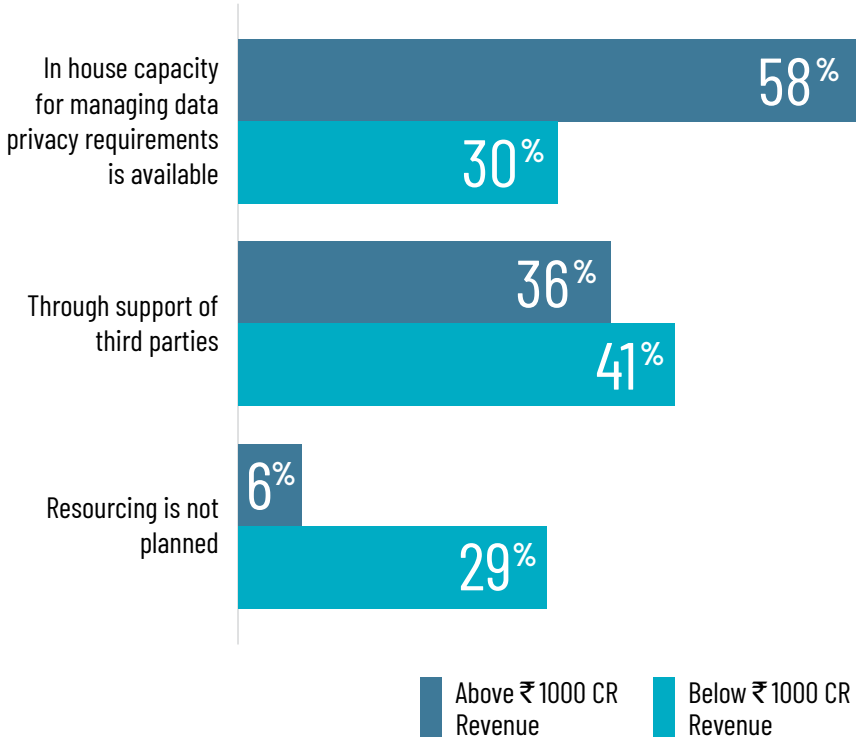
While a majority (42%) have defined their programs and are on the path to implementation, a significant portion is still in the early stages of planning or has not yet recognized the need for a formal program.

The responses indicate a varied level of maturity in data privacy program implementation across organizations. Only a small percentage have achieved an optimized state, demonstrating the need for many organizations to continue developing and enhancing their data privacy efforts to meet the demands of an increasingly data-driven world. This trend suggests that while progress is being made, there is still a considerable journey ahead for many organizations to reach a mature and fully optimized data privacy posture.

Meeting Privacy Requirements with Skilled Resources

Skilled resources, whether in-house or outsourced, are instrumental for executing the entire privacy journey, from conducting impact assessments and developing data governance frameworks to managing technology solutions, thus supporting privacy management objectives.

Does your organization have adequate skilled resources to manage privacy requirements, or would external partners be needed for support?



29% of Smaller Organizations such as MSME , Start-ups and similar Data fiduciaries lack planned resources for Privacy Management, raising readiness concerns

Confederation of Indian Industry

CONTRASTING STRATEGIES BASED ON SIZE OF THE ORGANIZATION

We observed that majority of organizations over ₹ 1000 crore revenue have in-house capacity for managing data privacy requirements compared to less than ₹ 1000 crore organizations. This indicates that larger organizations are more likely to invest in building internal capabilities for privacy management probably due to high resource availability, or complexity of operations.

OUTSOURCING TRENDS

Interestingly, the proportion of organizations outsourcing privacy management services is relatively similar between the two revenue groups, with 41% for under ₹ 1000 crore revenue and 36% for over ₹ 1000 crore revenue. This suggests that outsourcing is a common strategy regardless of organizational size, possibly due to the complexity and specialization required in privacy management.

UNPLANNED RESOURCING INDICATING A RED FLAG

In organizations with revenue under ₹ 1000 crore, our research unveils a troubling pattern: a significant 29% lack planned resources for managing privacy, hinting at a dearth of proactive measures and casting doubt on their readiness to tackle evolving privacy regulations. In contrast, the figure drops substantially to a mere 6% for those with revenue surpassing ₹ 1000 crore, suggesting a heightened level of preparedness and strategic anticipation in addressing privacy issues.

Relying on in-house expertise or third-party vendors, prioritizing skilled resources in privacy management is imperative. This proactive stance will ensure compliance, risk mitigation, and stakeholder trust across all organizational sizes and revenue brackets.

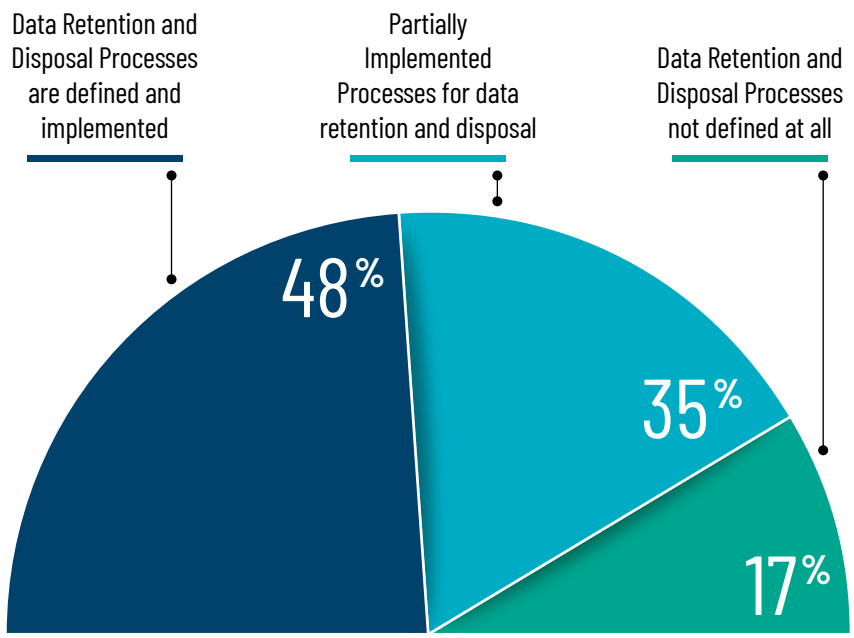
CII has taken a commendable step towards addressing the critical need for data protection expertise in India. Through its initiative to skill 1,000 personnel in data protection, CII is actively contributing to the development of a skilled workforce capable of safeguarding sensitive information. Furthermore, CII's organization of cyber security master classes serves as a valuable platform to raise awareness about data protection best practices among industry professionals. These master classes provide in-depth knowledge and practical guidance on safeguarding data, mitigating risks, and ensuring compliance with relevant regulations.

protiviti®

Exploring the Importance of Data Retention and Disposal Processes within Organizations

Data Retention and Disposal are crucial elements of data governance, ensuring ethical information management. Our survey delves into the significance of defining and implementing these processes within organizations.

Are processes for data retention and disposal of privacy-related data defined and implemented?



While a significant majority of organizations have established data retention and disposal processes, a notable minority still lack clear guidelines in this area. This indicates room for improvement in data management practices.

DPDPA, 2023 REQUIREMENT

A Data Fiduciary must erase personal data when consent is withdrawn or the purpose is no longer served, and ensure their Data Processor also deletes the data.

SIGNIFICANCE OF DATA RETENTION AND DISPOSAL PRACTICES

Compliance & Legal Obligations

Avoiding penalties and ensuring compliance with local and global regulations such as DPDPA, GDPR, HIPAA.

Data Security

Retaining data increases the risk of breaches; timely deletion minimizes liabilities.

Cost Reduction

Unnecessary data storage drains resources; efficient retention and disposal save costs.

Protecting Privacy

Holding onto data heightens privacy risks; deletion safeguards individuals' rights.

Business Efficiency

Removing outdated data streamlines operations and improves access to relevant information.

Enabling Trust

Mishandling data tarnishes reputation; responsible handling builds trust with stakeholders.

Privacy Risks Emerging From Third-Parties

Organizations often rely on a complex network of third-party vendors to perform essential services—ranging from IT support to customer relationship management. Though beneficial, these partnerships can pose privacy risks if sensitive data is not securely managed, potentially leading to exposures outside the organization's direct control.

Effective Third Party Risk Management (TPRM) practices are essential for identifying, assessing, and mitigating the risks associated with third-party vendors. Organizations must develop a comprehensive strategy that encompasses the entire lifecycle of the vendor relationship—from initial due diligence to ongoing monitoring. Privacy risk management in vendor relations is not a one-off task but a continuous process that evolves with the changing threat landscape.

Here's some insights on how companies are addressing privacy concerns with third-parties:

DPDPA, 2023 REQUIREMENT

A Data Fiduciary remains accountable for compliance with data protection laws and must ensure any Data Processor they use is engaged through a valid contract.

While the majority implements strategies like confidentiality agreements and risk assessments, signifying a proactive stance, a considerable segment relies solely on static agreements such as NDAs and SLAs. Notably, over 8% of companies are yet to take any significant measure for mitigating the risks associated with third parties and about 2% are at the stage of identifying the risk.

There is a clear need for a more consistent and rigorous approach to third-party risk management across the board to effectively protect data privacy and enhance regulatory compliance.

Organizations must rigorously evaluate their vendors, mandate contractual terms that underscore adherence to data protection standards and implement regular audits of third-party security measures. These steps are crucial not just for safeguarding data but also for affirming an organization's dedication to privacy.

How companies are addressing privacy concerns with third-parties:

38%
Both through contractual obligations / SLAs and performing third party risk assessments

32%
Only through contractual obligations / SLAs

20%
Through periodic third-party risk assessments

8%
Third-party vendor risks are identified but not yet addressed

2%
Not Identified/ Addressed

protiviti

Ensuring Privacy Compliance Beyond Borders

Indian DPDPA 2023 enforces a need to restrict data processing to such country or territory outside India as may be so notified by GOI. Additionally, in India some sectoral law reflects a need of data localization demonstrating a very nuanced approach towards personal data security, economic strategy, legal enforcement, and national security. For example, the Reserve Bank of India's (RBI) directive in 2018 mandated all payment system data to be stored exclusively in India. This directive was meant to assure better supervisory access to the critical financial data for the integrity of India's payment systems. According to the survey findings, here is how organizations respond to regulations concerning cross-border transfers:

DPDPA, 2023 REQUIREMENT

The Central Government can notify restrictions on transferring personal data by a Data Fiduciary to specific countries or territories outside India.

The analysis highlights the diversity of approaches adopted by organizations to comply with stringent regulations on cross-border transfers, reflecting varying levels of preparedness and compliance sophistication.

In case stringent rules for data cross-border transfers are effective, how would your organization address those?

35% **ENFORCEMENT VIA LEGAL AGREEMENTS**

Organizations will opt to manage cross-border data transfers through specific data protection clauses in their agreements. This suggests a tailored approach to compliance, with a focus on legal frameworks to safeguard data transfers.

27% **DATA RESIDING WITHIN TERRITORY**

The approach, planned to be adopted by over a quarter of organizations, is to store all personal data within the region and avoid any external transfers. This indicates a preference for a straightforward compliance method that minimizes legal complexities and risks associated with cross-border data flow.

20% **YET TO DEFINE APPROPRIATE MEASURES**

Some organizations see no need for data localization or transfer protocols, possibly due to domestic-only operations or an early stage in regulatory adaptation.

18% **EXPERT CONSULTATION**

A significant proportion of organizations engage experts to formulate compliant transfer strategies, showing a commitment to specialized solutions and potentially reflecting the complexity of navigating international data transfer regulations.

Organizational Preparedness for Incident Response

As organizations accumulate and handle extensive customer data, the potential for privacy breaches and incidents grows. Customer privacy concerns span across areas such as unauthorized access to personal information, data misuse, and breaches of confidentiality. To address these concerns to uphold privacy rights, organizations must establish formal processes and mechanisms for managing privacy incidents and reporting data breaches. Demonstrating the current state of data privacy practices within organizations to showcase the extent of formal processes implemented for managing & reporting personal data breaches, the respondents expressed the below.

How ready is your organization to identify and manage privacy breaches?

OPTIMIZED

23% of respondents have established optimized processes for managing privacy concerns and reporting data breaches. This suggests a focus on continuous improvement, where processes are regularly evaluated and refined to achieve optimal performance.

PROACTIVE

33% of respondents have implemented proactive measures, indicating that their processes are quantitatively managed. These organizations are likely using metrics to mitigate privacy breaches, ensuring that processes are not just followed but are also predictable and efficient.

MANAGED

28% of respondents have a managed approach, meaning their processes are defined, documented, and standardized across the organization. However, there may still be a need for further refinement and consistency in how these processes are implemented to reach higher maturity levels.

REACTIVE

14% of respondent's measures are reactive, meaning processes may exist but are not fully standardized or consistently applied. Such organizations respond to issues as they arise.

NO ASSESSMENT

2% of respondents report that their organizations have not conducted any assessment regarding management of privacy concerns or reporting data breaches.

The distribution of organizations across these readiness levels suggests that while a significant percentage have reached higher maturity levels (Optimized and Proactive), a substantial portion remains at lower maturity levels, with non-proactive approaches. This indicates a need for continued efforts in advancing process maturity, particularly for those organizations at the lower end of the maturity spectrum, to enhance their data privacy management capabilities.

protiviti

Navigating Privacy Concerns in Emerging Technologies

Advancing technology is reshaping how organizations handle data, introducing new opportunities and privacy challenges. Technologies like AI/ML algorithms, IoT devices, Blockchain, and the Metaverse are transforming data collection and usage. These advancements require proactive privacy management to safeguard individuals' rights. To assess organizational readiness in addressing privacy concerns tied to these technologies, we aim to uncover insights into privacy management amid rapid technological progress.

The analysis shows varying levels of readiness among organizations in addressing privacy concerns amid technological advancements. While some organizations are forging ahead with proactive plans, others are lagging, yet to evaluate the impacts of emerging technologies. The prevailing business model of tech companies relies on mass data collection, conflicting with privacy rights and jeopardizing the safety of privacy rights defenders.

In our survey, interestingly, technology focused companies are predominantly in the planning or ready stages. This indicates a cautious strategy, possibly due to the rapidly evolving nature of these technologies and uncertainty around future regulations.

What is the level of readiness your organization has for managing privacy concerns related to emerging technologies such as AI/ML, IoT, Blockchain and Metaverse?

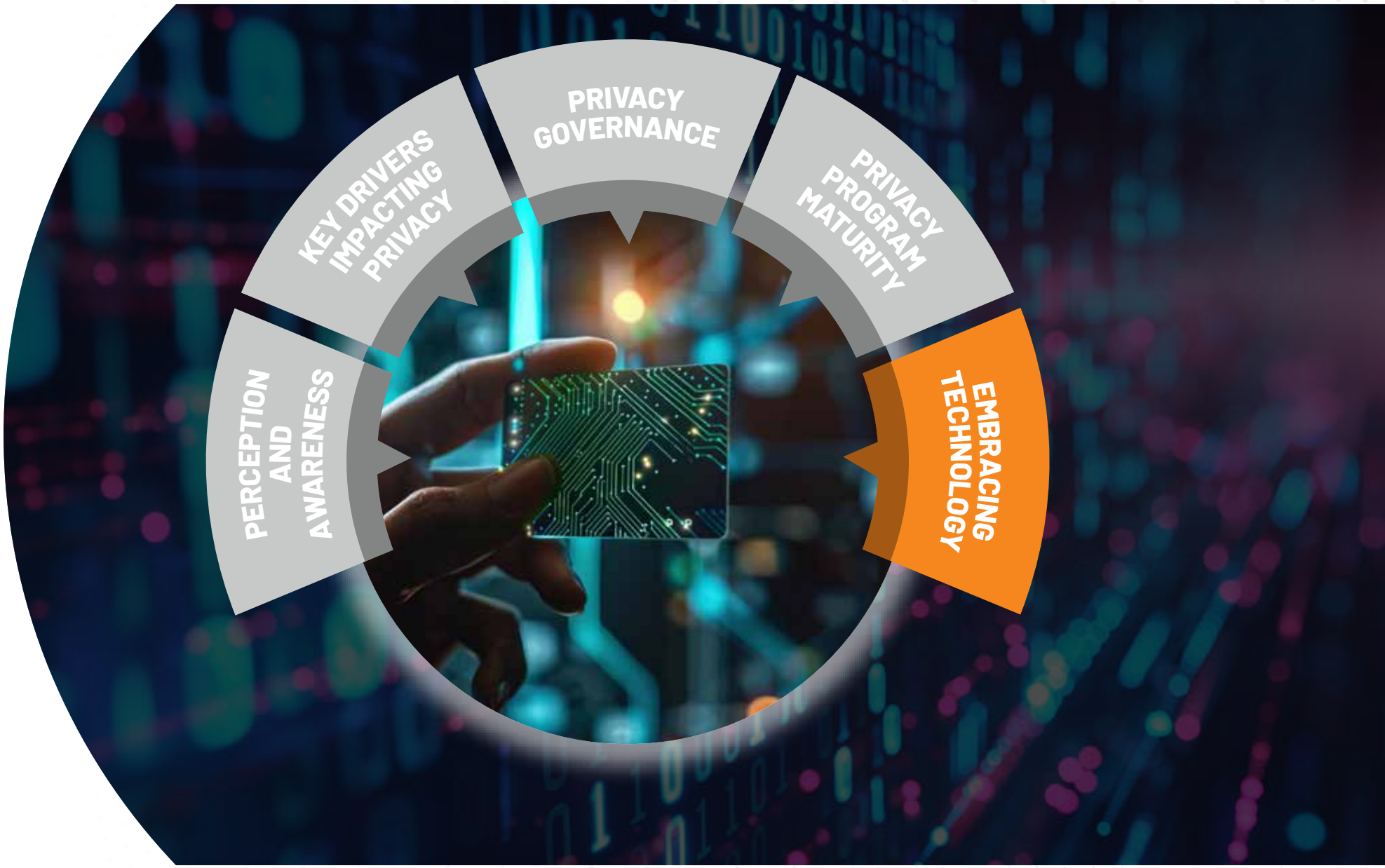
While some organizations are making significant strides, there is a noticeable variance in readiness and proactive planning across the industry.

37% Are in the process of developing plans to address privacy concerns arising from emerging technologies

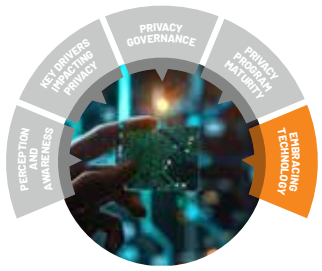
24% Feel prepared to manage privacy concerns associated with emerging technologies

27% Have not conducted assessments to identify the privacy impact of emerging technologies

12% Have implemented a "wait and see" approach, monitoring the landscape before acting


PRIVACY GOVERNANCE
PRIVACY PROGRAM MATURITY
EMBRACING TECHNOLOGY
PERCEPTION AND AWARENESS
KEY DRIVERS IMPACTING PRIVACY

protiviti



Embracing Technology

Empowering Data Privacy with Automation

Amidst growing data proliferation and heightened privacy concerns, organizations are increasingly turning to automation to strengthen their data privacy frameworks. Efforts are being channeled into automating critical elements such as Data Discovery and Classification, Data Principal Access Requests, Privacy Impact Assessments (PIAs), and Consent Management, and more. By automating key aspects of data governance and compliance, organizations aim to enhance process efficiency, improve accuracy, and solidify their compliance posture. We surveyed organizations to identify the top three priorities within their data privacy programs targeted for automation.

Which of the Data Privacy programs do you intend to automate?

01

Privacy Rights & Consent Management automation for effective handling and management of user consents and privacy rights to comply with regulations effectively and enhance customer trust.

02

PIA/DPIA/TPRM Automation is essential to assess personal data handling and ensure regulatory compliance.

03

Data Governance (Data Discovery/Data catalogue) Automation emphasizes on using technology to manage data assets efficiently and enforce policy compliance..

Given the vast amount of personal data processed today, data privacy automation is essential for efficiently managing privacy tasks. Some of the key areas in Data Privacy are Consent Management, Privacy Rights Management, Data Governance, and PIA/DPIA, which is essential for any data-reliant organization. This will enable consistent regulatory compliance, reduces human error, and streamlines data protection efforts.

In essence, automation enables real-time monitoring and reporting, facilitating the quick identification, reporting, and resolution of data breaches or privacy issues. It also frees up resources for strategic privacy initiatives, ultimately enhancing the organization's data security and building customer trust by demonstrating a commitment to protecting personal information.

Safeguarding Privacy Through Digital Identity Strategies

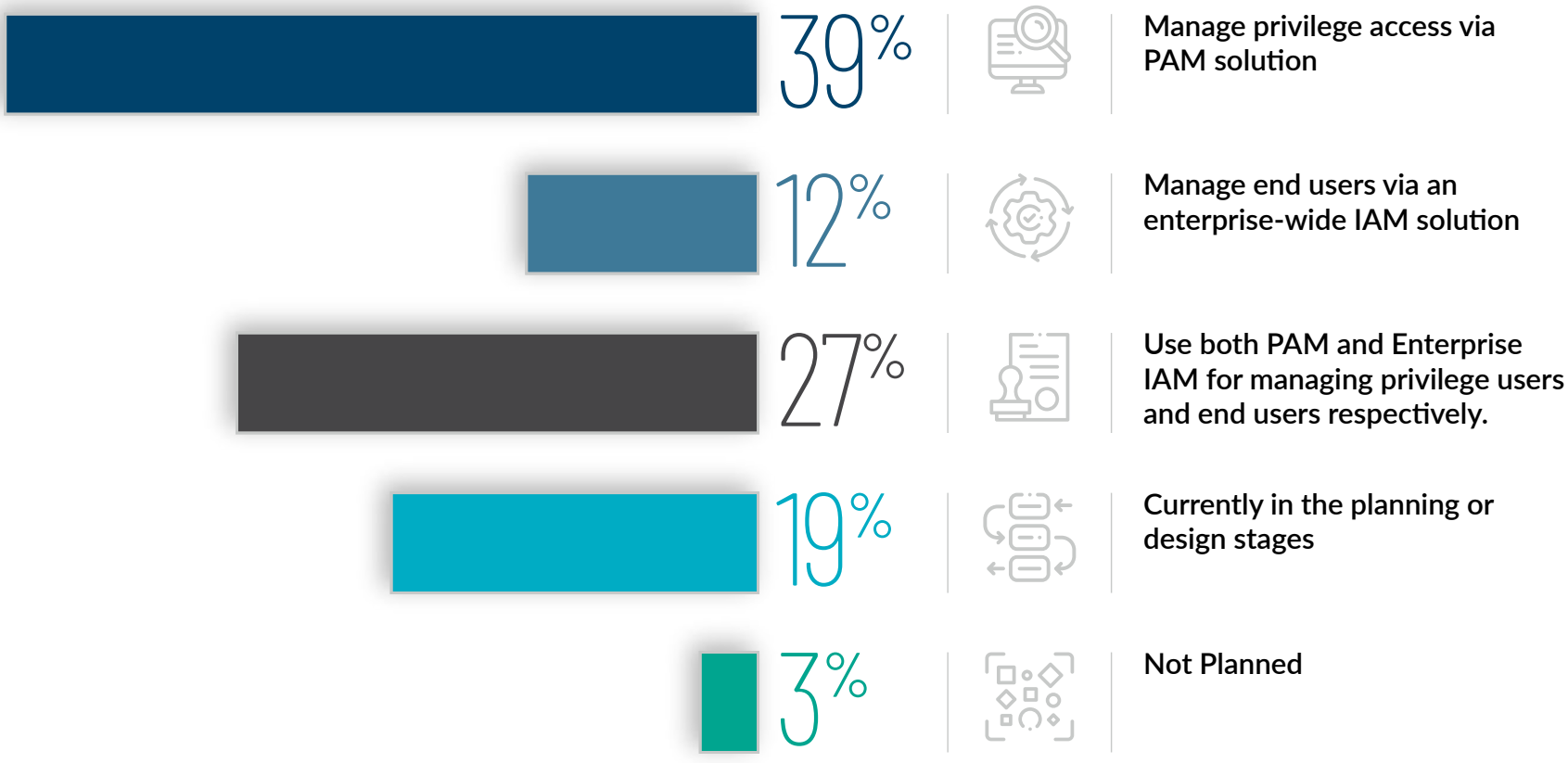
Data breaches have become a pervasive threat, with organizations grappling with a range of challenges including privilege escalation, insider threats, identity theft, and more.

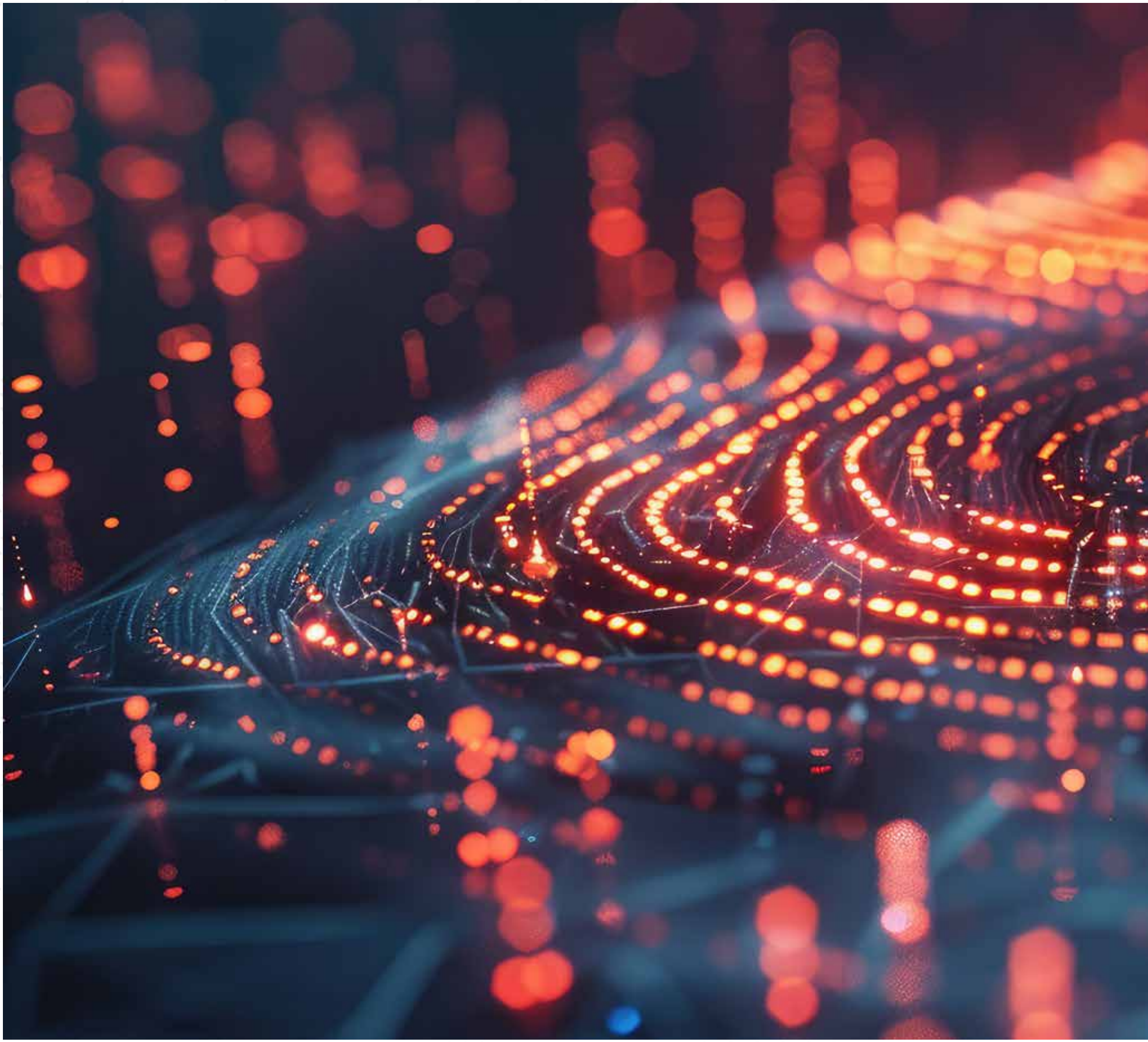
There is a critical importance of robust Identity and Access Management (IAM), including Privileged Access Management (PAM), which cannot be overstated.

Here's some insights on how companies are leveraging IAM strategies:

What areas around identity and access management are you focusing on supporting privacy compliance requirements?

The survey indicates that a significant focus is on managing just privilege access, with 39% of organizations only utilizing Privilege Access Management (PAM) solutions. Additionally, 27% use both PAM for privilege users and enterprise-wide IAM solutions to regulate end users. While 19% are in the planning or design stages, a smaller group (12%) relies solely on IAM solutions, and only 3% have no plans in place. These results emphasize the importance placed on improving identity and access management to meet privacy compliance requirements.





PATH AHEAD

PATH AHEAD

Developing a Robust Data Privacy Program

In today's environment of increased regulatory demands and customer expectation regarding data privacy and protection, organizations must treat efforts on privacy protection as integral compliance initiatives. By adopting a comprehensive privacy perspective, businesses can ensure that all aspects—from partnerships and marketing strategies to product launches and operational changes—are aligned with their data privacy and protection commitments.

Here is a roadmap designed to help organizations comply with the Digital Personal Data Protection Act, 2023, and implement best practices for personal data protection, thereby minimizing the risk of data breaches.

Key steps to attain compliance to Digital Personal Data Protection Act, 2023

01 — Appoint a competent person as data protection officer based in India and make the contact information available.

02 — Seeking consent from the Data Principal and informing about the type and purpose of data collected.

03 — Define privacy notice templates to be preceded or accompanied by consent requests.

04 — Define and document privacy policies.

05 — In case personal data transmission is required outside India, then an inventory of countries to which the transfer shall happen should be created. This can be validated once the central government defines the list of countries to which the data transfer is restricted.

06 — Initiate implementation of the policies and procedures to enhance privacy landscape.

07 — Define templates for responding to data principal rights requests related to the following:
- Data Fiduciary and Significant Data Fiduciary: Correction and erasure requests.
- Startups and other similar class of Data Fiduciary: Correction requests.

08 — Define process for grievance redressal for data principals.

09 — Ensure technology and process relevant measures to strengthen privacy.

10 — Have a data processer defined (in case required) but only after having the right safeguards and contract.

11 — Define data breach notification related process and templates for the Data Privacy Board and the Data Principal.

12 — Perform Data Protection Impact Assessment (DPIA).

13 — Have an independent data auditor appointed for validating the compliance.

14 — Perform periodic reviews.

DATA FIDUCIARY | SIGNIFICANT DATA FIDUCIARY | START-UPS AND OTHER SIMILAR CLASS OF DATA FIDUCIARIES

CII Digital is actively collaborating with the Government to develop strategic plans for various industries and sectors, with a strong emphasis on the Digital Personal Data Protection (DPDP) Act. The partnership aims to align industry practices with the new regulations, ensuring a forward-looking approach that addresses key data protection challenges.

Holistic Steps for an Effective Data Privacy Program

Step 1

Conduct Data Privacy Risk Assessment

A comprehensive data privacy risk assessment is essential for identifying compliance vulnerabilities and enhancing protection efforts. This assessment involves pinpointing the data that the organization collects, stores, and processes, evaluating the associated privacy risks such as confidentiality and security, assessing the effectiveness of current controls, and identifying any unresolved or emerging risks. This process enables leadership to comprehend crucial data privacy regulations, ascertain compliance obligations, and fortify the organization's data privacy framework.

Step 2

Establish a Baseline

Establishing a baseline is a foundational step for privacy compliance within any organization. It involves a thorough review of the organization's privacy commitments, pinpointing exactly what has been promised to customers regarding how their data is handled, including collection, processing, storage, and transfer processes. Most crucially, it verifies whether the organization is adhering to these promises. Expanding these commitments to include contracts with third-party vendors and training programs, enhances overall data privacy practices.

Step 3

Adopt Privacy-Enhancing Technologies

Organizations must implement privacy-enhancing technologies to safeguard data effectively. These technologies include encryption, data loss prevention tools, anonymization techniques, and automated systems for privacy governance, consent management, data mapping, and privacy impact assessments. They also encompass consent and preference management tools, as well as secure data storage solutions. These technologies are vital for protecting sensitive information, reducing unauthorized access, and ensuring compliance with regulatory frameworks.

Step 4

Manage Change

Organizations need to continuously evaluate how changes in service delivery, product offerings, and third-party interactions could affect their data privacy commitments. This is particularly crucial for larger organizations where changes can occur rapidly. Establishing a structured change management program ensures data privacy is treated as a strategic priority, fostering a compliance culture. Effective management of change helps maintain trust, aligns senior management with data privacy initiatives, and ensures that organizational commitments to privacy are met consistently.

Step 5

Documentation and Awareness

Effective documentation and awareness are crucial for any successful data privacy program. Organizations must thoroughly document their privacy procedures, including detailing processes, risks, and controls, and address any deficiencies by investing time and resources. Equally important is documenting how customer information is managed and the impacts of any changes to privacy risks. Clear, accessible records are essential for effective program management and maintaining compliance.

Step 6

Establish a Privacy Command Center

The Privacy Command Center will serve as a specialized hub dedicated to enforcing compliance with applicable privacy regulations. Such setup can elevate data protection maturity by serving as a centralized unit that enforces compliance, oversees privacy practices, and manages all aspects of data privacy, including consent management, data retention, disposal, and breach response coordination.

Embedding privacy considerations from the design phase of systems (Privacy-by-design), products, and services is crucial. This involves implementing privacy-enhancing technologies and practices to minimize personal data collection and storage, ensuring robust data protection throughout the data lifecycle. Such proactive privacy integration helps establish a comprehensive data privacy strategy that meets regulatory standards, builds consumer trust, and adapts to the evolving landscape of data privacy and protection.

CONCLUSION

CONCLUSION

The results from our comprehensive study on data privacy in India highlight the intricate and pressing challenges surrounding the implementation of the Digital Personal Data Protection (DPDP) Act 2023. The diverse perspectives captured in the survey emphasize the difficulty of crafting legislation that meets the varied needs of stakeholders while building trust and ensuring accountability.

Across all sectors, the development of robust privacy frameworks is essential. The survey results highlight the critical role that dedicated privacy teams, particularly within IT/IS and legal departments, play in driving these efforts. However, smaller organizations, such as MSMEs and startups, face considerable obstacles due to limited budgets and resources. This highlights the urgent need for accessible assurance mechanisms, including independent audits and privacy management tools, to support these organizations in achieving compliance and strengthening their data protection practices.

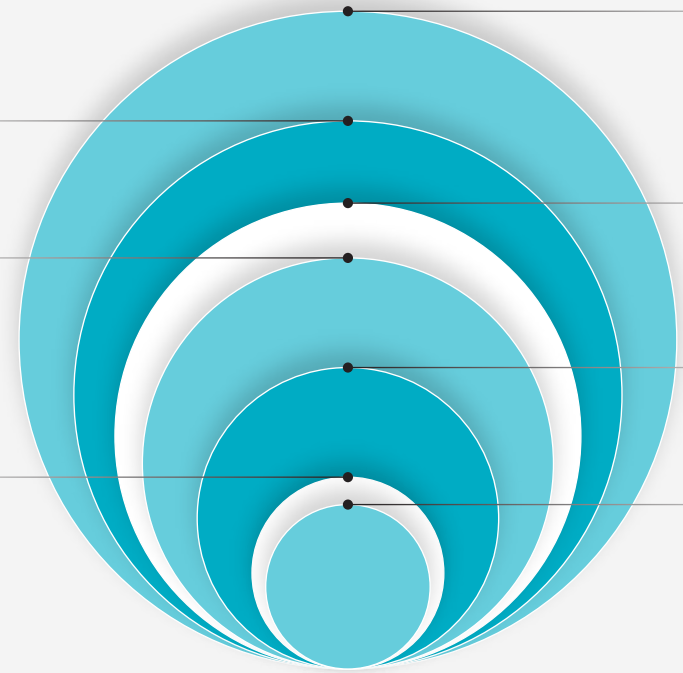
Moving forward, it is imperative for organizations of all sizes to adopt proactive strategies to navigate the complexities of regulations, emerging technologies and maintain stakeholder trust. Investing in privacy management and embracing automation will empower organizations to mitigate risks, ensure regulatory compliance, and safeguard sensitive data in an increasingly data-driven world.

This report offers critical insights into the current state of data privacy in India and serves as a valuable resource for decision-makers and privacy professionals. It aims to guide future policy decisions and advance data privacy practices across the country, with a focus on supporting industry stakeholders in implementing robust and adaptable data protection measures in the evolving digital landscape.

ANNEXURE

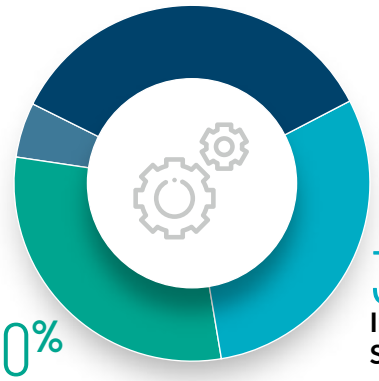
Survey Demographics

SECTORS



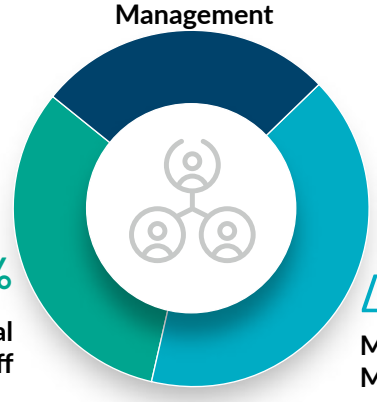
- 24% Banking, Financial Services, and Insurance (BFSI)
- 17% Manufacturing
- 11% Hospitality
- 6% Other Sectors
- 20% Information Technology
- 15% Healthcare & Life Sciences
- 7% Media & Telecommunications

FUNCTIONAL REPRESENTATION



- 35% Information Technology (IT)
- 30% Information Security (IS)
- 30% Business Functions (Operations, HR, Finance, Marketing)
- 5% Legal

ORGANIZATIONAL LEVEL



- 27% Senior Management
- 41% Middle Management
- 32% Operational Staff

About CII

The Confederation of Indian Industry (CII) works to create and sustain an environment conducive to the development of India, partnering Industry, Government and civil society, through advisory and consultative processes.

CII is a non-government, not-for-profit, industry-led and industry-managed organization, with around 9,000 members from the private as well as public sectors, including SMEs and MNCs, and an indirect membership of over 365,000 enterprises from 294 national and regional sectoral industry bodies.

For more than 125 years, CII has been engaged in shaping India's development journey and works proactively on transforming Indian Industry's engagement in national development. CII charts change by working closely with Government on policy issues, interfacing with thought leaders, and enhancing efficiency, competitiveness, and business opportunities for industry through a range of specialized services and strategic global linkages. It also provides a platform for consensus-building and networking on key issues.

Through its dedicated Centres of Excellence and Industry competitiveness initiatives, promotion of innovation and technology adoption, and partnerships for sustainability, CII plays a transformative part in shaping the future of the nation. Extending its agenda beyond business, CII assists industry to identify and execute corporate citizenship programmes across diverse domains including affirmative action, livelihoods, diversity management, skill development, empowerment of women, and sustainable development, to name a few.

For 2024-25, CII has identified "Globally Competitive India: Partnerships for Sustainable and Inclusive Growth" as its Theme, prioritizing 5 key pillars. During the year, it would align its initiatives and activities to facilitate strategic actions for driving India's global competitiveness and growth through a robust and resilient Indian industry.

With 70 offices, including 12 Centres of Excellence, in India, and 8 overseas offices in Australia, Egypt, Germany, Indonesia, Singapore, UAE, UK, and USA, as well as institutional partnerships with about 300 counterpart organizations in almost 100 countries, CII serves as a reference point for Indian industry and the international business community.

Confederation of Indian Industry
The Mantosh Sondhi Centre, 23, Institutional Area
Lodi Road, New Delhi - 110 003, India
Phone: 91 11 45771000/ 24629994-7
Email: info@cii.in
Web: www.cii.in

About CDT

Committed to empowering a Digital First India, CII is committed to nurture and catalyze India Inc's wholesome Digital Transformation through the CII-Centre for Digital Transformation. As a champion of digital transformation, CDT is powered by the responsibility of enriching and accelerating the technology journey of its members. Since its formation Centre for Digital Transformation has been creating awareness about benefits of various technologies and engaging with industry to help them in their Digital Transformation journey to help them become globally competitive.

CAPACITY BUILDING

CDT (Centre for Digital Transformation) enhances digital literacy and technological skills through its capacity-building training programs and technology webinars. These initiatives cover topics like digital transformation, Industry 4.0, cybersecurity, cyber law, blockchain, and emerging technologies, benefiting organizations across various sectors.

The webinars feature insights from technology and industry experts, providing valuable knowledge on the latest trends. CDT's capacity-building programs, organized in collaboration with premier institutes and industry experts, are tailored to meet the specific needs of different industries, ensuring participants gain relevant and high-quality training.

Through these efforts, CDT plays a key role in driving digital transformation and innovation, helping organizations stay competitive in a rapidly evolving technological landscape.

CII - Tata Communications Centre for Digital Transformation
249-F, Sector 18, Udyog Vihar, Phase IV
Gurugram, Haryana 122 015, India
Phone: +91 124 401 4060 - 67
Email: contact.cdt@cii.in
Web: ciict.com

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned member firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, HR, risk and internal audit through a network of more than 90 offices in over 25 countries.

Named to the 2024 Fortune 100 Best Companies to Work For® list for the past 10 years, Protiviti has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti is a wholly owned subsidiary of Robert Half Inc. (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Sandeep Gupta
Managing Director
sandeep.gupta@protivitiglobal.in
+91 9702730000

Vaibhav Koul
Managing Director
vaibhav.koul@protivitiglobal.in
+91 9819751715

Aju Sebastien
Managing Director
aju.sebastian@protivitiglobal.in
+91 9818286225

Sarita Padmini
Senior Director
sarita.padmini@protivitiglobal.in
+91 9953043552

Sahil Chander
Senior Director
sahil.chander@protivitiglobal.in
+91 8800490154

Protiviti India Offices

Bengaluru
Umiya Business Bay - 1, 9th Floor
Cessna Business Park, Outer Ring
Road, Kadubeesanahalli, Varthur
Hobli Bengaluru – 560 049
Karnataka, India
Phone: +91.80.6780.9300

Bhubaneswar
1st floor, Unit No 104, 105, 106
Utkal Signature, Chennai Kolkata
Highway Pahala, Bhubaneswar
Khordha - 752 101
Odisha, India

Chennai
10th Floor, Module No. 1007
D Block, North Side, Tidel Park
No. 4, Rajiv Gandhi, Salai,
Taramani, Chennai - 600 113
Tamil Nadu, India
Phone: +91.44.6131.5151

Coimbatore
TICEL Bio Park, (1101 - 1104)
11th floor Somaiyapalyam
Village, Anna University Campus,
Maruthamalai Road, Coimbatore
North Taluk, Coimbatore – 641046
Tamil Nadu, India

Gurugram
15th & 16th Floor, Tower A,
DLF Building No. 5, DLF Phase III
DLF Cyber City,
Gurugram – 122 002
Haryana, India
Phone: +91.124.661.8600

Hyderabad
Q City, 4th Floor, Block
B, Survey No. 109, 110 &
111/2 Nanakramguda Village
Serilingampally Mandal, R.R. District
Hyderabad – 500 032
Telangana, India
Phone: +91.40.6658.8700

Kolkata
PS Srijan Corporate Park,
Unit No. 1001 10th & 16th Floor,
Tower - 1, Plot No. 2 Block - EP &
GP Sector-V, Bidhannagar
Salt Lake Electronics Complex
Kolkata –700 091,
West Bengal, India
Phone: +91.33.6657.1501

Mumbai
1st Floor, Godrej Coliseum
A & B Wing Somaiya Hospital Road
Sion (East) Mumbai – 400 022
Maharashtra, India
Phone: +91.22.6626.3333

Noida
Windsor Grand, 14th & 16th Floor
1C, Sector - 126 Noida
Gautam Buddha Nagar- 201313
Uttar Pradesh, India
Phone: +91.120.697.2700

Notes

Notes

Disclaimers

Published by Confederation of Indian Industry (CII),
The Mantosh Sondhi Centre; 23, Institutional Area,
Lodi Road, New Delhi 110003, India,
Tel: +91 11 45771000;
Email: info@cii.in; Web: www.cii.in

Face the Future with Confidence®