jsa
advocates & solicitors

Investigations readiness for a new risk reality

The better the question.
The better the answer.
The better the world works.

EY
Shape the future with confidence

EY Foreword

Arpinder Singh

India & Emerging Markets Leader, EY Forensic & Integrity Services

Saguna Sodhi

Partner, EY Forensic & Integrity Services

Investigations today operate in a fundamentally evolving environment. Issues emerge faster, evidence is spread across an expanding digital ecosystem, and organizations are expected to respond with speed, transparency and confidence. At the same time, advances in analytics, digital forensics and AI are transforming how facts are identified, assessed and processed, raising new questions around trust, validation and accountability.

In this environment, investigation readiness is becoming a strategic capability rather than a reactive function. Organizations can no longer afford to assemble teams, locate evidence and define processes after an issue arises. The effectiveness of an investigation is often determined by the preparation that takes place beforehand, calling for clear governance, defined escalation protocols, multidisciplinary coordination, data readiness and well-tested response mechanisms. This requires organizations to balance speed with rigor, leverage technology responsibly, and maintain confidence in both the investigative process and its outcomes.

This playbook has been developed to support that journey. It examines the forces reshaping the investigations landscape, highlights readiness priorities across sectors, and outlines practical steps organizations can take to strengthen governance, capabilities and operating models.

As regulatory expectations rise, risks become more interconnected, and digital evidence continues to grow in volume and complexity, investigation readiness will increasingly distinguish organizations that can respond with confidence from those that struggle to keep pace. We hope this playbook serves as a practical guide for leaders seeking to build investigation functions that are resilient, technology-enabled and prepared for the challenges ahead.

JSA Foreword

Rupinder Malik

Partner, JSA and Chapter Leader,
WWCDA India Chapter

Corporate investigations have undergone a fundamental transformation. What once unfolded as a discrete, contained exercise has evolved into a multidisciplinary undertaking that simultaneously engages governance, compliance, data protection, cybersecurity and board-level oversight. The pace at which matters escalate has accelerated multi-fold, and organizations frequently find themselves managing reputational, regulatory, and litigation exposure before the underlying facts have been fully established.

Compounding this complexity is the sheer volume of digital evidence now dispersed across cloud environments, mobile devices, collaboration platforms, third-party systems, and the emergence of AI-powered analytical tools that, whilst capable of processing vast datasets with unprecedented speed, introduce their own questions of reliability, defensibility and evidentiary integrity. In India, this shift is being shaped by evolving legal and regulatory expectations. As organizations navigate increasing volumes of information and digital evidence, the ability to identify, preserve and assess relevant information early is becoming critical to an effective investigation.

This playbook is intended to address that reality. Drawing on our experience advising clients through complex investigations — both in India and across multiple jurisdictions — we have sought to distill the critical elements of investigation readiness into a practical framework. It examines the forces reshaping the investigative landscape and translates these insights into concrete guidance. It covers how to establish the governance, protocols and capabilities necessary to respond effectively before an incident arises; how to assemble and coordinate the right team when one does.

It also addresses navigating evidence preservation, privilege and regulatory engagement across borders, and avoiding the procedural missteps that too often transform a manageable matter into a protracted crisis. This is not meant to be a one-size-fits-all prescription. It is a framework that legal, compliance, risk and business teams can adapt to their organization's specific needs, so that when the next matter arises, they are positioned to respond with clarity, rigor and confidence.

Content

Section 1

Changing investigations landscape

In today's increasingly complex business environment, investigations are rapidly evolving from a reactive function into a strategic capability that enables organizations to anticipate, manage and respond to risk. Matters now move faster than traditional response processes can accommodate. In the coming years, investigations will only become faster, more data-driven and more closely integrated with governance, compliance and enterprise risk functions. To keep pace, organizations need to build the capabilities to identify and respond to issues proactively.

Building this capability requires more than having processes in place; organizations also need to ensure that investigations are legally structured from the outset, with appropriate safeguards around privilege, evidence and regulatory engagement. External counsel should therefore be involved at the outset, rather than only once a matter escalates, to help structure the investigation, assess and preserve privilege and work-product protection, ensure compliance with applicable requirements, guide evidence preservation and manage interactions with regulators.

Factors reshaping the investigations landscape

Technology-driven misconduct risks

AI, advanced analytics and digital forensics are increasingly powering the investigative lifecycle, helping organizations sift through vast volumes of data, identify anomalies and prioritize potential issues with greater speed and accuracy. As these technologies become mainstream, the differentiator is shifting from mere access to such tools toward the ability to use them in a transparent, defensible and responsible manner. Organizations realize the need for clear audits, explainable methodologies and documented decision-making that can withstand regulatory scrutiny.

This widespread adoption of AI tools is also creating new categories of records, decisions and digital footprints, and investigation teams are being called upon to assess AI-related misconduct, governance failures, bias, misuse and accountability issues.

However, it should be ensured that the use of such data, communications and patterns is aligned with applicable Indian law, including requirements relating to data protection, confidentiality, privilege and electronic evidence. To preserve confidentiality while using these tools, AI and analytics platforms deployed in investigations should operate within secure, access-controlled environments approved for confidential data, with evidence and work product shielded from public or unvetted tools. Further, AI outputs should be independently validated against the underlying evidence and should not, by themselves, form the basis for material investigative conclusions.

Increasing regulatory expectations

At the same time, rising regulatory scrutiny is placing greater emphasis on rapid triage, timely escalation and well-documented decision-making. Organizations are expected to assess allegations quickly, preserve evidence effectively and demonstrate that concerns have been investigated independently and fairly. To avoid common investigation/legal failures such as delayed evidence preservation, inadequate documentation, uncontrolled

circulation of sensitive information, inappropriate handling of privileged material and arriving at premature conclusions, certain actions need to be undertaken at the very outset:

- Having a clear triage protocol, documented decision-making, controlled access to information and a consistent investigation framework.
- Legal counsel should be engaged at the triage stage, rather than after initial fact-finding, so that privilege attaches early and evidence collection is guided appropriately.
- A contemporaneous investigation record/decision log recording documenting the allegations, scope and methodology, reasons for key decisions – including the triage rationale, escalation timing, privilege calls and the basis for key procedural choices, evidence collected and reviewed, interview records, findings/conclusions along with the status of remediation measures. This can help demonstrate that the investigation was independent, fair and legally defensible, while balancing speed with due process.

Investigation triage

Effective investigation readiness begins with the ability to assess an allegation consistently and proportionately. Organizations should establish predefined triage criteria that consider the credibility of the allegation, potential financial or reputational impact, involvement of senior personnel, regulatory or law-enforcement exposure, risk of continuing misconduct and the volatility of relevant evidence. Matters should be capable of being reclassified as new facts emerge or the risk profile changes.

The triage protocol should also specify who acts as the first responder, who determines whether there is a sufficient basis to investigate, how conflicts are identified, which matters require legal or board-level escalation and how cases that do not meet the investigation threshold are recorded and closed. Documenting the rationale for these decisions creates an early audit trail and helps demonstrate that the organization responded consistently, independently and in accordance with its established framework.

Proliferation in digital evidence

Establishing trust in digital evidence is emerging as a critical capability. Today, evidence may sit across cloud collaboration tools, mobile devices, identity logs, financial systems and vendors and legal, regulatory, employment and reputational consequences often arise before the full fact pattern is known. Investigators should assess the legal and contractual basis for accessing, collecting, processing and transferring such evidence upfront, including applicable requirements under (i) existing Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules), established under the Information Technology Act, 2000 (IT Act), (ii) the Digital Personal Data Protection Act, 2023 (DPDP Act) (along with the underlying rules), which is not yet fully implemented but once operative, will provide legal basis for processing personal data for "certain legitimate uses", including employment-related purposes or safeguarding the employer from loss or liability, (iii) contractual agreements and employment terms and (iv) relevant organizational policies, procedures and guidance documents. The collection should be proportionate to the investigation, with appropriate safeguards.

The approach should distinguish between employee and data held by third parties: for employee data, organizations should ensure that applicable notices, consent protocols, policies and access controls are in place, while for vendor, contractor or other third-party data, the contractual basis and compliance with policies for access, preservation, confidentiality, security, retention and permitted processing should be established upfront. Key decisions, approvals and the basis for collection should be documented to demonstrate that access was necessary, proportionate and appropriately authorized.

In the time ahead, organizations will be expected to demonstrate elevated levels of evidential integrity. As deepfakes, manipulated communications and AI-generated content proliferate, investigators devote as much time to validating authenticity as to uncovering facts. Original records, metadata, audit trails and chain-of-custody should be preserved wherever practicable, with collection methods designed to support authenticity and integrity, including applicable requirements under the Bharatiya Sakshya Adhiniyam, 2023. Under this framework, electronic records are admissible as evidence, but only when accompanied by a certificate from a person holding a responsible official position in relation to the operation of the relevant device or the management of the relevant activities.

Regulators are also paying closer attention to employees' use of disappearing-message and ephemeral chat applications during live matters, since leaving auto-delete settings active after a legal hold can amount to spoliation of evidence. Accordingly, relevant retention and preservation requirements should be identified early and, where legally appropriate, auto-delete or

ephemeral settings should be suspended, and the preservation steps documented. Before collecting evidence from collaboration platforms, cloud systems or third-party environments, organizations should confirm the applicable legal basis and authority for collection, assess privacy, data-protection and employment-law requirements, and ensure appropriate contractual safeguards are in place where evidence is held by vendors or external platforms.

Speed of impact

Reputational damage, regulatory scrutiny, customer concerns, and business disruption can materialize within hours of an allegation becoming public, often before all the facts have been established.

Cross-functional response requirements

Modern investigations frequently require coordination across legal, compliance, risk, HR, cybersecurity, internal audit and business teams to ensure a consistent and defensible response.

Need for investigation readiness

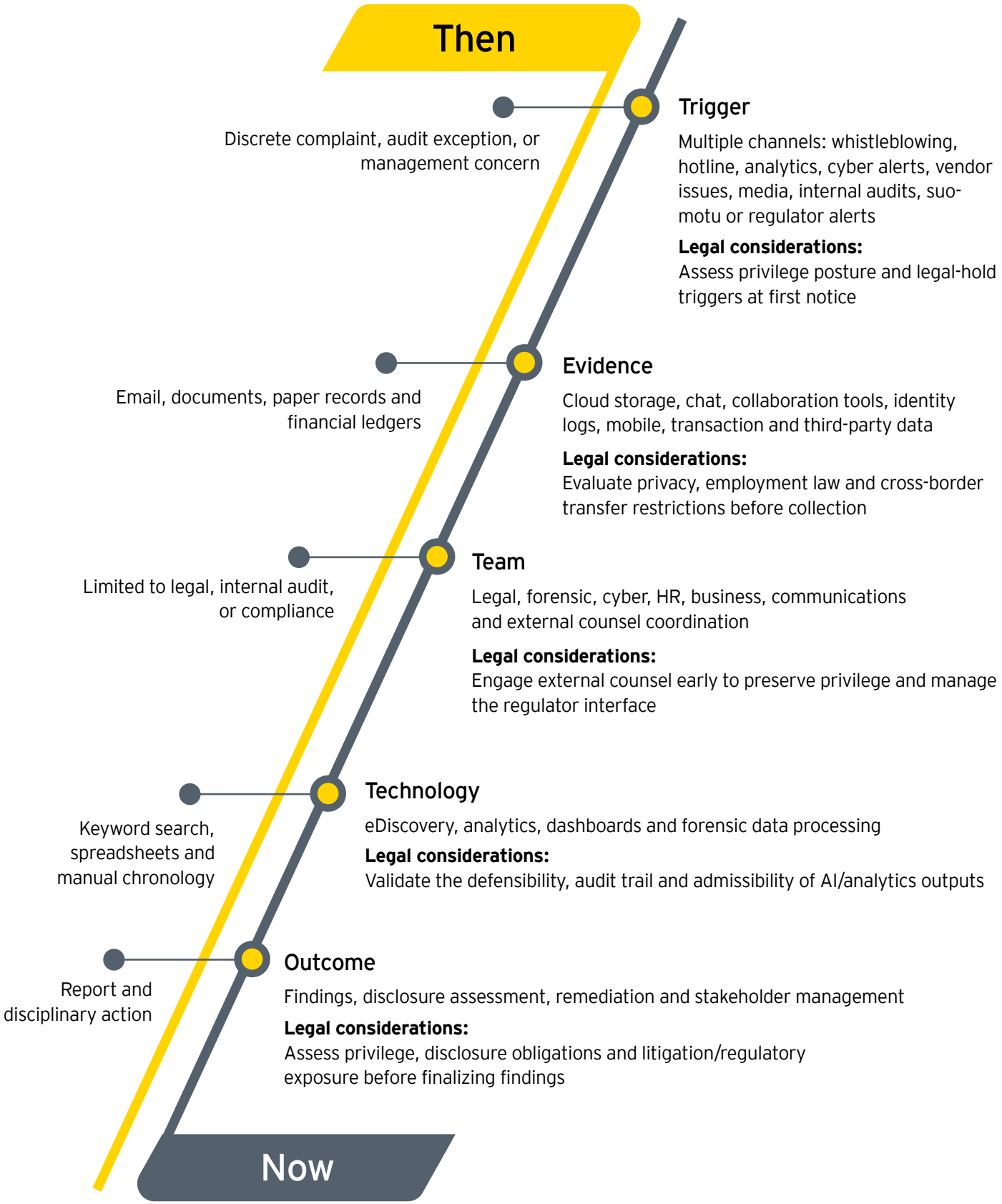
Organizations can no longer rely solely on ad hoc responses. They need predefined processes, clear governance, evidence preservation mechanisms, investigation playbooks and trained personnel to respond effectively when issues arise.

At a minimum, organizations should have a clear code of conduct and relevant policies, along with defined protocols for escalation and reporting, privilege protection, evidence-preservation and confidentiality control. Further, the roles for relevant functions, such as legal, HR, compliance and management, should be clearly identified in advance. This will help ensure that potential issues are identified and escalated promptly, enabling investigations to commence quickly and avoiding unnecessary delays at the outset.

A privilege protocol should distinguish privileged legal advice from ordinary business, HR or investigative communications. Given the lack of clarity under Indian law on whether legal privilege extends to in-house counsel in the same manner as communications with an external legal practitioner as defined under Indian law, the protocol should clearly set out engagement of external counsel, who controls and receives privileged communications, how documents and communications are marked and stored, access restrictions, treatment of third-party investigators/consultants, interview notes and investigative work product, and procedures for avoiding inadvertent disclosure or waiver of privilege.

Despite these technological advances, human expertise remains essential to effective investigations. Judgment, credibility, ethics, and the ability to navigate sensitive stakeholder dynamics continue to be critical to reach fair and defensible outcomes. Ultimately, the future of investigations lies in combining technology-enabled intelligence with human insight, creating investigation functions that are not only more efficient but also more trusted, resilient and better equipped to address emerging risks.

Evolution of investigations



Key changes that will define the future of investigations

01

Always-on readiness

- Investigation readiness will become a standing capability, not a reactive exercise.
- Organizations will maintain data inventories, legal hold protocols, evidence retention procedures, escalation criteria, regulator engagement frameworks and key contact networks on an ongoing basis.
- Critical investigation assets will remain current and accessible before issues arise.

02

Event-driven mobilization

- Organizations will adopt predefined investigation response models to enable faster and more consistent action.
- Matters will be escalated based on severity, impact and risk, with oversight ranging from local teams to boards, external counsel, regulators, or law enforcement.
- Clear triage thresholds will guide proportionate and timely decision-making.

03

Unified evidence narratives

- Investigators will consolidate evidence from multiple sources into a single, defensible chronology.
- Technical, financial, operational, governance and communication records will be connected to provide a holistic view of events.
- Contradictory evidence, gaps and limitations will be documented and visible.

04

AI-assisted, human-accountable workflows

- AI will accelerate investigations through anomaly detection, data clustering, evidence prioritization and summarization.
- Human investigators will retain responsibility for scope, interpretation, findings, credibility assessments and decisions.
- AI will augment investigative judgment rather than replace it.

05

Continuous evidence preservation

- Evidence preservation will become increasingly automated through predefined workflows.
- Relevant data across emails, collaboration platforms, cloud environments, devices, logs and third-party systems will be identified and secured rapidly.
- Chain of custody, integrity and traceability will remain critical throughout the process.

06

Regulator-ready documentation

- Organizations will document both investigative outcomes and the rationale behind them.
- Decision logs will capture scope, preservation actions, privilege considerations, reporting obligations, employee actions, limitations, and remediation measures.
- Documentation will support transparency, consistency and regulatory scrutiny.

07

Case-to-control learning

- Investigations will extend beyond fact-finding to drive organizational improvement.
- Findings will inform root-cause analysis, policy and control enhancements, monitoring programs and employee training.
- Lessons learned will strengthen resilience and help prevent the recurrence of issues.

Key trends shaping India's digital forensics landscape

The Indian digital forensics market is on a strong upward trajectory and is estimated to grow at a **40% CAGR** to reach **INR11,924 crore by 2030**[1]**.** With cybercrime complaints in India surpassing **15.9 lakh** in 2023[2], forensic readiness is now a core leadership imperative.

In FY 2025-26 alone, the Directorate of Enforcement (ED) recorded property attachments of **INR81,422 crore**[3], alongside a reported conviction rate of approximately 94%[4] for the same year.

Recent legislation boosting digital forensics and modern investigations:

- Insolvency and Bankruptcy Code (IBC) 2016
- The Real Estate (Regulation and Development) Act, (RERA) 2016
- The Digital Personal Data Protection (DPDP) Act 2023
- The Bharatiya Nyaya Sanhita (BNS)
- Bharatiya Nagarik Suraksha Sanhita (BNSS)
- Bharatiya Sakshya Adhiniyam (BSA)

[1] *Indian digital forensics market to reach Rs. 11,924 crore (US$ 1.39 billion) by 2030: Report | IBEF*

[2] *Cyber security incidents nearly double in two years, govt says*

[3] *ED attaches Rs 81,422 cr assets in FY26 - ByNewsIndia*

[4] *ED achieves 94.82% conviction rate in money-laundering cases at end of 2025 - The Hindu*

Embedding AI and advanced analytics into investigation workflows

AI can perform high-volume triage tasks, freeing up the time of specialized forensic teams to focus on the how and why of the investigation. However, AI should only be embedded as a controlled accelerator, not an autonomous investigator. Leveraging AI can be justified when the use case is approved, secure, explainable, validated, proportionate and reproducible.

Ways in which AI can assist investigations:

I
Grouping similar complaints

How can AI help? By helping to spot related complaints, repeat issues, common vendors, or emerging patterns

Safeguards: Human intervention during the final decision-making

Records to maintain: Reason for grouping, supporting evidence and reviewer approval

II
Document sorting, prioritization and summarization

How can AI help? Quickly organize large volumes of documents and highlight key topics

Safeguards: Using approved tools and verifying output to ensure accuracy

Records to maintain: Search method used, tool version, validation checks and reviewer notes

III
Analyzing people, entities and transactions

How can AI help? Identifying unusual relationships, suspicious transactions, conflicts, or duplicate records that may warrant further legal checks/investigation

Safeguards: Using trusted data sources and reviewing results for errors, maintaining the document trail and consent protocol from a data protection and evidentiary perspective

Records to maintain: Data sources, analysis rules, reports generated, consent logs (where applicable) and final actions taken

IV
Creating timelines and interview preparation documents

How can AI help? Speeding up case preparation, organizing key facts and evidence and highlighting missing information or inconsistencies

Safeguards: All findings must be linked back to evidence and reviewed before use

Records to maintain: Timeline, assumptions made, interview plan and approval records

V
Support legal analysis

How can AI help? Assist in structuring factual and evidentiary findings, identifying relevant patterns and organizing large volumes of information in a meaningful manner to facilitate efficient and timely legal analysis

Safeguards: Appropriate legal review and supervision; AI-generated outputs should be treated as a tool to support, and not replace, legal analysis. All material findings should be traceable to the underlying evidence and independently reviewed before being relied upon

Records to maintain: AI tool/model used, purpose and scope of its use, relevant inputs and outputs, methodology/prompts where material and records of human/legal review and validation

Questions to ask while navigating cross-border regulatory and data challenges

Q

Where does the data reside?

Before collecting evidence, organizations should have a clear understanding of where relevant data is stored, who owns it, who has access to it and regulatory restrictions that may apply. Understanding the data landscape upfront helps avoid delays and ensures compliance with local laws.

Q

Can evidence be preserved without triggering data transfer risks?

When an issue arises, the immediate priority is to preserve potentially relevant evidence so that it is not altered, deleted, or lost. However, preserving data does not automatically mean it can be reviewed or transferred across borders. Organizations should first assess applicable legal requirements, privacy restrictions, employee rights, privilege considerations and regulatory obligations.

Q

What legal requirements apply across different jurisdictions?

Privacy and data protection laws vary significantly across jurisdictions. What may be permissible in one country could require additional approvals, notifications, or safeguards in another. Organizations should ensure investigation procedures are adaptable to local legal requirements while maintaining consistency in the overall investigative approach.

Q

Have the right stakeholders been engaged early?

Cross-border matters often require input from legal, compliance, HR, IT, cybersecurity and external counsel. Early coordination helps organizations identify potential restrictions, determine the appropriate investigation strategy and avoid delays caused by jurisdiction-specific requirements.

Q

Is the process adequately documented?

Organizations should document key decisions pertaining to data collection, access rights, transfer mechanisms, legal approvals and investigation scope. Clear documentation helps demonstrate compliance and provides support if regulators, auditors, or courts later review the investigation process.

Q

Are we taking a risk-based approach to data access?

Instead of collecting large amounts of data indiscriminately, organizations should focus on gathering only relevant information. This minimizes privacy risks, reduces review costs and supports compliance with data minimization principles.

Q

Are we prepared before an incident occurs?

Organizations that maintain up-to-date data maps, predefined legal hold procedures, approved data transfer mechanisms, and local legal contacts can respond significantly faster when a matter arises. Proactive preparation reduces delays and improves the defensibility of the investigation process.

Strategic priorities for Indian companies

- Proactive workflow coordination
- Engage jurisdictional experts
- Technology integration
- Data inventory and mapping
- Distinct investigation governance
- Building multidisciplinary investigations teams

Who should your dream team for investigations consist of?

Role	Primary accountability	Early actions	Risks
Sponsor/board committee	Authority, independence, budget and oversight	Approve mandate, escalation thresholds and establish reporting cadence	Conflicts, delay and weak defensibility
External counsel/ legal lead	Provide 360-degree legal oversight across all investigation workstreams, acting as the central integrator across various functions such as the Board, forensic, compliance, internal audit, management, HR, IT/data	Set legal purpose, privilege protocol, issue map and regulator timetable	Privilege waiver, over-collection, or under-disclosure
Forensic/data lead	Preservation, collection, analytics, chain of custody and evidence narrative	Issue preservation plan, data map, forensic collection route and integrity controls	Evidence loss, metadata alteration or inadmissibility challenge
Compliance/ internal audit	Policies, controls, prior issues, remediation ownership	Map controls, root causes and prior similar allegations	Findings remain isolated and recurrence risk persists
Information Security/IT	Access, logging, identity, containment and cloud/mobile evidence	Protect logs, credentials, devices, cloud repositories and time synchronization	Volatile evidence loss and uncontrolled access
HR/employee relations	Fair process, interim measures, interviews and discipline	Support witness sequencing, anti-retaliation and employee action protocol	Employment claims, retaliation risk and inconsistent discipline
Communications/ stakeholder lead	Internal and external messaging discipline	Prepare holding lines, leak response and approval workflow	Narrative outruns facts or compromises confidentiality

From a contact list to a mobilization model

Identifying relevant functions is the first step. Investigation readiness requires a predefined method to bring those functions together when a significant matter arises.

Organizations should establish activation criteria for an investigation response team, identify primary and alternate representatives and clarify who has the authority to mobilize the team.

The model should define:

- Team's initial actions
- Decision rights
- Information-sharing rules
- Meeting and reporting cadence
- Routes for securing specialist or external support

Ready-to-use templates for initial assessment, preservation notices, investigation planning, stakeholder updates and decision logging can reduce avoidable delays during the first stage of a matter.

The response model should be tested periodically through tabletop exercises involving realistic scenarios, such as an allegation involving senior personnel, suspected evidence destruction, a cross-border data issue or potential regulatory notification.

Lessons from each exercise should be recorded and used to update roles, contact details, workflows and templates.

Seven-stage investigation workflow

Detect

Scope out the allegation/ anomaly

Questions you need to ask
Has a potential issue been identified?
Does it need immediate attention?

Ideal outcomes
Initial issue logged and urgent risks identified

Triage

Assess credibility, materiality, conflicts

Questions you need to ask
Who should handle the matter and how serious is it?

Ideal outcomes
Ownership assigned and response approach agreed

Preserve

Protect evidence and chain of custody

Questions you need to ask
Have all relevant documents, emails, devices and records been secured?

Ideal outcomes
Critical information preserved for review

Plan

Define issues, scope and workstreams

Questions you need to ask
Do we have a clear investigation plan, team and resources?

Ideal outcomes
Investigation scope, timeline and responsibilities defined

Investigate

Collect, analyze, interview and corroborate facts

Questions you need to ask
What happened and what evidence supports the findings?

Ideal outcomes
Facts gathered, analyzed and documented

Decide

Assess findings, disclosure and establish discipline

Questions you need to ask
What actions should be taken based on the findings?

Ideal outcomes
Decisions made and corrective actions initiated

Remediate & Learn

Report, remediate, validate and retain learnings

Questions you need to ask
Have the root causes been addressed and lessons learned?

Ideal outcomes
Investigation closed and improvements implemented

Challenge mapping

Investigations and response efforts are often complicated by operational, regulatory, technological and stakeholder-related challenges. Identifying these barriers early is essential to strengthening readiness, improving decision-making and achieving effective outcomes. The following map outlines some of the most common challenges organizations face in this process

Unclear ownership

Material allegations can be delayed or handled inconsistently when no one knows who owns triage, who can instruct external counsel, who approves preservation, who holds legal sign-off authority, or when board oversight is required.

Three-point remediation strategy

1. Define tiered triggers by severity, seniority, jurisdiction, regulatory exposure and evidence volatility.
2. Pre-identify the sponsor, legal lead, forensic lead, alternates and external adviser routes, with legal holding sign-off authority over privilege, disclosure and regulator communications.
3. Record triage decisions, conflicts and rationale in a decision log from the first response.

Evidence management

Relevant evidence may exist across cloud repositories, collaboration platforms, chat, mobile devices, identity logs, SaaS systems, endpoints, transaction systems, physical records and third parties. Volatile logs or anti-forensic conduct can make evidence unavailable before the investigation team is mobilized.

Four-point remediation strategy

1. Maintain an evidence map showing key systems, owners, data location, retention period and collection method. Keep ready-to-use legal hold and preservation templates for common investigation scenarios, with defined approval and escalation protocols for employees and cross-border data.
2. Third-party data: Notify the vendors/service providers to retain relevant records and logs in accordance with applicable contractual and legal requirements.
3. Establish predefined preservation procedures for common scenarios rather than developing them during a live matter, including:
    i. Cloud systems: Preserve emails, SharePoint files, Teams data, cloud folders and audit logs
    ii. Mobile devices: Secure phones, messages, call logs, WhatsApp chats and device backups
    iii. Identity logs: Preserve login records, access logs, MFA records and VPN logs
    iv. Third-party data: Notify vendors/service providers to retain relevant records and logs
    v. Disappearing/ephemeral messaging apps: Suspend auto-delete settings for custodians under legal hold and export chats before scheduled deletion cycles
4. Test whether important data sources can be preserved and collected before a live matter arises, including the ability to preserve metadata and maintain chain of custody, and identify any legal, technical, contractual or cross-border constraints that could affect timely collection.

Privacy and data minimization risks

Investigations often require personal data, employee communications and device data. The need to investigate should be balanced against privacy, employment law and data-protection considerations, with a clear distinction between employee/in-house data and data held by vendors, contractors or other third parties. The purpose, scope and applicable legal basis for collection should be established upfront, with consent or notice protocols applied where applicable. Over-collection can create privacy and employment risks, while under-collection can undermine the investigation.

Three-point remediation strategy

1. Clearly define the required data, collect only the data that is relevant to the investigation and assess the legality of collecting it. For employee data, consider applicable employment terms and organizational policies; for third-party data, establish the contractual basis for access.
2. Preserve data first where permitted, then review, access or transfer only what is necessary for the investigation.
3. Document the data lifecycle, including the categories of data collected, custodians, purpose and legal basis, approvals, notices/consents where applicable, access rights, transfers, retention and deletion decisions. Key collection and access decisions should be documented to demonstrate necessity, proportionality and appropriate authorization.

Maintain documented protocols for employees and third-party data, with legal involvement where collection involves personal devices, sensitive information, cross-border access or material third-party restrictions.

Evidence, integrity, admissibility and chain of custody

Screenshots, forwarded chats, altered PDFs, extracted spreadsheets and unlogged transfers may be challenged as incomplete, manipulated or unauthenticated.

Three-point remediation strategy

1. Use forensic collection methods where needed, preserving originals and metadata before processing or conversion.
2. Maintain chain-of-custody records for collection, transfer, storage, access and analysis; use hashes or equivalent integrity controls.
3. Prepare an evidence map linking each finding to source material, collection method, limitations and reviewer.

Cross-border regulatory and data action is delayed

Data, people, systems, banks or counterparties may be located in different countries. Local laws and approvals can delay evidence collection or tracing

Three-point remediation strategy

1. Create a jurisdiction heat map covering data location, transfer restrictions, employment rules, privilege and regulator triggers.
2. Secure the data first, then decide how it can be legally reviewed or moved across countries.
3. Document the legal basis, approvals, minimization, chain of custody and notification decisions.

AI introduces opaque or unreliable outputs

AI can accelerate triage, review and analytics, but unvalidated summaries, classifications or anomaly detections may influence scope, interviews, employee action or disclosure decisions without adequate traceability.

Three-point remediation strategy

1. Approve AI use cases and environments before deployment; prohibit the use of uncontrolled public tools for confidential evidence.
2. Require source traceability, validation sampling, human reviewer sign-off and documented limitations.
3. Retain the prompt, method, tool/model version, input categories and output relied upon where these are material to the outcome.

Lack of coordination across teams

Legal, forensic, HR, cyber, business and communications teams may act on different priorities. At the same time, early assumptions can prematurely narrow the matter, while uncontrolled expansion delays closure.

Three-point remediation strategy

1. Create an integrated investigation plan with workstreams, milestones and scope-change criteria.
2. Use periodic challenge reviews to test hypotheses, contrary evidence, bias and new issues.
3. Escalate unresolved scope or priority conflicts and record decisions in the decision log

---

Remediation stops at recommendations

Investigations are often closed with recommendations but no validated closure, residual risk decision or monitoring rule. This weakens the organization's ability to demonstrate durable risk reduction.

Three-point remediation strategy

1. Link each finding to root cause, control failure, risk owner, due date and closure evidence.
2. Require independent validation of completed actions, especially for high-risk findings.
3. Feed lessons learned into risk assessment, monitoring scenarios, training, policies and future tabletop exercises

Section 2

Sector lens: Investigative risks, response gaps and readiness priorities

While core principles of investigation readiness remain consistent across industries, the specific risks organizations face, the evidence they rely upon and the regulatory expectations they operate under can differ significantly from one sector to another. The nature of misconduct, the velocity at which incidents escalate, and the complexity of available data often shape how investigations are initiated, managed and scrutinized.

For this reason, adopting a one-size-fits-all approach to investigations does not work. An effective response framework must take sector-specific realities of the business into account, including the regulatory landscape, operational model, third-party ecosystem, technology environment and stakeholder expectations. The controls required to investigate a procurement fraud allegation in a manufacturing company may differ substantially from those needed to respond to a market conduct concern in a financial institution or a product integrity issue in a retail business.

Consumer products and retail

Key investigation risks

Consumer products and retail organizations typically operate across extensive supplier, distributor and logistics networks that create multiple points of vulnerability. Common investigation triggers include third-party fraud, procurement irregularities, vendor collusion, product diversion, inventory manipulation, bribery in sourcing activities, counterfeit goods, conflicts of interest and allegations related to labor practices within supply chains.

The sector's growing dependence on e-commerce platforms, loyalty programs and digital customer channels is also increasing exposure to cybersecurity incidents, data misuse, fraudulent transactions and misconduct involving customer information. Investigations frequently require organizations to trace activity across numerous internal systems and third-party partners while maintaining visibility over fragmented data sources.

Common response gaps

Many organizations face challenges in obtaining timely access to supplier and distributor records, particularly where contracts lack appropriate audit, data retention or investigation clauses. Evidence may be dispersed across enterprise systems, logistics providers, outsourced operations and external platforms, making preservation and collection difficult.

Organizations also commonly underestimate the legal and reputational consequences of product-related allegations. Delays in escalation, unclear ownership of investigations and insufficient documentation of decision-making can create challenges when responding to regulators, customers or litigation.

Readiness priorities

Organizations should establish investigation-ready third-party governance frameworks that clearly define audit rights, retention obligations, data access requirements and escalation protocols with suppliers and distributors.

Consumer product schemes

Counterfeit finished goods using near-genuine packaging

- Conduct controlled purchases and obtain technical authentication from quality/brand teams
- Undertake market enquiries, surveillance and link analysis to identify printers, refillers, stockists and financiers
- Preserve evidence and coordinate any enforcement action through authorized legal and law-enforcement channels

Leakage of genuine packaging material

- Inspect destruction practices and perform surprise counts at plants, converters and scrap yards
- Analyze abnormal yield, scrap ratios, repeat scrap buyers and off-hours movements
- Interview packaging, quality, stores, security and scrap-vendor personnel

Reuse or re-tagging of expired, near-expiry or damaged products

- Test batch and date-code continuity and inspect label-printing access and consumables
- Trace movements from stores and depots to warehouses, rework locations and scrap vendors
- Conduct market checks and test purchases in suspected diversion channels

Product diversion into unauthorized channels

- Analyze bulk orders, unusual discounts, address overlap, repeated transport routes and sales spikes
- Review distributor incentives, secondary-sales evidence and channel-partner communications
- Quantify diverted volume, margin leakage and parties benefiting from the diversion

Trade promotion and secondary-sales inflation

- Reconcile primary sales, secondary sales, stock, collections and scheme claims at invoice and outlet level
- Verify outlet existence and sales through field visits, customer confirmations and geo/location checks
- Test duplicate GST/tax IDs, bank accounts, mobile numbers, addresses and invoice sequences

Fictitious or inflated damage, expiry and trade-return claims

- Match claims to goods-receipt notes, photographs, batch details, credit notes and destruction evidence
- Perform surprise physical verification and inspect quarantined stock
- Confirm selected claims with retailers, transporters and independent auditors

Theft of formulas, products, pricing or channel data

- Issue a legal hold and preserve laptops, email, cloud, mobile and relevant logs
- Classify the information taken and confirm access need, ownership and confidentiality
- Conduct conflict-of-interest, competitor-link and market-intelligence checks, together with a review of messaging activity around key events

Retail schemes

POS void, cancellation and refund fraud

- Analyze voids, post-voids, refunds, reprints and cancelations by user, terminal, time and store
- Match exceptions to bills, CCTV, cash-till records, inventory movements and customer contacts, together with any control overrides or credential sharing
- Perform surprise till counts and end-of-day reconciliation

Misuse of loyalty points, gift cards and promotional vouchers

- Analyze enrollment, earning, manual adjustments, transfer and redemption logs
- Identify shared devices, mobile numbers, addresses, IPs and redemption locations
- Review administrator access, overrides and dormant-account reactivations

Manual discount and price-override abuse

- Profile manual prices, stacked discounts and employee discounts by user, SKU and customer
- Compare transaction prices with approved promotion calendars and master data
- Test for repeat beneficiaries, bulk quantities and non-business-hour transactions

Bulk sale of promotional or scarce goods to connected buyers

- Identify bulk invoices, repeated customer identifiers, split bills and rapid inventory depletion
- Conduct market visits or controlled purchases to locate diverted stock
- Quantify stock-out impact, discount leakage and beneficiaries

Store shrinkage through short-receipt and inventory manipulation

- Reconcile dispatch, GPS/transporter proof, store receipt, serial/batch scan and inventory adjustments
- Analyze repeated shortages by route, store, SKU, approver and threshold
- Conduct inventory counts and trace high-value goods

Lease rental, store-location and fit-out kickback scheme

- Benchmark rentals and fit-out rates for comparable locations and specifications
- Review site evaluations, footfall studies, negotiation records, approvals and bid comparisons and stakeholder relationships
- Conduct site visits and market enquiries with property consultants and vendors

Financial services

Key investigation risks

Amid today's fraud landscape, financial institutions operate within some of the most highly regulated environments, facing continuous scrutiny from regulators, customers and markets. Common investigation triggers include fraud, anti-money laundering (AML) concerns, sanctions violations, insider trading, market abuse, employee misconduct, conflicts of interest, unauthorized trading, cyber incidents and customer complaints.

The rapid digitization of financial services has expanded the volume of structured and unstructured data available to investigators. Communications records, transaction data, surveillance alerts, customer interactions and digital activity logs increasingly form the basis of investigations. At the same time, organizations face mounting expectations to identify suspicious activity quickly and demonstrate robust governance over decision-making.

Increased coordination and information-sharing among law enforcement and regulatory authorities in India raises the risk of parallel investigations under multiple frameworks. For example, a single allegation of financial misconduct could trigger simultaneous inquiries by SEBI, the Enforcement Directorate and the Income Tax Department, each with distinct disclosure obligations, timelines and penalties, thereby compounding legal, regulatory and operational exposure.

Common response gaps

A recurring challenge is the inability to connect information across compliance, cyber, fraud, legal and business functions. While institutions often possess substantial amounts of data, investigations can stall when evidence exists in disconnected systems or when ownership of cases is fragmented.

Another common gap is inconsistent documentation of investigative rationale and escalation decisions. Regulators increasingly expect organizations to demonstrate not only what actions were taken, but how decisions were reached and whether investigations were conducted fairly and independently.

Readiness priorities

Organizations should maintain integrated investigation response frameworks that bring together legal, compliance, fraud, cybersecurity and business stakeholders under clearly defined governance structures.

Investigation independence and oversight

- Investigations involving senior stakeholders or oversight functions may face actual or perceived independence concerns.
- Perform an upfront independence and conflict-of-interest assessment.
- Establish independent oversight for high-risk or senior-management matters.
- Leverage external counsel or forensic experts where additional independence is required.

Evidence preservation across distributed environments

- Issue an immediate legal hold and preservation notice covering internal systems, vendors, cloud environments and downstream service providers.
- Invoke contractual audit, access, data-return, regulator-access and incident-cooperation rights through legal and vendor management.
- Maintain a source-to-evidence register recording the data owner, custodian, system of record, extraction method, date range, limitations and completeness validation.

Evidence collection in live, business-critical environments

- Adopt a risk-based forensic collection plan that prioritizes volatile and overwrite-prone evidence without interrupting critical services.
- Use targeted methods such as logical acquisition, API-based extraction, database snapshots, cloud snapshots and endpoint triage; reserve full forensic imaging for appropriate endpoints or servers.
- Obtain IT, business continuity and legal sign-off on collection methods, documenting what could not be collected, why, and the resulting evidentiary limitation.

Confidentiality risks in investigation records

- Classify investigation data by sensitivity and apply need-to-know access, encryption, controlled workspaces and download restrictions.
- Maintain an access log for the investigation repository, including external advisers and reviewers.
- Define retention, legal-hold and secure-disposal requirements by evidence category, legal requirement and anticipated proceedings.

Facts, inferences and conclusions not clearly segregated

- Separate established facts, analysis and conclusions in report drafting.
- Link every finding to specific supporting evidence.
- Clearly distinguish investigative observations from legal conclusions.

Fragmented accountability across multiple lines of defense

- Prepare a decision-level accountability map identifying who initiated, recommended, checked, approved, executed, monitored and challenged each relevant action.
- Test actual conduct against the delegation of authority, committee charter, job description, maker-checker matrix and regulatory responsibility, rather than relying only on stated roles.
- Distinguish primary misconduct, supervisory failure, control-function failure, negligent oversight and systemic design failure in the final findings.

Staff accountability determined before due process

- Provide individuals with the relevant allegations and a fair opportunity to respond, subject to legal and HR guidance.
- Assess conduct against the policy, authority, information and system capability available at the relevant time.
- Apply a consistent accountability framework distinguishing intentional misconduct, gross negligence, ordinary error, supervisory lapse and institutional control failure.

Regulatory reporting amid evolving facts

- Create a regulatory matrix covering reporting timelines, responsible owner, approval authority and required information.
- Separate confirmed facts, preliminary indicators, assumptions and unresolved questions in every notification.
- Maintain a single disclosure log to ensure consistency across regulators, law enforcement, auditors, insurers, customers and market disclosures.

Inconsistent positions across parallel proceedings

- Establish a single matter-governance group, led by legal, to coordinate facts, disclosures and strategic decisions.
- Maintain a controlled core fact pack, chronology, issues matrix and disclosure register for use across proceedings.
- Document differences in evidentiary standards, confidentiality constraints and decision thresholds for each proceeding.

Management overrides and emergency actions not retrospectively reviewed

- Extract and analyze override, exception and emergency-access populations, including frequency, approver and business justification.
- Test whether each override was time-bound, independently reviewed and supported by compensating controls.
- Require post-event review and formal closure of all emergency rights, temporary limits and manual workarounds.

Closure does not address recurrence or systemic exposure

- Define a proportionate look-back period and population based on root cause, data availability, regulatory exposure and customer impact.
- Quantify financial, customer, conduct, prudential, operational and reputational impact, including potential exposure rather than only booked loss.
- Obtain formal closure from the designated risk owner, compliance, legal and an independent validator, with explicit documentation of residual risk and monitoring arrangements.

Advanced manufacturing and infrastructure

Key investigation risks

Advanced manufacturing and infrastructure organizations often operate across complex and geographically different environments involving large capital investments, extensive contractor ecosystems and critical operational assets. Common investigation triggers include procurement fraud, bid-rigging, corruption, conflicts of interest, contractor misconduct, safety incidents, quality failures, asset misappropriation, cyber intrusions and environmental compliance breaches.

The convergence of operational technology, industrial control systems and enterprise IT environments creates additional investigative complexity. Incidents frequently require analysis of physical records, operational logs, equipment data, project documentation and communications spanning multiple contractors and jurisdictions.

Common response gaps

Organizations often struggle with fragmented ownership of evidence and limited visibility over third-party contractors. Critical information may be distributed across project management systems, engineering platforms, operational technologies and contractor-controlled environments.

Another challenge is preserving evidence from industrial and operational systems that were not originally designed with investigative requirements in mind. Delays in evidence collection can affect the integrity and availability of important records.

Readiness priorities

Organizations should establish investigation readiness programs that extend beyond corporate functions and include project sites, contractors, joint ventures and operational teams.

Bid rigging and procurement collusion between employees, bidders or intermediaries

- Regularly analyze bid patterns, common ownership, pricing similarities and unusual bidder relationships.

Kickbacks and conflicts of interest involving employees, vendors, or contractors

- Maintain updated vendor ownership information and periodically screen for employee-vendor connections.

Inflated contractor bills and false claims for manpower, materials or equipment

- Link invoices with work orders, site records, attendance, material movement and payment data.

Manipulation of change orders and project costs

- Keep a clear record of the request, justification, approval, revised scope and payment for each change order.

Quality and safety record manipulation to hide defects, delays or non-compliance

- Preserve test reports, inspection records, photographs, CCTV and system logs at the start of an investigation.

Subcontractor misconduct, including bribery, labor violations or permit irregularities

- Map the complete contractor chain and include investigation, audit and evidence-access rights in contracts.

Inventory, equipment and asset theft from factories, warehouses or project sites

- Compare inventory movements with gate records, access logs, CCTV, work orders and disposal records.

Intellectual property and confidential-data theft

- Monitor downloads, external transfers and unusual access to sensitive engineering or project information.

Vendor impersonation and payment diversion

- Independently verify changes to vendor master data and bank details before releasing payments.

Section 3

Operating models, capabilities and governance for modern investigations

The effectiveness of an investigation is often determined before an incident ever occurs. Organizations must establish clear governance structures, defined processes, appropriate technology, and skilled resources to ensure investigations can be conducted efficiently, defensibly and in compliance with legal and regulatory requirements.

The following readiness checkpoints can help organizations assess their preparedness.

Readiness checkpoint 01

Governance and decision rights

Clear ownership and decision-making authority are essential to ensure investigations remain objective, timely and well-governed. Organizations should establish an investigation charter, define roles and responsibilities through a responsible, accountable, consulted and informed (RACI) framework, set escalation thresholds and maintain conflict management protocols and decision logs.

Investigation governance should define not only who owns a matter but also who may access information about it. A formal need-to-know protocol should limit information sharing to those with a legitimate investigation, oversight or legal requirement.

The protocol should establish confidentiality boundaries, access controls and communication expectations for key stakeholders, while respecting requests for anonymity wherever possible. These measures help protect evidence integrity, safeguard participants and prevent unnecessary disclosure of sensitive information.

- **Ask yourself:** Who owns the matter, who has the authority to approve its scope, reporting and closure, and who genuinely needs access to investigation information?

- **Evidence of readiness:** Approved investigation charter, role matrix, conflict declarations, committee minutes, decision logs, need-to-know protocol and communication matrix.

Readiness checkpoint 02

Legal and regulatory readiness

Investigations frequently raise legal, regulatory and privilege considerations. Organizations should have protocols in place to assess privilege, understand jurisdiction-specific requirements, identify reporting triggers and engage external counsel where necessary.

- **Ask yourself:** Have legal purpose, privilege considerations and disclosure obligations been assessed and documented?

- **Evidence of readiness:** Privilege memoranda, regulatory trigger matrices, counsel instructions and reporting records.

Readiness checkpoint 03

Investigation risk assessment

Investigative steps can create or intensify risks, even when the underlying allegation is credible. Organizations should therefore conduct an initial risk assessment when a matter is opened and refresh it throughout the investigation as facts, stakeholders and circumstances change.

The assessment should consider potential evidence loss or tampering, retaliation or pressure affecting reporters and witnesses, conflicts of interest, confidentiality breaches, continuing misconduct, legal or regulatory deadlines, cross-border restrictions, business disruption and risks to the integrity of the investigative process. Each material risk should have a defined owner, mitigation action and escalation route.

- **Ask yourself:** Are risks to people, evidence, confidentiality and business continuity being identified and reassessed throughout the investigation?

- **Evidence of readiness:** Investigation risk-assessment template, risk register, mitigation plan, escalation records and periodic review notes.

Safeguarding reporters and witnesses

Investigation readiness should include practical measures to protect reporters and witnesses from retaliation, intimidation, unnecessary exposure and inadvertent identification. Relevant risks should be assessed from the outset and reviewed as the matter progresses, particularly where the allegation concerns senior personnel, sensitive conduct, or individuals within the reporter's management chain.

Organizations should define how retaliation concerns are reported and escalated, who is responsible for implementing protective measures, and how confidentiality will be maintained to the extent possible. Investigation teams should also coordinate with HR, legal, security and other appropriate functions where interim safeguards are required. Any concern relating to retaliation, interference with witnesses or leakage of confidential information should be documented and addressed promptly.

- **Ask yourself:** Can reporters and witnesses raise concerns safely during an investigation, and is there a predefined route for responding to potential retaliation?

- **Evidence of readiness:** Anti-retaliation protocol, witness risk-assessment record, escalation pathway, confidentiality guidance and documented protective actions.

Readiness checkpoint 04

Forensic data readiness

Preserving evidence in a defensible manner is critical to maintaining the integrity of an investigation. This requires an understanding of key data sources, retention requirements, legal hold procedures and chain-of-custody processes.

Ask yourself: Can relevant evidence be identified, preserved and collected without compromising its integrity, context, or metadata?

Evidence of readiness: Data maps, preservation registers, hash records and secure evidence repositories.

Readiness checkpoint 05

Case management and investigation documentation

Organizations should define the minimum records required for a complete investigation file and maintain them in a secure, access-controlled case-management environment. At a minimum, the case file should contain the initial allegation or intake record, the triage assessment, investigation plan or terms of reference, risk assessment, key decision record, evidence register, interview records, findings, review and approval records, final report and remediation or closure documentation. The file should enable an independent reviewer to understand what was alleged, how the matter was assessed, what evidence was considered, why key decisions were taken, and how the outcome was reached.

A designated reviewer should verify case-file completeness and the quality of the investigation report before closure. Closure criteria should specify who may approve closure, what mandatory records must be present, and how outstanding remediation actions will continue to be monitored.

Ask yourself: Could an independent reviewer reconstruct the investigation and understand the basis for its findings from the case file alone?

Evidence of readiness: Case-file index, standard terms of reference, investigation plan, decision log, evidence register, interview templates, quality-assurance checklist and closure approval record.

Readiness checkpoint 06

Technology and analytics

Technology can significantly enhance the speed and effectiveness of investigations. Organizations should evaluate whether they have access to appropriate eDiscovery tools, transaction analytics capabilities, case management systems, dashboards and governance frameworks for the use of AI.

- **Ask yourself:** Are analytical procedures reproducible, transparent, and subject to appropriate validation and review?

- **Evidence of readiness:** Use-case approvals, validation records, tool and model inventories and reviewer sign-offs.

Readiness checkpoint 07

People and surge capacity

Investigations often require specialist expertise and the ability to mobilize resources quickly. Organizations should identify a core response team, maintain access to specialist advisers, and ensure the availability of trained interviewers, translators and field personnel when required.

- **Ask yourself:** Can the organization rapidly deploy qualified, independent resources when a significant matter arises?

- **Evidence of readiness:** Contact trees, vendor retainers, training records and tabletop exercise results.

Readiness checkpoint 08

Learning and remediation

An investigation should not end with a final report. Organizations should establish mechanisms to identify root causes, track remediation activities, validate corrective actions and capture lessons learned to strengthen future resilience.

- **Ask yourself:** Are remediation actions tracked to closure and monitored to prevent recurrence?

- **Evidence of readiness:** Remediation trackers, validated closure documentation, updated controls and readiness dashboards.

Building investigative readiness: A timeline

Investigation readiness is not built overnight. Adopting a phased response strategy that prioritizes foundational governance, strengthens operational capabilities, tests response mechanisms, and continually evolves in line with emerging risks and regulatory expectations. By sequencing actions across short- medium- and long-term horizons, organizations can establish a sustainable framework that enables timely, coordinated, and defensible responses to incidents while continuously improving their preparedness.

First 90 days

Lay the foundation

The initial focus should be on putting together the core elements that will be required to respond to an investigation from day one. This includes approving an investigation charter and escalation thresholds, identifying the core investigation team and alternates, mapping priority evidence sources, reviewing critical vendor contracts and conducting at least one tabletop exercise.

Key deliverables during this period

- Board-approved charter
- Contact tree
- Data map
- Preservation templates
- Tabletop action log

Q **Board-level question to be asked**

Can we identify accountable decision-makers and protect priority evidence from day one?

3-6 months

Strengthen processes and capabilities

Once foundational elements are established, organizations should focus on formalizing standards and enabling consistent execution. This includes setting minimum logging and retention standards, configuring a secure case repository, establishing an AI use policy, and training legal, compliance, IT, HR and business responders.

Key deliverables during this period

- Logging standard
- Secure case management repository
- AI-use register
- Training records

Q **Board-level question to be asked**

Can we demonstrate that investigation technology is governed and human-reviewed?

6-12 months

Test resilience and scalability

As capabilities mature, organizations should challenge and refine their readiness through more complex scenarios. Priority actions include testing cross-border and data-related matters, integrating whistleblowing and incident data, establishing surge capacity and measuring remediation closure.

Key deliverables during this period

- Scenario testing results
- Regulator trigger matrix
- Vendor readiness documentation
- Remediation dashboard

Q **Board-level question to be asked**

Can we respond to a multi-jurisdictional matter without losing time or privilege?

Continuous

Sustain and improve readiness

Investigation readiness should be treated as a continuous program rather than a one-time exercise. Organizations should regularly refresh regulations, contacts, data maps, AI use cases and playbooks, while reviewing closed matters to identify recurring themes and opportunities for improvement.

Key deliverables during this period

- Quarterly readiness dashboard
- Annual independent effectiveness review

Q **Board-level question to be asked**

Do closed investigations measurably improve our controls and monitoring?

Based on the themes developed across the playbook, this section brings the insights together into a forward-looking perspective on how organizations can build investigation functions that are resilient, technology-enabled and legally defensible. It reinforces the key messages from the preceding sections while outlining practical priorities for the road ahead.

Section 4

The road ahead: Building resilient and future-ready investigations

The investigations landscape is entering a period of significant transformation. Rapid technological change, evolving regulatory expectations, increasing volumes of digital evidence, cross-border complexities, and heightened stakeholder scrutiny are fundamentally changing how organizations identify, assess and respond to allegations. Investigations are no longer viewed as isolated compliance exercises. They are becoming a core component of organizational governance, risk management and resilience.

As highlighted throughout this playbook, successful investigations of the future will require more than advanced tools or reactive response mechanisms. Organizations will need to build investigation capabilities that are proactive, multidisciplinary and embedded into broader risk and compliance frameworks. Readiness, rather than response alone, will increasingly determine the effectiveness and defensibility of an investigation.

Technology will continue to play a pivotal role in accelerating investigations through analytics, automation, digital forensics and AI-enabled workflows. However, technology must operate within clear governance frameworks supported by human judgment, legal oversight, transparency and accountability. The most effective organizations will be those that successfully combine technology-enabled intelligence with experienced professionals capable of interpreting facts, exercising judgment and managing complex stakeholder considerations.

At the same time, legal and regulatory considerations must remain central to investigation design. Privilege, privacy, evidence integrity, cross-border compliance and documentation requirements should be incorporated from the outset rather than addressed retrospectively. Organizations that integrate legal readiness into their investigation operating model will be better positioned to withstand regulatory scrutiny and defend investigative outcomes.

Ultimately, the future of investigations will be shaped by an organization's ability to respond with speed, integrity and confidence while maintaining trust among regulators, employees, customers and other stakeholders. Organizations that invest today in readiness, governance, technology and capability development will be best positioned to navigate tomorrow's risks and build sustainable resilience.

Key takeaways

1. **Treat investigation** readiness as a continuous capability, not a crisis response.
2. **Establish clear** governance, ownership and escalation mechanisms.
3. **Build multidisciplinary teams** that can respond quickly and cohesively.
4. **Strengthen** forensic readiness and evidence preservation processes.
5. **Adopt AI** and advanced analytics responsibly, with appropriate controls and human oversight.
6. **Embed** legal, regulatory and privacy considerations throughout the investigation lifecycle.
7. **Use investigation outcomes** to drive remediation, enhance controls and strengthen organizational resilience.
8. **Regularly test and update** investigation frameworks to address emerging risks and changing regulatory expectations.

Contributors

EY

Arpinder Singh
India & Emerging Markets Leader,
EY Forensic & Integrity Services
Arpinder.Singh@in.ey.com

Saguna Sodhi
Partner, EY Forensic & Integrity Services
Saguna.Sodhi@in.ey.com

JSA

Rupinder Malik
Partner, JSA and Chapter Leader,
WWCDA India Chapter
Rupinder.Malik@jsalaw.com

Ishita Parashar
Principal Associate, JSA
Ishita.Parashar@jsalaw.com

Divyaanshi Chandra
Principal Associate, JSA
Divyaanshi.Chandra@jsalaw.com

Disclaimer

1. This playbook should not be constituted as legal advice.
2. External counsel should be involved after thorough consideration of the allegations, privilege objectives, regulatory exposure, and, more importantly, the applicable law and jurisdiction.
3. Market enquiries should be subject to prior legal, privacy and applicable law and jurisdiction.

Ernst & Young LLP

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EYG member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/en_in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at Ground Floor, Plot No. 67, Institutional Area, Sector - 44, Gurugram, Haryana - 122 003, India.

EYIN2609-016
ED None

MMA

ey.com/en_in

EY_India EY EY India EY Careers India ey_india