

SAFEGUARDING FROM WITHIN: INSIDER RISK MANAGEMENT IN INDIA

A Study on Strategies to Identify,
Govern and Mitigate Insider Risk
in the age of AI

CONTENTS

Foreword	03
Preface	05
Introduction	06
Insider Risk Types & Challenges	08
Corporate Perspectives on Insider Risk Management in India – Study Findings	12
Way Forward – Building a Mature Insider Risk Program	18
Call to Action	28
Conclusion	30
Additional Resources	32
References	34
Our Recent Reports	35
About Microsoft	36
About Protiviti	37

Foreword



Sandeep Gupta
Managing Director
Protiviti Member Firm for India

In today's rapidly evolving digital landscape, the nature of risk has transformed. Insider threats—once considered rare and isolated—have emerged as persistent and complex challenges for organizations across sectors. As India embraces digital transformation and generative AI tools reshape the workplace, the need for proactive, intelligent, and privacy-conscious insider risk management has never been more urgent.

This whitepaper, a collaborative effort between Protiviti and Microsoft, aims to illuminate the insider risk landscape in India. It draws on real-world insights from leading Indian enterprises across banking, healthcare, pharmaceuticals, technology, and other sectors. Their candid perspectives and shared experiences have been instrumental in shaping the findings and recommendations presented here.

We extend our heartfelt gratitude to the clients and organizations who participated in this study. Your openness and commitment to improving security practices have enriched this research and helped create a resource that is both practical and forward-looking.

We also wish to thank Microsoft for their unwavering support and partnership. Their cutting-edge solutions have provided a powerful lens through which to examine and address the multifaceted nature of insider threats. Their contributions have been vital in demonstrating how technology, when thoughtfully applied, can empower organizations to detect, prevent, and respond to risks with agility and confidence.

Importantly, insider risk management is no longer a discretionary initiative—it is a regulatory imperative. With frameworks such as SEBI's Prohibition of Insider Trading Regulations, the Digital Personal Data Protection Act (DPDPA) 2023, and sectoral mandates from RBI, IRDAI, Telecommunication Act, Indian organizations are expected to demonstrate robust internal controls that safeguard sensitive data and uphold compliance standards.

Beyond regulatory alignment, effective insider risk management is foundational to customer trust. In industries where data sensitivity is paramount, clients expect their information to be handled with integrity, discretion, and accountability. By proactively managing insider risks, organizations not only reduce exposure but also reinforce their reputation as responsible and trustworthy custodians of data.

As you read through this paper, we hope it sparks meaningful conversations within your organization and inspires action. Insider risk is not just a technical issue—it is a business imperative. By investing in the right tools, processes, and culture, Indian enterprises can safeguard their most valuable assets, meet regulatory expectations, and build enduring trust with their customers.



Insider risk is no longer a hidden threat—it's a strategic priority. In the age of AI and data-driven enterprises, protecting from within is not just about security, it's about trust, compliance, and resilience.



Preface



Nishan DeSilva
Partner Group Product Manager,
Microsoft



Ashish Adhikari
Principal Product Manager,
Microsoft



Danika Loadholt
Principal Group Product Manager,
Microsoft

For today's leaders, insider risk has moved from a peripheral concern to a boardroom priority. In India's fast-digitizing economy, threats from within—whether intentional, accidental, or through compromised identities—pose a direct challenge to regulatory compliance, brand reputation, and operational continuity. Hybrid work, multi-cloud adoption, and the rise of AI have amplified this risk, expanding both its scale and complexity.

Addressing it effectively requires visibility, speed, and governance at the enterprise level. Microsoft Purview Insider Risk Management delivers these capabilities—detecting subtle behavioral patterns, correlating signals across HR, security, and collaboration platforms, and embedding privacy safeguards that preserve trust while enabling decisive action.

The trust of employees, customers, and regulators is now also tested in the AI era. Employees can unintentionally expose sensitive information via AI tools, and AI itself can act as a “digital insider.” Purview's AI risk indicators allow organizations to govern both human and AI-driven activities with equal rigor, ensuring no blind spots in oversight.

For executives, the imperative is clear: insider risk management is not just a security function—it's a strategic lever for resilience. By integrating advanced tools like Purview into core operations, organizations can protect their data, preserve stakeholder confidence, and ensure that trust remains their most valuable asset.



Introduction

Insider risk—the potential for a trusted individual to misuse their authorized access, whether **maliciously** or **unintentionally**, in a way that negatively impacts the organization—has become a **critical security concern**. In India's fast-digitizing enterprises, **data is now one of the most valuable strategic assets**, and insider incidents—ranging from inadvertent leaks to deliberate internal fraud—can cause severe operational, reputational, and regulatory damage.

Recent cases in India have shown how internal actors can exploit **gaps in visibility and control**, quietly diverting sensitive resources or data over extended periods. These incidents underscore the urgent need for **comprehensive safeguards** that combine **data classification**, **access governance***, and **behavioral monitoring** to detect and mitigate misuse before it escalates.

Adding to the challenge is the **rapid adoption of generative AI (GenAI) tools** in the workplace. Employees may **unwittingly feed confidential information** into AI chatbots or generate content that violates corporate policies, intellectual property protections, or regulatory requirements. In fact, **84% of organizations believe they need to do more to protect against risky employee use of AI¹**. This new AI dimension magnifies insider risk, requiring companies to rethink how they **govern information use** in a hybrid and AI-driven business environment.

¹ <https://techcommunity.microsoft.com/blog/microsoft-security-blog/insider-risk-management-empowering-risky-ai-usage-visibility-and-security-invest/4298246>

From an **India-specific standpoint**, the urgency is amplified by:

- The **BFSI sector**, where **SEBI (Prohibition of Insider Trading) Regulations** mandate strict control of **Unpublished Price Sensitive Information (UPSI)***
- The **healthcare and pharmaceutical sectors**, bound by **patient data protection** and **clinical trial confidentiality**
- The **technology and IT services sectors**, where **IP theft, client data protection, and export control compliance** are critical
- The **Digital Personal Data Protection Act (DPDPA) 2023**, which places legal obligations on companies to safeguard personal data and prevent unauthorized disclosures, with significant penalties for violations*

Against this backdrop, Indian organizations are expected not only to protect sensitive data but also to demonstrate **regulatory compliance**, maintain **market trust**, and ensure **business continuity**.

This whitepaper adopts a **problem-solution** methodology. It begins with an analysis of the

insider risk landscape in India, supported by insights from interviews with multiple Indian corporations that reveal common gaps and challenges. It then examines different categories of insider risks and showcases strategies that can help address these challenges.

Our goal is to enable organizations to:

- Build awareness of the full spectrum of insider risks
- Implement a **proactive, trust-based** approach to data governance
- Leverage **technology and process controls** to detect, prevent, and respond to risks effectively

By fostering understanding and encouraging the adoption of comprehensive strategies, companies can better protect sensitive data, **prevent costly incidents**, and **uphold compliance**—even as new risks emerge in the AI era. To support this, we conclude with **practical next steps**—including a webinar, demo, and trial—and provide additional resources to help organizations begin implementing these recommendations.”

84%

of organizations believe they need to do more to protect against risky employee use of AI

24%

of organisations feel prepared to manage privacy concerns associated with emerging technologies (such as AI/ML, IoT Blockchain)²

* More details can be shared on request.

² <https://www.protiviti.com/in-en/state-of-data-privacy-in-india-survey-report-2024>



Insider Risk Types & Challenges

Insider threats are more frequent than many realize. According to Microsoft's latest security insights, **63% of data breaches involve an insider** in some capacity¹ – whether it's a well-meaning employee accidentally sharing confidential data or a malicious actor exploiting their access for personal gain. Organizations worldwide are increasingly concerned; in one survey, 93% of companies expressed worry about insider risks. Indian businesses, facing massive data growth and strict regulatory expectations, are no exception. Yet, many firms lack dedicated measures to address insider risk, creating a dangerous gap in their cyber defenses.

As Indian enterprises expand in scale, digitize operations, and adopt cloud and AI-driven workflows, the potential for insider-driven incidents has grown exponentially. Insider risk can stem from malicious intent, negligence, or compromise by external actors—and in many cases, these categories overlap.

¹ <https://techcommunity.microsoft.com/blog/microsoft-security-blog/insider-risk-management-empowering-risky-ai-usage-visibility-and-security-invest/4298246>

The key types of Insider risk are as below:

1. Malicious Insider Risks

Malicious insiders intentionally misuse their access to harm the organization—motivated by personal gain, revenge, or external influence.

Use Case	Description	Example Scenario
IP Theft	Exfiltration of source code, designs, or product strategies	Developer downloads AI model code before joining a competitor
Sabotage	Intentional disruption or destruction of data, systems, or services	Fired IT admin deletes database back-ups and encrypts config files
Corporate Espionage	Insider shares secrets with competitors or foreign entities	R&D scientist leaks drug trial data to an overseas lab in return for payment
Policy Circumvention	Bypassing DLP, logging, or access con-trols to hide malicious activity	Admin disables endpoint security agents before transferring files
UPSI Leakage (Intentional)	Pre-release financials or strategic disclo-sures leaked for trading or influence	Finance staff emails draft earnings to external trader ahead of board release
Obfuscated Data Transfer	Using encrypted ZIPs, renamed files, or steganography to hide exfiltrated data	Insider hides board data in an image file and uploads to GitHub
Collusion with External Actors	Working with threat groups or activist networks	Internal resource leaks vulnerability reports to hacktivists

2. Negligent Insider Risks

Negligent insiders cause risk through carelessness, ignorance, or poor digital hygiene—often with no intent to harm.

Use Case	Description	Example Scenario
Unintentional Data Leakage	Accidental disclosure of sensitive docu-ments or credentials	Employee emails salary file to the wrong client
Shadow IT Usage	Use of unauthorized tools or cloud ser-vices	Staff uploads proposal to personal Dropbox to work from home
Poor Security Hygiene	Weak passwords, no MFA, ignoring soft-ware updates	Password reused across apps results in credential stuffing
Misdelivery of UPSI	Accidentally sharing financials, M&A da-ta, or investor presentations	Junior analyst attaches Q3 financials to external email instead of press kit
Unsecured Collaboration Tools	Use of WhatsApp/Slack/Teams with ex-ternal guests for sensitive data	Project decks shared via WhatsApp without encryption
Chatbot/GenAI Over-sharing	Uploading sensitive business data into public AI tools	Legal counsel pastes acquisition term sheet into GenAI platform
Screenshots/Print Leakage	Taking screenshots or printed copies of sensitive information	Staff prints board notes and leaves them unattended in a café

3. Compromised Insider Risks

These insiders are not acting maliciously or negligently—but their identities or systems are compromised and used as attack vectors.

Use Case	Description	Example Scenario
Credential Theft / ATO	External attacker uses stolen cre-dentials for insider-level access	Phished CFO credentials used to initiate wire fraud
Malware Infection	Insider's endpoint spreads malware unknowingly	Employee clicks on malicious link, trigger-ing ransomware in corporate network
Business Email Com-promise (BEC)	Account takeover or impersonation for fraud	Attacker sends fake invoice from a com-promised vendor email
Privileged Access Misuse	Attacker escalates privileges using insider's access	Compromised user credentials allow ac-cess to source code repositories
GenAI Tool Misuse via Compromise	AI-based assistant used to extract insider data unknowingly	Attacker prompts LLM-integrated tool with sensitive internal queries
Delayed Insider Ac-cess (Post-Exit)	Ex-employees retain access or data post-exit	Former employee downloads roadmap documents using unrevoked access

Core Challenges in the Indian Context

1. Lack of Comprehensive Visibility

- Many Indian enterprises operate in **multi-cloud and hybrid environments**, but lack integrated visibility across platforms, collaboration tools, and endpoints.

2. Weak Data Governance for Sensitive Information

- In BFSI, **UPSI handling procedures** are often manual and prone to oversight.
- In healthcare and pharma, **patient data and trial data confidentiality** are not consistently monitored across all endpoints and apps.

3. Inadequate Insider Risk Detection Capabilities

- Traditional SIEMs detect external threats well but are **not optimized for insider behavior analytics**.

4. Regulatory Compliance Pressures

- **SEBI (PIT) Regulations** mandate stringent UPSI control for listed companies.
- **DPDPA 2023** imposes penalties for unauthorized personal data processing.
- Sectoral regulators like **RBI** and **IRDAI** require customer data protection and breach notification.

5. Cultural and HR Sensitivities

- Balancing **employee trust** with effective monitoring remains challenging, leading some companies to **avoid proactive insider risk programs** until an incident occurs.

The Risk Amplification from GenAI Adoption

The introduction of **Generative AI** in the workplace adds a new dimension to insider risk:

- Employees can inadvertently **feed confidential corporate, financial, or R&D data** into AI models, leading to **uncontrolled data persistence**.
- AI-generated outputs may inadvertently **include sensitive internal content** or violate regulatory disclosure timelines.
- Indian BFSI, pharma, and tech firms face heightened **compliance and reputational risks** when AI tools are used without governance frameworks.

Many Indian organizations are unprepared, focusing more on external threats and compliance over insider risk management. We investigated multiple Indian companies' current approaches to insider risk management for more insights.

Negative consequences of insider incidents can be severe



The current Indian corporate landscape can present a perfect storm with rapid digitization, increasing data volumes, dispersed workforces, and the adoption of AI—without a corresponding maturity in insider risk management. This creates an urgent need for integrated solutions that combine policy, technology, and awareness programs to address insider risks proactively.



03

Corporate Perspectives on Insider Risk Management in India – Study Findings

To understand the current state of **insider risk awareness, challenges, and maturity**, we conducted in-depth interviews with senior leaders from **Indian enterprises** spanning across **banking and financial services (BFSI), healthcare, pharmaceuticals, FMGC, Airlines, Technology and others**. These uncovered consistent trends in insider risk management practices. Despite differences in size and industry, each organization had similar strengths and clear opportunities in how they handle insider threats—Many Indian organizations are unprepared, focusing more on external threats and compliance over insider risk management. We investigated multiple Indian companies' current approaches to insider risk management for more insights.

Key Findings: Gaps in Security without Insider Risk Management

Given the current state of many Indian corporations relying only on basic Security Operations Center (SOC) monitoring and Data Loss Prevention (DLP) solutions, several critical gaps emerge when compared to organizations that leverage a dedicated Insider Risk Management (IRM) program. Below we outline the findings, each highlighting how the absence of specific IRM features can leave companies vulnerable:

01



Basic Controls, No Advanced Analytics

Organizations have solid foundational controls (logs, DLP) but lack the anomaly detection and user behavior analytics that IRM tools provide, meaning subtle insider warning signs can be missed.

02



Siloed & Reactive Approach

Monitoring and response are confined to IT/SOC teams with minimal HR or legal input. Without IRM's cross-functional workflows and system integrations, off-boarding lapses and context from HR events can slip through the cracks.

03



Limited Privacy Safeguards

Conventional tools reveal user identities in alerts, risking investigator bias. IRM solutions pseudonymize usernames by default - a protection absent in basic setups.

04



Emerging Risk Channels Unmonitored

Use of generative AI tools, risky browser behaviors, and cloud app uploads aren't effectively tracked by baseline SOC/DLP solutions, leaving modern data leakage avenues wide open.

9 Key Findings: How Missing IRM Features Leave Companies Vulnerable

01

Basic Controls in Place – Ready for Advanced Monitoring

02

Clean Track Record – Need to Reinforce Vigilance Proactively

03

Strong Security Culture – Needs to Expand into a Dedicated Insider Risk Program

04

Siloed Efforts – Need for Cross-Department Collaboration

05

Lack of User Anonymity Protections – Risk of Biased Investigations

06

No Defined Indicators or Triggers for Insider Risk Activities

07

Limited Integration and Context – Limitations of Basic DLP/SOC Solutions

08

Emerging Risks Untracked – (Generative AI Usage)

09

Risky Browser and Cloud Usage – Lack of Visibility with Basic Tools

1. Basic Controls in Place – Ready for Advanced Monitoring

All firms have fundamental security controls like system log monitoring and DLP rules guarding their data. This provides a solid foundation – for example, banks block unacknowledged USB usage and external email uploads unless expressly approved. However, none of the companies currently use advanced behavioral analytics or dedicated insider risk tools, so their monitoring is mostly manual and rules-based. This means they **lack the intelligent detection capabilities that an IRM solution would offer**, such as anomaly detection or AI-driven user behavior analytics to catch subtle warning signs that traditional rule-based tools might miss. In other words, they have the basics covered, but they are now well-positioned to benefit from modern insider threat monitoring solutions that **proactively identify risky patterns** (just because you have basic solutions doesn't guarantee you can detect nuanced insider risks). An IRM platform could introduce automated alerts for unusual user behaviors (e.g. sudden bulk file downloads or off-hours access spikes) which their current tools may not flag.

2. Clean Track Record – Need to Reinforce Vigilance Proactively

Each organization reported **no major insider** incidents in recent memory, which is encouraging. To date, their preventive measures have successfully mitigated the risk of significant insider breaches. Nevertheless, this record of success may inadvertently foster complacency, as limited active monitoring could allow minor policy violations or gradual data leaks to go undetected. Rather than presuming

that the absence of incidents equates to security, these organizations recognize the importance of enhancing their vigilance. Industry research indicates that a substantial proportion of organizations encounter insider threats, with nearly two-thirds reporting multiple malicious incidents within a year; thus, undetected issues may still be present. By proactively investing in more robust insider risk detection, organizations can identify and address potential concerns at an early stage, mitigating escalation into major incidents. Ultimately, by prioritizing proactive strategies over reactive responses, organizations can convert a strong compliance history into a foundation for sustainable security, ensuring that unseen risks are adequately managed.

3. Strong Security Culture – Needs to Expand into a Dedicated Insider Risk Program

Multiple companies demonstrated a robust overall cybersecurity posture. They enforce strict access controls (role-based access, periodic privilege reviews, multi-factor authentication) and align with industry standards like ISO 27001 for information security. These practices create a strong culture of security and compliance to build upon.

The key opportunity here is to develop a focused insider risk management program that knits these existing practices together. Currently, none of the firms has a formal insider risk team or software platform, and insider risk handling tends to be siloed within IT or security operations. This means even with good general security hygiene, there isn't a unified strategy to specifically anticipate and mitigate insider threats.

Implementing an Insider Risk Management (IRM) program would establish well-defined procedures, specialized tools, and clear accountability for addressing internal threats. Such a program integrates various controls—including access management, data loss prevention, and human resources policies—and ensures that indicators of insider risk are effectively identified and managed. While fostering a robust security culture provides a solid foundation, it is essential to supplement this with a dedicated insider risk framework to adequately address challenges that may not be detected by standard security measures.

4. Siloed Efforts – Need for Cross-Department Collaboration:

In current practice, IT security teams and Human Resources (HR) departments have yet to achieve close collaboration on insider threat scenarios. For example, one organization reported that an ex-employee's account remained active even after their departure, revealing a deficiency in off-boarding procedures.

The current process reveals a disconnect between HR events (such as terminations or resignations) and timely communication with IT security for appropriate follow-up actions, and vice versa. While it is encouraging that these organisations already have the foundational elements—policies, tools, and awareness—in place, there remains a need for an integrated workflow. Implementing a cross-functional insider risk program that **links HR events (including resignations, disciplinary procedures, or policy violations) to prompt IT monitoring and response** can greatly strengthen protection against insider threats. Contemporary IRM solutions support this by correlating relevant signals and establishing workflows that engage

all necessary stakeholders: for example, **associating a resignation documented in HR systems with increased data activity alerts and enabling coordinated review and action from SecOps, HR, and legal teams.** Adopting this approach enables organisations to shift from a reactive, retrospective posture to a proactive and holistic strategy, in which potential insider risks are detected through interdepartmental collaboration. In summary, although baseline policies exist, they must be unified within an IRM program to ensure effective, joint efforts between HR and IT.

5. Lack of User Anonymity Protections – Risk of Biased Investigations

Another gap in the current setups is the **absence of user anonymity during insider incident alerts and investigations.** In the companies' existing tools, if a security alert is generated, it likely identifies the employee directly. This can introduce bias – investigators might treat cases differently based on knowing who the person is (for instance, a high-performing employee might get the benefit of the doubt, whereas a new or unrelated employee's actions might be scrutinized more strictly). An effective IRM solution addresses this by **anonymizing or pseudonymizing user identities by default in alerts.** Insider threat solutions are built with privacy by design: users under investigation are shown with randomized aliases to investigators, and only authorized reviewers can de-anonymize if necessary. The companies not using IRM currently lack this feature, meaning any internal investigations could be subjective. Implementing a solution that can hide the usernames (until a certain stage of investigation or with proper approval) helps promote objectivity and fairness in insider risk reviews.

6. No Defined Indicators or Triggers for Insider Risk Activities

In the absence of an IRM platform, the companies rely on basic alerts (like DLP rule violations or manual observations) to catch risky activities. They don't have a systematic way to look for patterns of behavior or triggering events that might indicate elevated insider risk. By contrast, **Insider Risk Management solutions define specific risk indicators and triggering events that feed into alerts.** For example, IRM policies can be configured to watch for things like a sudden spike in file downloads, repeated attempts to access sensitive files, copying data to personal cloud storage, or even HR events like a resignation, as triggers that elevate a user's risk score. Without this, the current monitoring might only catch what is explicitly disallowed (per DLP rules) but miss compound behaviours that are individually benign yet collectively suspicious. In essence, **these companies lack the rich library of insider risk indicators that an IRM system provides.**

An IRM program would allow them to set up "tripwires" for insider activity – for instance, if an employee has a poor performance review (HR event) and starts downloading many documents (IT event), and then tries to disable security software, those together would trigger an alert. Currently, such correlations aren't being made. This is a challenge: not having defined insider risk triggers means potential red flags (like mounting data exfiltration over time, policy evasions, or unusual work-hour activity) might not be detected until it's too late. Adopting IRM would introduce those analytics-driven alerts to catch problems early. In short, **the gap is the lack of an "early warning system"**

for insider behavior, which IRM's combination of signals and analytics would fulfill by automatically generating alerts when certain risk thresholds are crossed.

7. Limited Integration and Context – Limitations of Basic DLP/ SOC Solutions

Many organizations' security tools lack integration across data sources and don't use context from non-IT systems like HR data, missing critical events such as resignations or demotions. Basic SOCs rely on logs, while DLP focuses on content violations—neither gives a full picture of user behaviour or risk.

DLP alone often fails to spot gradual insider threats, as it lacks behavioural context. IRM platforms address this by correlating content with user actions, intent, and employment status, providing a more comprehensive view.

Ultimately, insufficient integration leads to fragmented security and increases the risk of missing complex insider threats. IRM solutions unify signals and workflows, helping security teams detect issues that span multiple systems.

8. Emerging Risks Untracked – (Generative AI Usage)

A novel challenge that companies are beginning to face is the misuse of **Generative AI tools** by employees – for example, an employee might input proprietary code or data into an AI chatbot or use AI-based writing assistants to generate content that could include sensitive information. With only basic controls in place, these firms likely have **no visibility or policies around the use of generative AI or other**

new technologies. This is becoming an important gap: if employees use external AI services, they might inadvertently expose confidential data or violate compliance policies, and a traditional DLP might not catch it if it's done through web channels or API calls not monitored. The companies not using IRM don't have any such specialized detection. The risk of not tracking AI usage is that a whole vector of data leakage and inappropriate behavior (like an employee asking an AI model to write code using proprietary algorithms) goes completely unseen. **This gap can lead to significant blind spots** in an era where AI tools are ubiquitous. By not having an IRM or equivalent solution, these organizations may not realize if sensitive documents are being fed into GenAI platform, if employees are using AI to generate content that violates policies, or if someone is using AI agents to systematically scrape or export data. Thus, incorporating IRM would help set up monitoring and controls for these new AI-related risks (as evidenced by IRM's new AI risk indicators), whereas currently they remain unaddressed.

9. Risky Browser and Cloud Usage – Lack of Visibility with Basic Tools

Finally, there is a challenge around web and cloud-based exfiltration that basic SOC and DLP setups struggle with. If an employee decides to upload files to a personal cloud drive (like Google Drive or Dropbox) via a web browser, or uses a personal webmail to send data out, a standard on-prem DLP might not catch that – especially if it happens over an encrypted web session or outside the corporate network. Likewise, if an employee uses a “risky browser” (for

example, an unauthorized browser or one with insecure extensions) to handle company data, the organization might have no insight into that activity. Currently, these companies do not have specialized tools to monitor **risky browser behaviors** (such as copying data from a secure system and pasting into a web form, or using a browser that bypasses certain controls). An IRM solution can help fill this gap. Without IRM, these companies have **limited visibility into cloud service interactions and browser-based actions** beyond what their network proxy or gateway logs might show (if they even monitor those in real-time). Data exfiltration via cloud storage or web channels is a major insider threat vector, and relying on basic SOC monitoring means many of these events would blend in with normal traffic. The gap here is essentially **the lack of cloud-aware, user-centric monitoring**. Basic DLP might be installed on corporate email and devices, but it might not cover, say, an employee on a BYOD device uploading files through a web browser. IRM, being integrated with cloud ecosystems and endpoint signals, would provide alerts on such risky behavior. Therefore, not having IRM leaves the organization exposed to stealthy data exfiltration that leverages browsers or unsanctioned cloud apps. Adopting IRM would introduce tailored detection for these scenarios (for example, alerting if an employee normally using Edge suddenly installs another browser and downloads a lot of files). In summary, **any feature that IRM highlights (like monitoring AI usage, browser activity, unusual file movements, etc.) currently corresponds to a challenge for these companies because their basic tools do not capture that information.**

The analysis uncovered multiple gaps in the insider threat defenses of companies not using a modern Insider Risk Management solution. While their baseline security controls and strong security culture are valuable, these gaps – ranging from missing behavioral analytics and cross-department workflows to lack of privacy safeguards and blind spots in new technology usage – put them at risk. Every capability that an IRM program provides (holistic user activity correlation, privacy-by-design investigations, integration of HR and IT data, advanced risk indicators, and coverage of emerging risk channels) translates into a corresponding weakness for an organization that relies solely on a traditional SOC and DLP. Addressing these findings by implementing an IRM solution would help the companies move from a reactive posture to a proactive and resilient insider risk management strategy, closing the gaps identified above and strengthening their overall security posture.



Way Forward – Building a Mature Insider Risk Program

Based on the challenges and gaps identified through our research and interviews, it is clear that **Indian enterprises require a multi-layered insider risk management strategy** that integrates people, process, and technology.

The objective is not only to **prevent insider incidents** but also to **foster a trust-based, proactive culture** where risks are identified and mitigated before they cause damage.

Components of a Mature Insider Risk Program

1. Clear Ownership and Governance

- Establish a cross-functional Insider Risk Committee with representation from Security, HR, Legal, Compliance, and Business Units.
- Assign a single accountable owner responsible for the overall insider risk strategy and execution.

2. Risk Categorization and Prioritization

- Classify insider risks into Malicious, Negligent, and Compromised categories.

- Identify high-value data assets—such as UPSI, intellectual property, patient records, and source code—and apply enhanced monitoring and protection controls.

3. Policy and Process Alignment

- Define UPSI handling Standard Operating Procedures (SOPs) aligned with SEBI (PIT) Regulations for BFSI and listed companies.
- Embed Digital Personal Data Protection Act (DPDPA) 2023 compliance requirements into all personal data governance activities.
- Integrate access governance with joiner–mover–leaver workflows to prevent post-exit access and reduce residual risk.

4. Technical Controls

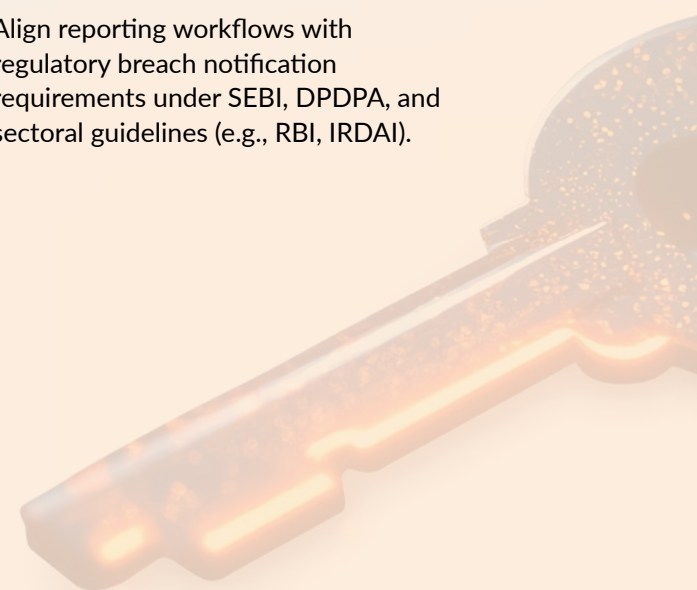
- Deploy tools and controls for prevention of Insider Risk
- Implement role-based access controls with just-in-time privilege escalation to limit exposure.
- Apply policy-based restrictions to secure collaboration tools, cloud storage platforms, and data transfer channels.

5. Awareness and Cultural Integration

- Deliver role-specific training for high-risk functions such as Finance, Legal, R&D, and Investor Relations.
- Promote a culture of responsible data handling that reinforces trust while enabling effective monitoring.

6. Incident Response Integration

- Develop insider-specific incident response playbooks covering detection, investigation, evidence preservation, and escalation.
- Align reporting workflows with regulatory breach notification requirements under SEBI, DPDPA, and sectoral guidelines (e.g., RBI, IRDAI).



Insider Risk Management with Microsoft Purview

Microsoft Purview Insider Risk Management is a comprehensive solution developed to **identify, investigate, and mitigate insider risks** before they escalate into serious incidents. It effectively addresses the aforementioned challenges by offering continuous detection, sophisticated analytics, and integrated workflows, all while ensuring privacy protections are maintained.

Breaches with Insider Involvement

63%

of data breaches involve an insider, highlighting the urgency of managing internal risks.¹

Key Capabilities of Microsoft Purview IRM

01

Advanced Analytics for Subtle Threats

02

Continuous Vigilance Over Complacency

03

Dedicated Insider Risk Program

04

Cross-Departmental Integration (HR + Security)

05

Privacy & Unbiased Investigations

06

Advanced Risk Indicators & Automated Triggers

07

Integrated Signals & Unified Context

08

Monitoring Generative AI Usage

09

Browser and Cloud Exfiltration Visibility

10

Quick Response & Remediation

¹ <https://techcommunity.microsoft.com/blog/microsoft-security-blog/insider-risk-management-empowering-risky-ai-usage-visibility-and-security-invest/4298246>

1. Advanced Analytics for Subtle Threats

Basic security controls (e.g. DLP and log monitoring) lack intelligent behavior analytics. Microsoft IRM introduces built-in risk indicators and machine learning models for anomaly detection, catching nuanced insider risks that rule-based tools might miss. For instance, IRM's cumulative exfiltration detection is capable of identifying patterns indicative of gradual data removal—such as printing a file on one day and subsequently emailing another—by benchmarking user activities against organizational norms. This advanced anomaly detection approach issues automated notifications for atypical behaviors, including sudden mass downloads which may not be detected by standard DLP rules.

2. Continuous Vigilance Over Complacency Actively

The absence of recent incidents may foster a misleading sense of security. IRM facilitates proactive risk monitoring and analytics, enabling organizations to identify latent issues before they escalate, instead of relying on the assumption that “no news is good news.” Microsoft Purview's Insider Risk Analytics can detect potential insider risks even without predefined policies, highlighting areas that require attention (such as frequent*

external sharing of sensitive files by users) and recommending relevant policy implementations. This approach transitions organizations from reactive to proactive risk management—addressing minor policy breaches or data leaks at an early stage, and thereby maintaining rigorous vigilance regardless of incident history.

3. Dedicated Insider Risk Program

Strong general security exists, but no focused insider risk framework. Microsoft IRM provides a purpose-built solution with defined policies, role-based access, and end-to-end workflow for insider risk management. Organizations can create insider risk policies (using templates) tailored to scenarios like data theft by departing users or privileged user risks, ensuring insider threat monitoring isn't siloed in IT but managed as a distinct compliance initiative. The IRM solution integrates various controls (DLP, HR signals, device logs, etc.) into a unified workflow, assigns dedicated risk analyst roles, and enables case escalation to legal or investigation teams (e.g. to eDiscovery) as needed. This formalized approach knits existing security practices into a cohesive insider risk program with clear accountability and process.

4. Cross-Departmental Integration (HR + Security)

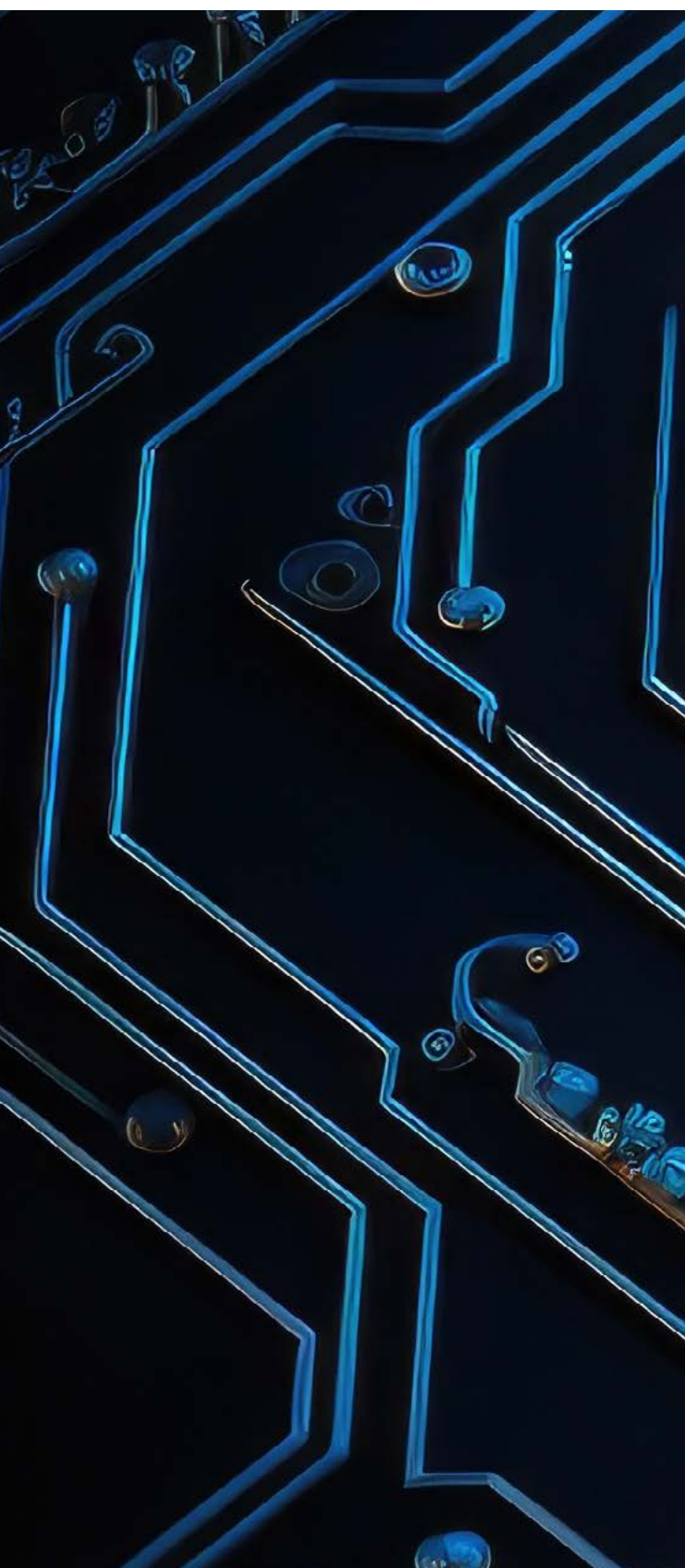
HR events and IT security monitoring are not connected, creating gaps (e.g. account not disabled

after termination). IRM bridges organizational silos by correlating HR events with security signals and enabling collaborative workflows. For instance, Microsoft IRM's HR connector can integrate personnel changes (like resignations or terminations) as triggers – a departing user is automatically brought into scope for heightened monitoring. Moreover, IRM workflows facilitate coordinated review by security, HR, and legal stakeholders: cases can be shared with relevant reviewers, and role-based access ensures each team accesses necessary info while preserving privacy. This means insider risks are managed through a unified process – for example, a documented resignation combined with unusual file downloads will generate an alert for joint HR/SecOps evaluation, transforming a reactive disconnect into a proactive, cross-functional response.

5. Privacy & Unbiased Investigations

Current most tools expose user identities in alerts, risking investigator bias. Microsoft IRM is built with privacy-by-design – users are pseudonymized (anonymized) by default in insider risk alerts and cases. Instead of showing employee names, IRM assigns aliases until a case reaches a stage that warrants identity reveal (with proper authorization). This anonymity feature ensures investigations focus on behavior facts rather than the individual's identity, promoting objectivity. Only authorized personnel can de-anonymize a user if absolutely

* DSPM for AI
(<https://learn.microsoft.com/en-us/purview/dspm-for-ai>)



necessary. By hiding usernames during initial alert triage and investigation, IRM helps eliminate preconceived biases (e.g. treating a high performer more leniently) and enforces fairness in how insider incidents are handled. Additionally, only administrators possessing privilege rights are permitted to monitor user activities; these individuals are responsible for identifying organizationally defined risky activities and ensuring those actions are appropriately tracked.

6. Advanced Risk Indicators & Automated Triggers

Traditional systems often lack defined “tripwires” for risky behavior, relying instead on manual reviews or basic rule-based alerts. IRM offers a comprehensive library of risk indicators and configurable triggers designed to automatically flag suspicious behavioral sequences or event combinations. Organizations can establish policies to identify complex patterns—such as the sequential downgrading of a file’s classification, followed by its download and subsequent exfiltration—which may appear harmless as isolated actions but collectively signal potential risk. Microsoft IRM’s sequence detection capabilities can correlate user activities to infer intent, enabling the generation of high-quality alerts for scenarios that conventional tools may overlook. Furthermore, IRM provides numerous built-in risk indicators (such as mass file downloads or the transmission of sensitive information to personal accounts) and enables threshold-based triggers. These may be linked to contextual factors (for example, a poor performance

review or assignment to a high-risk group) to dynamically adjust risk scoring. In essence, IRM acts as an advanced early warning system, continuously monitoring for predefined risk patterns and issuing alerts when specified thresholds are exceeded—capabilities that were previously unattainable without dedicated analytics-driven solutions.

7. Integrated Signals & Unified Context

*Traditional tools often operate in silos, focusing solely on IT logs or content-based rules, which limits visibility. Insider Risk Management (IRM) correlates signals across *Microsoft 365* services, and third-party systems to deliver a comprehensive perspective on user risk activity.* IRM consolidates data from email, Teams chats, SharePoint/OneDrive, Fabric (Power BI), endpoint devices, and external sources (non-M365 sources that we currently monitor through Microsoft Defender for Cloud Apps integration like Box, Dropbox, Google Drive & AWS) through connectors—such as physical badge access logs or security alerts from non-Microsoft cloud applications. This level of integration allows an alert to encompass various activities; for example, if an employee downloads a customer list from SharePoint and subsequently uploads it to a personal Dropbox account, IRM captures both the file interaction and the cloud upload. Integration with Microsoft Defender for Cloud Apps further enhances IRM by incorporating anomalies from third-party SaaS solutions (e.g., atypical file deletions in Google Drive or suspicious actions within AWS), and identity-related signals (such as Azure AD compromised sign-in detections)

can be included to provide enriched context.

By aggregating these diverse signals, IRM delivers contextual insights beyond those provided by standalone SOC or DLP tools, effectively minimizing blind spots. Security analysts benefit from a unified alert timeline rather than disparate information, facilitating the identification of sophisticated insider threat patterns. Additionally, IRM provides built-in *reports and dashboards* for monitoring insider risk metrics and organizational trends—offering a consolidated view of alerts over time, user behavior, and case statuses. This holistic visibility supports teams in identifying risks that extend across multiple environments and enables measurement of program effectiveness from a single platform.

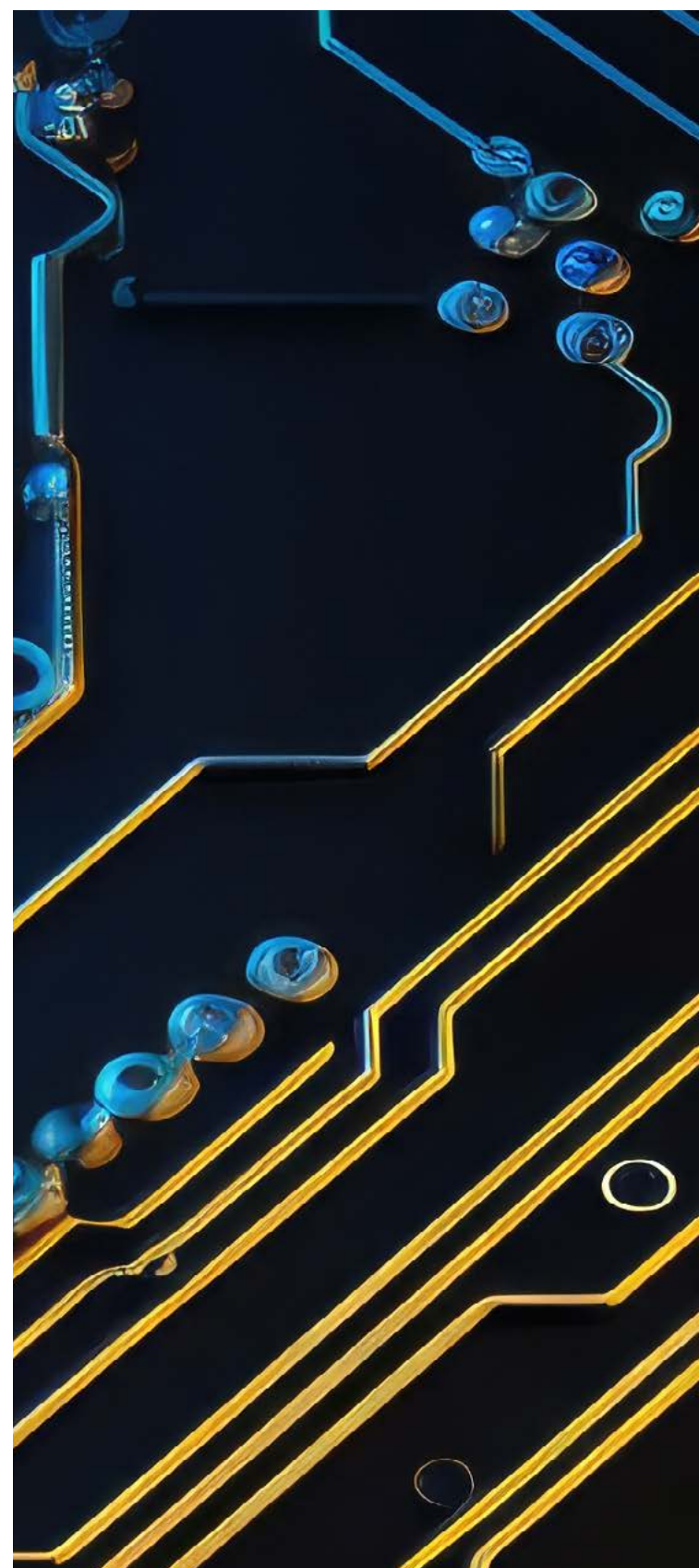
8. Monitoring Generative AI Usage

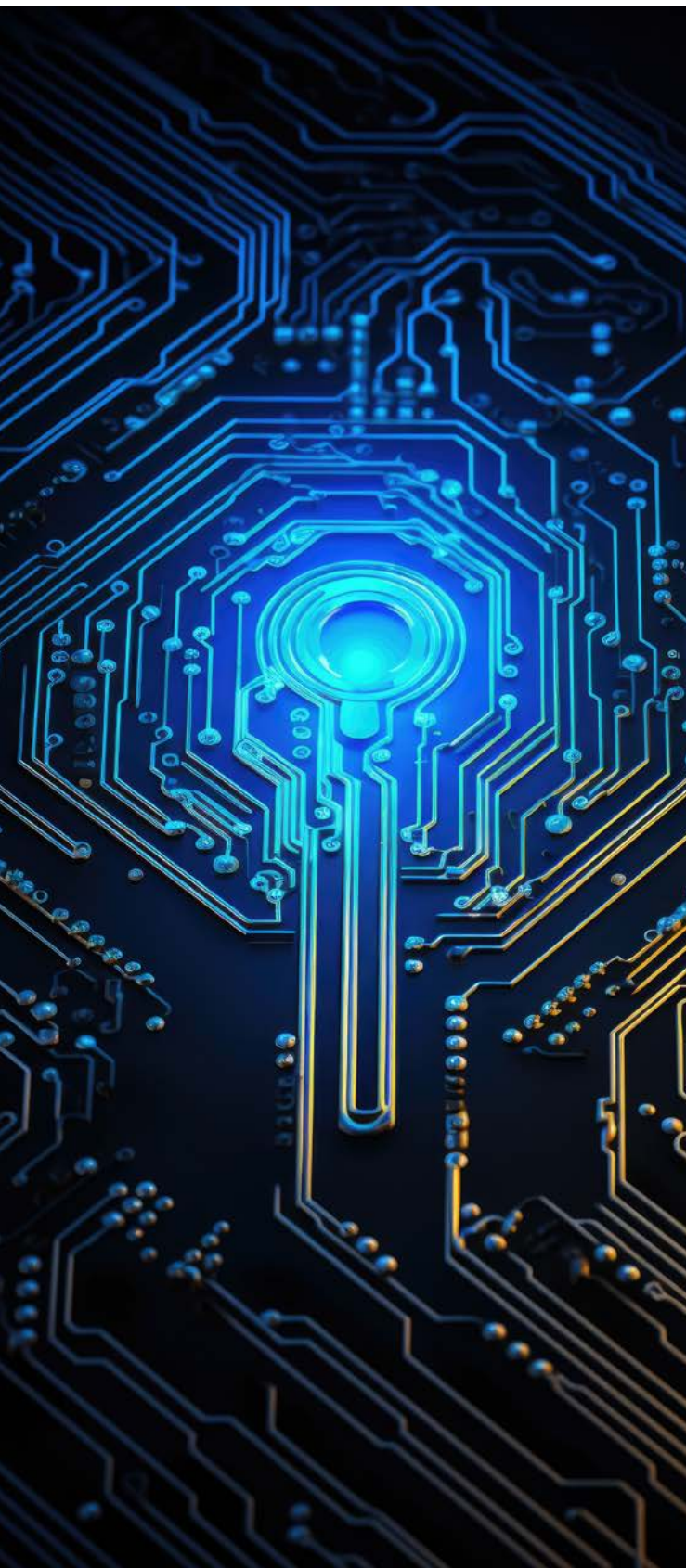
*Emerging risks associated with employees utilizing generative AI, such as entering sensitive data into chatbots, often go undetected by legacy monitoring solutions. Microsoft IRM addresses these evolving threats through specialized “Risky AI usage” indicators and policies designed to detect improper use of AI platforms. Recently introduced in IRM these features can identify when users input confidential information into AI applications including *Microsoft 365 Copilot, ChatGPT, or other AI assistants*, or when AI-generated content contains sensitive organizational data. IRM’s capabilities include detecting both risky prompts—such as attempts to share proprietary code or data with an AI service—and risky outputs where responses contain sensitive file information, thereby alerting*

administrators to potential data leakage via AI channels. By extending detection to encompass shadow AI activity, IRM provides organizations with visibility into risk vectors commonly overlooked by traditional DLP tools. This empowers organizations to leverage AI productivity solutions securely, with assurance that inappropriate usage (such as submitting proprietary information to external AI platforms) will be flagged for administrative review. *(AI-focused signals within IRM also integrate with Adaptive Protection, enabling dynamic adjustment of controls like restricting high-risk users from submitting sensitive queries.)*

9. Browser and Cloud Exfiltration Visibility

Transfers to personal cloud services or the use of unauthorised browsers may bypass conventional on-premises DLP and network monitoring solutions. IRM enhances oversight of potentially risky web and cloud activities, offering comprehensive visibility and proactive alerts for browser-based or cloud-based data exfiltration often overlooked by legacy tools. Microsoft IRM now features a “Risky browser usage” policy (currently in preview) designed to identify unsafe browser behaviours. For example, if an employee typically utilises Edge but unexpectedly installs an alternative browser and downloads a significant volume of data, IRM can detect this abnormality. Additionally, IRM integrates with cloud app security platforms to monitor unsanctioned cloud uploads—such as an employee transferring files to personal Dropbox or Google Drive accounts from a corporate device,





which would prompt an IRM alert via Defender for Cloud Apps signals. The solution examines activities including copying data from secure environments into web forms or exporting large numbers of files to external sites, even when such actions may appear routine. By jointly monitoring endpoints and cloud interactions, IRM addresses visibility gaps associated with browser-based exfiltration and BYOD practices. In summary, activities like using personal email or cloud drives for company file transfers or disabling browser security extensions to circumvent controls are identified and assigned risk scores by IRM, significantly mitigating exposure that previously existed under traditional network or device-level DLP solutions lacking this integrated, cloud-aware approach.

10. Quick Response & Remediation

Once an insider issue is confirmed, swift action is critical. IRM enables or integrates with remediation steps to contain and address the threat. For example, through integration with Azure Active Directory and Microsoft 365, an admin can disable a user's access directly if a malicious insider is identified. IRM can also trigger a notice to the employee – a gentle reminder of policy if the offense is minor (e.g., “You forwarded a confidential file outside the company, which is against policy. Please refrain from doing so.”).

A major advantage of Microsoft's approach is Adaptive Protection, where IRM works hand-in-hand with Microsoft Purview Data Loss Prevention (DLP). If IRM flags a user as high-risk, Adaptive Protection can automatically adjust DLP policies for that user. For instance, a user under investigation might be simply blocked from downloading sensitive files or emailing externally, even if such actions are normally allowed. This dynamic tightening of controls can thwart an insider's attempts in real-time. In other words, IRM not only raises alerts, but it also helps disrupt potential insider attacks as they are unfolding.

Insider Risk Management Workflow: From Policy to Case Resolution

Step 01

Configure Settings & Policies

Setup. An administrator prepares the IRM environment by configuring prerequisites (permissions, roles, and any connectors like HR or third-party integrations) and creating insider risk policies. Policies are created using built-in templates and define which triggering events and risk indicators to monitor (e.g. departing user data theft, data leaks, risky browser or AI usage).

Step 02

Continuous Monitoring & Alert Generation

Detect. Once policies are active, IRM continuously collects and correlates signal data across Microsoft 365 (and connected sources). When user activities meet the policy conditions - for example, a sequence of actions or a threshold of risky activity - IRM automatically generates an alert. The alert (with a unique ID, severity, involved user alias, triggering event, etc.) appears on the IRM dashboard for analysts to review.

Step 03

Alert Triage (Copilot-Assisted)

Triage. A risk analyst triages the alert using the IRM Alert Dashboard. Microsoft Purview IRM includes an Alert Triage Assistant (powered by Security Copilot) to help prioritize and summarize alerts. The analyst can invoke Copilot to summarize the alert, which produces an AI-generated brief of key details (triggered policy, activities, user's risk factors, etc.). The Copilot-driven Alert Triage Agent can also auto-prioritize alerts that pose the greatest risk, highlighting which alerts should be handled first based on content and intent analysis. This guided triage helps the analyst quickly understand the alert's context and decide on next steps.

Step 04

Initial Alert Disposition

Decide. After reviewing, the analyst takes action on the alert. If the alert appears valid (indicative of a real risk), the analyst confirms the alert and escalates it into a case for deeper investigation. (They may either create a new case or add it to an existing case if related.) Conversely, if the alert is a false positive or benign (no real risk), the analyst can dismiss the alert, resolving it without a case. At this point, the alert's status is updated (e.g. "Closed - Dismissed" or linked to an open case).

Step 05

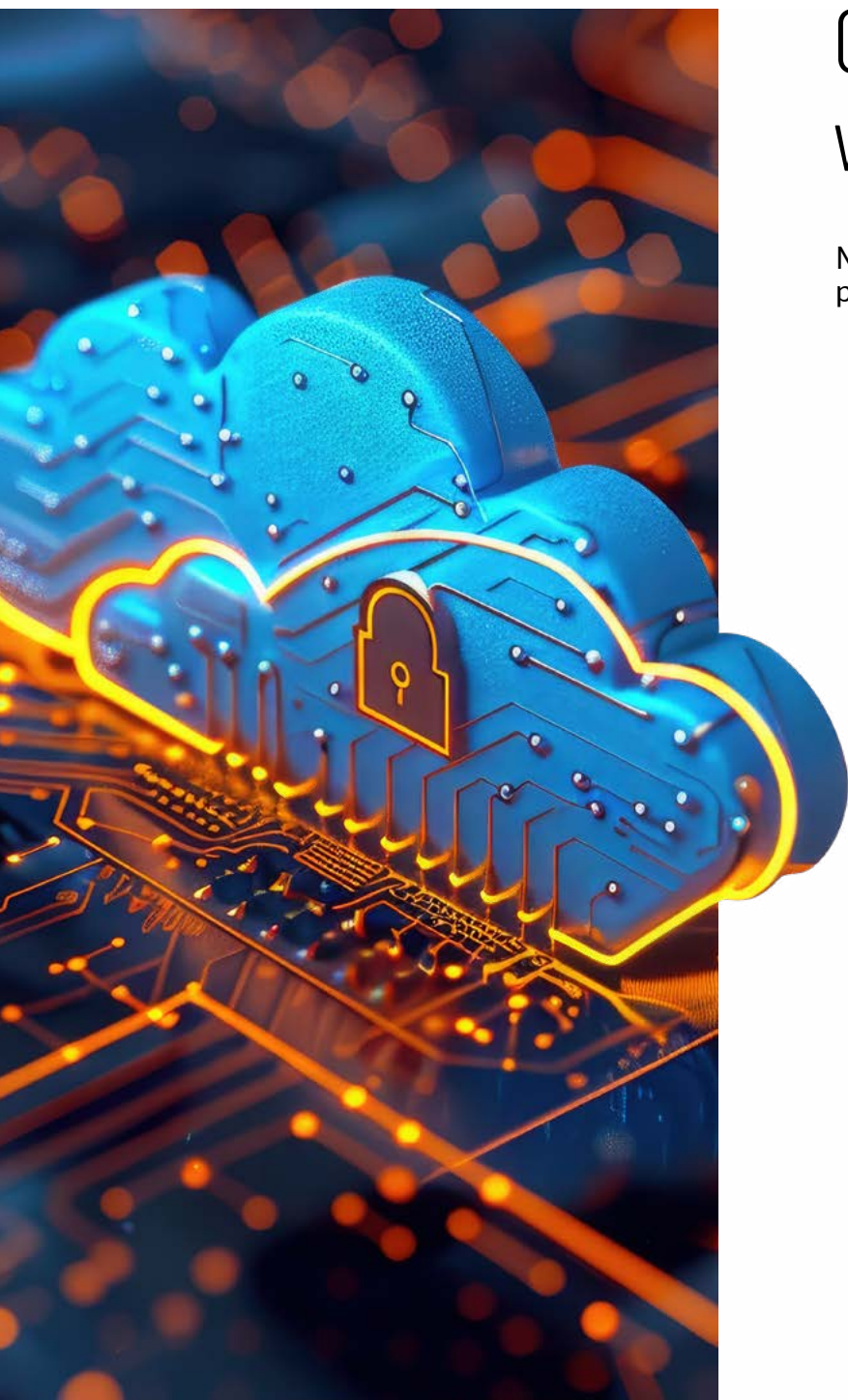
Case Investigation & Analysis

Investigate. For confirmed alerts, an Insider Risk Management case is opened. The case aggregates all related alerts and activities for the user in question, giving investigators a consolidated view of the incident. In the case portal, reviewers can examine a timeline of the user's risk activities, view relevant files or emails involved (through content explorer), and see contextual information (e.g. the user's department, last day of employment, risk history). The system preserves user pseudonymization during investigation to maintain privacy. Investigators analyze the collected evidence and add notes or findings in the case log. This thorough review determines whether the risk is substantiated and what the intent and impact might be.

Step 06

Case Resolution & User Notification

Act. After investigation, the organization takes appropriate action to resolve the case. If the activity was unintentional or minor in impact, the response might be to send a notice to the user - using a pre-approved reminder or warning template. This notification educates the employee on the policy and can direct them to training or guidelines to prevent future incidents. The case is then closed with a benign resolution. If the incident is serious (e.g. malicious data theft or policy violation), the case may be escalated: IRM allows exporting case details to Microsoft Purview eDiscovery for legal investigation, or otherwise involving HR and legal teams for disciplinary action. Throughout this process, audit logs and reports are updated. By the end of this workflow, the risk incident is either mitigated through user coaching or handled through formal processes, and the insider risk program has a record of the outcome for tracking and compliance reporting.



Comprehensive Defense Strategy with Purview Data Security Suite

Microsoft Purview IRM is part of a broader, integrated **data security suite** that provides multiple layers of defense against insider threats:

01

Microsoft Purview Information Protection (MIP):

This tool classifies and labels sensitive data, such as marking documents "Confidential" or "Highly Confidential," and applies encryption or access restrictions. Labels travel with the data, informing other protections like DLP policies and IRM alerts. MIP makes sensitivity visible to deter insiders and prevent accidental leaks by auto-blocking or requiring justification for sending emails with confidential attachments.

02

Microsoft Purview Data Loss Prevention (DLP)

DLP monitors and blocks sensitive data egress in real time, covering endpoints, emails, SharePoint/OneDrive, Microsoft Teams, and some third-party apps via integration. It prevents actions like emailing customer PAN numbers or uploading trade secrets to personal storage. DLP is essential for insider risk management, stopping risky actions as they occur. Integrated with IRM, DLP events feed into a user's risk timeline, and IRM's risk scoring can tighten DLP controls through Adaptive Protection. Together, they detect and block attempts to leak data.

03

Microsoft Purview Data Security Posture Management (DSPM)

While IRM and DLP focus on user activities, DSPM helps by scanning for **misconfigurations or exposed sensitive data** in your environment. Data Security Posture Management (DSPM) helps organizations assess how effectively their sensitive data is protected across environments. By identifying misconfigurations or exposure risks, DSPM enables teams to proactively reduce vulnerabilities. This strengthens the overall security posture, making it significantly harder for insiders or external actors to locate and exploit weak points for unauthorized access

04

Integration with SOC and Compliance

IRM is designed to integrate with broader security operations and compliance workflows. Insider risk alerts and insights can be shared to Microsoft Sentinel (SIEM) or the Defender security portal, ensuring your Security Operations Center has a unified view of threats. Likewise, if your compliance team uses Microsoft's Compliance Manager or Communication Compliance (for monitoring communications for misconduct), those can complement IRM (e.g., serious HR policy violations might raise someone's risk profile). This integration means insider risk management doesn't happen in a silo – it's part of your organization's overall security posture, enriching other tools and processes with insider context.

05

Copilot and agents

Microsoft's **comprehensive strategy** establishes a multi-layered defense system: **deter** through awareness and least privilege, **detect** via continuous intelligent monitoring, and **disrupt** through automated or timely manual intervention. For the Indian companies examined in our study, implementing Purview IRM alongside these additional tools would directly address the deficiencies they identified. They would achieve essential visibility into internal activities, automated identification of risky behaviors (rather than relying on chance or retrospective analysis), and systematic processes for managing incidents in a manner compliant with privacy regulations.



05

Call to Action

Effective insider risk management is achievable with the right solution and strategy. Here are recommended next steps to start strengthening your organization's defenses from the inside out:

01

Request Zero Investment Insider Risk Assessment & Demo:

We offer a **complimentary assessment** of your current insider risk posture, conducted by Protiviti's specialists, followed by a tailored demo of Microsoft Purview IRM on sample scenarios.

This one-on-one session will highlight how IRM would identify and mitigate risks relevant to your business. It's a risk-free way to envision the value of the solution. *(To schedule this, reach out to your Microsoft account team or Protiviti representative – we'll connect you with the technical security experts.)*

02

Get Instant Insights - Using 90 Days Free Trial: Microsoft offers a trial of Microsoft Purview Insider Risk Management (as part of the broader Purview suite). We encourage you to enable this in a pilot capacity. During the trial, you can activate a couple of insider risk policies (for instance, monitor "Departing employees" and "General data leaks") and see what alerts and insights are generated. This

hands-on experience often reveals previously unseen issues (or assures you that things are under control). **Start Your Free Trial**¹ – Experience proactive insider risk management today.

The trial can be set up via your Microsoft 365 admin center, and Microsoft engineers or partners can assist with any questions during the pilot.

FURTHER STEPS

03

Attend the Insider Risk Webinar: Participate in our upcoming webinar on Insider Risk Management in India, co-hosted with Protiviti. This session (available in-person and online) will include a deep dive into Microsoft Purview IRM, live demos of detecting and stopping insider threats (including scenarios with generative AI and

data theft), and a Q&A with experts. It's an excellent opportunity for your team to see the technology in action and get their questions answered.

(Details on date, time, and registration will be provided separately.)

04

Educate Your Team: Leverage Microsoft's free learning resources to upskill your security and compliance team on insider risk management. Microsoft Learn offers step-by-step modules (with labs) on configuring and using Purview IRM. There are also detailed docs and community blogs with best practices.

(See the **Additional Resources** section for links.)

Consider appointing an "Insider Risk Champion" within your organization – someone who can become the subject matter expert by completing these trainings and then lead the internal rollout.

05

Review and Update Policies: Regularly revise policies to align with technological advancements. Define acceptable data use and consequences for breaches, and develop an incident response plan for insider incidents involving HR, Legal, and evidence management. Encourage employees to report suspicious activities and remind them about data protection through training or internal campaigns. Microsoft Purview IRM can produce anonymized trend reports to educate staff.

By taking these steps, you will initiate a comprehensive insider risk program combining **people, process, and technology**. Microsoft and Protiviti are here to support you throughout – from initial assessment to full deployment and training. The key is to start the journey: every day without an insider risk solution is a day of potential undetected exposure.

Get in touch with us to explore our accelerated 6–8 week program—that takes you from discovery to deployment in Insider Risk Management.

¹ <https://aka.ms/MicrosoftPurviewTrial>



CONCLUSION

Insider risk is a significant concern for every organization in India. Whether it stems from an unintentional error by a well-meaning employee or a premeditated act by a rogue insider, the consequences can be equally detrimental – and often more subtle – than external cyber threats. It has become evident that traditional defenses and compliance checklists are insufficient on their own; without dedicated insider risk controls, companies remain vulnerable where they may believe themselves to be secure.

The positive aspect is that with solutions such as Microsoft Purview Insider Risk Management (IRM), organizations can effectively address these challenges. By implementing IRM, you gain the capability to identify early warning signs of potential issues that might otherwise go unnoticed, and take preemptive actions to prevent significant damage. Additionally, you can achieve this while respecting employee privacy and promoting a constructive security culture. The integration of Purview IRM with tools like Data Loss Prevention (DLP) and Information Protection ensures that your approach is not merely reactive but also proactive, facilitating the anticipation and prevention of incidents as part of routine operations.

For high-level executives evaluating this investment, consider the implications highlighted in this paper: a single insider incident can result in significant financial losses, invite regulatory scrutiny, and cause long-term damage to your brand. Conversely, investing in an insider risk program (encompassing people, processes, and technology) serves as an insurance policy for your most critical assets. It also enhances overall

business resilience. When employees are aware that systems are in place to detect errors or malfeasance, they are more likely to adhere to best practices, and those who might be tempted to misuse data will reconsider their actions. Over time, this fosters a security-conscious workforce, achieving the ultimate goal where security becomes everyone's responsibility.

In closing, managing insider risk proactively is a hallmark of a mature and forward-thinking organization. It demonstrates to regulators, partners, and customers that you take data protection seriously, at every level. It also equips your leadership with peace of mind – an internal incident no longer has to be a nightmare scenario feared in the dark, but rather a risk that is identified and managed like any other.










We encourage you to act on the recommendations in this paper. Start with small steps – attend the webinar, run a pilot – and you'll likely uncover immediate insights. Many organizations find that once they turn on insider risk monitoring, they quickly catch policy violations or inefficiencies they had no idea about. Those early "wins" build the momentum and justification to scale up the program.

Protecting your organization from the inside out is not just a security task, but a smart business move. With Microsoft Purview Insider Risk Management, you have the tools to do it effectively. Now is the time to shine a light on insider risk and ensure that your company's sensitive data, reputation, and operations are safeguarded – from all threats, external and internal alike.

We are ready to partner with you to bring actionable insider risk management strategies to life—driving measurable competitive advantage, ensuring regulatory compliance, safeguarding your reputation, and building enduring stakeholder trust.

ADDITIONAL RESOURCES

To further explore insider risk management and best practices, consider these Microsoft resources:

Resource and Link	Description	Links
Microsoft Security Blog – “Insider Risk Management in the AI Era”	Microsoft's security blog covers emerging insider risks with Generative AI and new features in Purview IRM, including risky AI usage detections and Security Copilot integration. It's useful for understanding Microsoft's approach to these new challenges.	
Microsoft Learn – Insider Risk Management Modules	A collection of free, self-paced learning modules that cover planning, configuring, and managing Microsoft Purview Insider Risk Management. These interactive guides (with hands-on labs) help administrators and risk officers build expertise in setting up policies, analyzing alerts, and responding to incidents.	     
Tech Community “Insider Risk Management Ninja” Blog Series	Insider risk experts share detailed blog posts on the Microsoft Tech Community, covering advanced IRM tips, HR signal integration, case studies, and compliance alignment. These are helpful for security professionals seeking nuanced insights and community best practices.	 

(All links above point to Microsoft’s official platforms or trusted Microsoft partners. They offer valuable insights and guidance to complement the strategies discussed in this paper.)

REFERENCES

01 What Is Insider Threat? Unraveling
Insider Risks | Microsoft Security



05 Learn about Insider Risk
Management | Microsoft Learn



02 Insider Risk Management
empowering risky AI usage
visibility and ...



06 Mitigating insider risks in the
age of AI with Microsoft Purview
Insider Risk Management |
Microsoft Community Hub



03 Use reports in Insider Risk
Management | Microsoft Learn



07 SEBI | Guidelines for MIIIs regarding
Cyber security and Cyber resilience



04 Adapting for the new workplace
with updates from Microsoft
Purview Insider Risk Management |
Microsoft Community Hub



08 Reserve Bank of India



OUR RECENT REPORTS

INSIGHT



Navigating Data Privacy in Digital India



REPORT



State of Data Privacy in India



REPORT



State of Data Privacy in India



REPORT



AI Trends and Future Impact Industry Adoption & Insights



WHITEPAPER



DRIVE SECURE: NAVIGATING CYBER SECURITY, & PRIVACY IN CONNECTED VEHICLES



WHITEPAPER



ML Model Validation Best-practice



INSIGHT



Top compliance challenges facing the technology industry in 2025



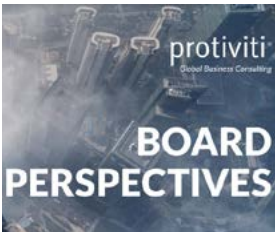
INSIGHT




Technology-modernization projects



NEWSLETTER



The Directors Playbook for Gen AI




SURVEY REPORT




From AI To Cyber - Deconstructing A Complex Technology Risk Landscape



INSIGHT




Harnessing the future: Protiviti's research on AI adoption



REPORT



Navigating DPDPA in Banking



ABOUT MICROSOFT

Who Microsoft Is

“Microsoft’s mission is to empower every person and every organization on the planet to achieve more. We’re living in an era in which technology has the potential to power awesome advancements across every sector of our economy and society. This places us at a historic intersection of opportunity and responsibility. To realize our mission, we must create a future that benefits everyone.”

[Microsoft About Page \[Our Missio...Microsoft\]](#)

What Microsoft Offers

“Explore Microsoft products and services and support for your home or business. Shop Microsoft 365, Copilot, Teams, Xbox, Windows, Azure, Surface and more.”

[Microsoft Homepage](#)

Microsoft Security Solutions

“Safeguard your people, data, and infrastructure with an AI-first, end-to-end security platform. Deliver comprehensive protection on a platform that’s powered by Copilot and threat intelligence that’s unmatched.”

[Why Microsoft Security](#)

Microsoft creates platforms and tools powered by AI to deliver innovative solutions that meet the evolving needs of our customers. The technology company is committed to making AI available broadly and doing so responsibly, with a mission to empower every person and every organization on the planet to achieve more.

Corporate Address
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-7329, USA
Tel: (425) 882-8080
Fax: (425) 706-7329

[Microsoft Worldwide Sites](#)

Why Microsoft Security

AI-powered, end-to-end security

Safeguard your people, data, and infrastructure.

- Get powerful protection for your data, endpoints, and identities with unmatched threat intelligence and best-in-class tools.
- Accelerate the secure adoption of AI with security and governance tools purpose-built for generative AI.

Microsoft Security Products : Below is a screenshot refer to link to get details

[Cloud Security Services | Microsoft Security](#)

CONTACTS

Anand Jethalia

Country Head - Cybersecurity -
Microsoft India & South East Asia
Anand.Jethalia@microsoft.com

Ashish Kumar

Principal Product Manager
Purview CXE | Customer Acceleration Team
Kumar.Ashish@microsoft.com

Fatma Balala

Product Manager
Purview CXE | Customer Acceleration Team
Fatma.Balala@microsoft.com

Danika Loadholt

Principal Group Product Manager
Purview CXE | Customer Acceleration Team
Dloadholt@microsoft.com

Microsoft Defender

Detect and respond to attacks against your devices, identities, apps, email, and clouds with leading extended detection and response (XDR) products.

Microsoft Sentinel

Get unmatched visibility into threats with a security and information management (SIEM) solution that includes a unified data lake—now in preview.

Microsoft Entra

Verify every identity and access request across your clouds, platforms, and devices with a collection of identity and access products.

Microsoft Purview

Safeguard data wherever it lives with a collection of unified information protection, governance, and compliance products.

Microsoft Priva

Respect customer and employee privacy with proactive risk mitigation and compliance management products that work together on a single platform.

Microsoft Intune

Strengthen device security and enable seamless hybrid work experiences with endpoint management products.

The Microsoft Difference

Four reasons to choose Microsoft.

- Protects comprehensively**
 Take advantage of a broad security portfolio that has integrated tools across 50 product categories that share insights to eliminate silos.
- Lowers total cost of ownership**
 Get a best-in-class, end-to-end solution for cost-effective security. Read the Forrester Consulting Total Economic Impact™ (TEI) studies commissioned by Microsoft.
- Empowers your talent**
 Multiply your teams' productivity and accuracy—generative AI helps automate and speed up remediation.
- Safeguards your AI future**
 Get the latest solutions to secure and govern AI. Comply with the evolving regulatory and audit requirements in the age of AI.

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 *Fortune* 100 Best Companies to Work For® list for the 11th consecutive year, Protiviti Inc. 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 Inc. is a wholly owned subsidiary of Robert Half (NYSE: RHI).

CONTACTS

Sandeep Gupta

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

Vaibhav Koul

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

Deepak Chawla

Managing Director
+91 98100 49791
Deepak.Chawla@protivitiglobal.in

Sahil Chandra

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

Sarita Padmini

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

Nagesh Akula

Senior Director
+91 9866694411
Nagesh.Akula@protivitiglobal.in

ACKNOWLEDGEMENT

We acknowledge the contributions of Ashish Adhikari and Fatma Balala from Microsoft, and Vaibhav Koul and Sahil Chander from Protiviti's Technology and Digital practice, in the preparation of this publication

PROTIVITI INDIA OFFICES

Ahmedabad

6th Floor, West Gate, E-Block,
Near YMCA Club, SG Highway,
Gujarat, 380 015, 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

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

Mumbai

The Westin Garden City, 13th Floor, Commerz
1- International Business Park, Behind Oberoi
mall, South Side, Goregaon, Mumbai - 400063,
Maharashtra, India

Bengaluru

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

Coimbatore

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

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

Noida

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

Bhubaneswar

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

Gurugram

15th & 16th Floor, Tower A,
DLF Building No. 5, DLF Phase III
DLF Cyber City,
Gurugram - 122 002
Haryana, India

Mumbai

1st Floor, Godrej Coliseum
A & B Wing Somaiya Hospital Road
Sion (East) Mumbai - 400 022
Maharashtra, India

Face the Future with Confidence[®]

This publication has been carefully prepared, but should be seen as general guidance only. You should not act or refrain from acting, based upon the information contained in this publication, without obtaining specific professional advice. Please contact the person listed in the publication to discuss these matters in the context of your particular circumstances. Neither Protiviti India Member Private Limited nor the shareholders, partners, directors, managers, employees or agents of any of them make any representation or warranty, expressed or implied, as to the accuracy, reasonableness or completeness of the information contained in the publication. All such parties and entities expressly disclaim any and all liability for or based on or relating to any information contained herein, or error, or omissions from this publication or any loss incurred as a result of acting on information in this presentation, or for any decision based on it.