

CA. (Dr.) Durgesh Pandey
Member of the Institute

Forensic Readiness in Practice: The FRMM Approach

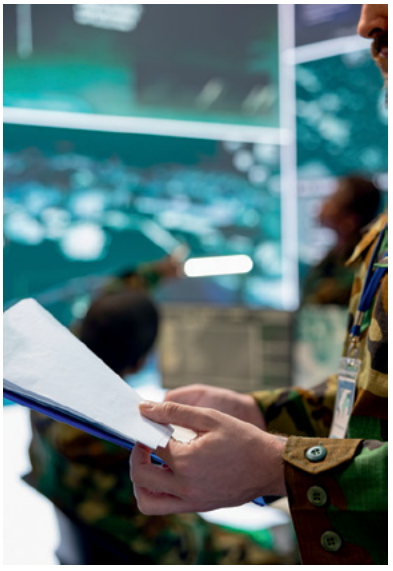
A whistleblower complaint followed by an allegation may set functions in motion before an organisation appoints a forensic professional. However, important decisions concerning authority, evidence, access and reporting may already shape the investigation during that appointment interval. This article introduces the Forensic Readiness Maturity Model (FRMM), an author-developed model for assessing an organisation's preparedness to respond to such suspected financial misconduct. It distinguishes forensic readiness from fraud risk management and explains how the model complements ICAI's Forensic Accounting and Investigation Standards (FAIS). FRMM examines four independent domains: Governance, Recognition and Escalation; Investigation Capability; Evidence and Analytical Reliability; and Remediation and Organisational Learning. Each domain is considered across four maturity levels: Reactive, Defined, Managed and Embedded. The article shows how readiness may influence engagement scope, evidence strategy, reporting arrangements and follow-up using an illustrative case. It also considers how FRMM can support scoping, assessment and remediation without displacing the professional's responsibilities under FAIS.

The audit committee chair on Monday morning opens an email from the whistleblower channel. The email names a senior executive and alleges that procurement contracts were awarded to connected entities and includes three transaction references, two vendor names, and copies of invoices. It is detailed enough to demand attention, although no one yet knows whether the allegation is true. Management wants to know how quickly it can present a preliminary view to the board. The organisation has started responding by noon. Internal audit starts examining the transactions. Procurement has been asked to provide vendor records, and Legal has downloaded the attachments. Another team is extracting emails from the accounts identified in the complaint. Each function is already trying to shape the investigation, raising important questions. Was the complaint preserved in its original form? Can the extracted emails and vendor records be traced back to their sources? Who authorised the review, and where will it report if the allegation reaches the person who normally controls access? By the time an external Professional is appointed, important decisions concerning authority, evidence and scope may already have been made.

What follows the tip

The whistleblower channel is not an exceptional starting point. The Association of Certified Fraud Examiners (ACFE's) *Occupational Fraud 2026: A Report to the Nations*, covering 2,402 cases across 143 countries and territories, found that 43% of occupational fraud cases were detected through tips. A tip may bring the matter to light, but the quality of the response that follows depends on what the organisation already has in place. Once the allegation moves towards a formal inquiry, this organisational readiness must work alongside a clear professional framework for conducting the engagement.

In India, that professional framework has acquired a more defined structure in recent years. ICAI became the first accounting body in the world to issue detailed Forensic Accounting and Investigation Standards (FAIS). The FAIS were implemented for forensic engagements undertaken by ICAI members on 01 July 2023. An implementation guide was also issued to support their application. The Standards were an important development for a field in which the terminology, mandate, procedures and expected outputs could vary considerably from one engagement to



another. A forensic engagement may influence disciplinary proceedings, regulatory action, recovery efforts, litigation or criminal investigation. The work may later be questioned by people who were not present when the engagement began. Consistency in how the Professional accepts, plans, conducts, documents and reports the work therefore matters.

FAIS provides professional discipline. The standards also clarify the distinction between a forensic engagement and a conventional audit, an area where expectations have often been blurred. In practice, however, much also depends on the organisation. The Professional needs a clear mandate, access to reliable records and support from the relevant teams. There should also be an independent reporting route, particularly where senior personnel may be involved. If these arrangements are unclear, the investigation can lose valuable time at the outset. It may also affect the evidence available and the usefulness of the final report.

An organisation may have a whistle-blower mechanism, an active audit committee and a detailed fraud-risk register. Yet it may still struggle when an allegation requires a forensic response. Existing policies do not always show whether the matter can be recognised and escalated promptly, the right capability mobilised, evidence handled reliably, or lessons carried into remediation.

The Forensic Readiness Maturity Model (FRMM) assesses these practical conditions. It complements FAIS by helping the Professional understand the organisational environment in which the engagement will be carried out. The real test begins when an allegation arrives. At that point, the organisation has to work with the arrangements it already has.

Risk Awareness and Forensic Readiness

Most organisations already have processes for identifying and recording fraud risks. These processes help them recognise vulnerable transactions, functions and relationships. However, the presence of a risk register or preventive controls does not necessarily show how the organisation will handle an actual allegation.

The idea of forensic readiness has developed over more than two decades. Tan (2001) approached it through an organisation's preparedness to collect credible digital evidence while controlling the cost of an investigation. Rowlingson (2004) later set out a ten-step process for building forensic readiness. Englbrecht, Meier and Pernul (2020) developed this further through a capability maturity model for digital forensic readiness. Much of this literature emerged from the field of digital evidence, although it established a wider principle: readiness must be built before an incident if it is to support the response that follows.

The distinction can be stated simply:

> "ICAI became the first accounting body in the world to issue detailed Forensic Accounting and Investigation Standards (FAIS)."

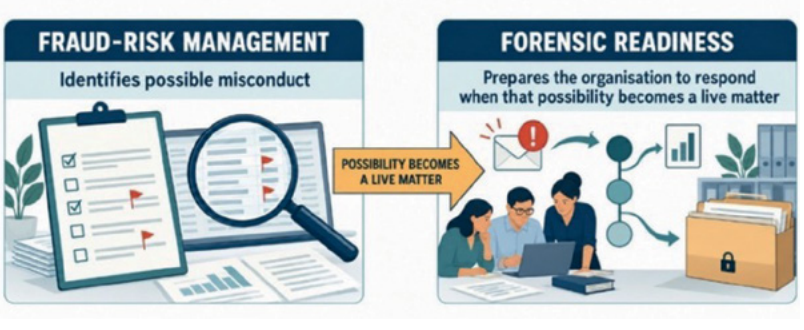
In the opening example, procurement may already be recognised as a high-risk area. That says little about how the complaint will be handled. The organisation still needs an independent escalation route and reliable evidence. It must also be able to bring in suitable capability and act on what the investigation ultimately reveals.

The FRMM gives structure to these aspects of organisational response. It examines the conditions surrounding the response, how well those conditions operate in practice and what they mean for the Professional conducting the engagement.

Forensic Readiness Maturity Model (FRMM)

The model is built around four areas of organisational readiness:

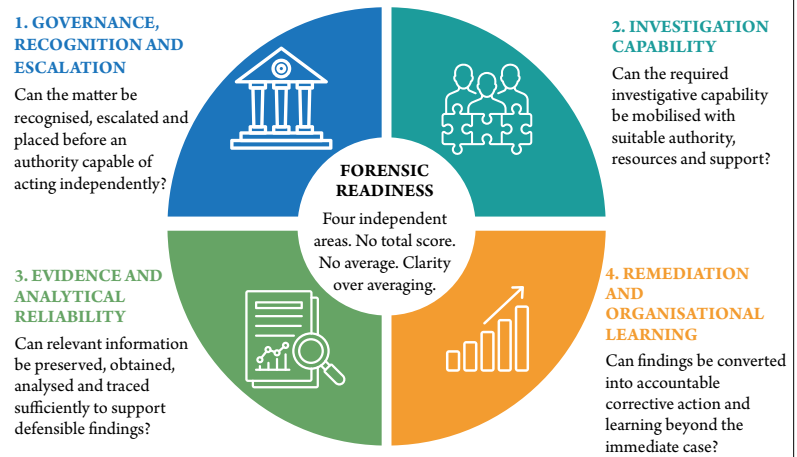
- **Governance, Recognition and Escalation** considers whether a suspected matter can reach the appropriate authority in time. It also examines whether that authority can commission and oversee an independent response, particularly when senior personnel may be involved.
- **Investigation Capability** considers whether the organisation



can mobilise suitable people and specialist support. Not every organisation needs a permanent forensic team. It should, however, have a workable way to obtain the required capability and support it internally.

- **Evidence and Analytical Reliability** considers how records are preserved, obtained and used. The Professional should be able to trace the path from the original source to the analysis and, eventually, to the finding.
- **Remediation and Organisational Learning** considers what happens after the immediate matter has been examined. It looks at whether findings lead to corrective action and whether the lessons are carried to other parts of the organisation where the same weakness may exist.

FIGURE 1 THE FOUR QUESTIONS OF FORENSIC READINESS



The four domains often affect one another. The model still considers each one separately. An organisation may have a clear authority structure and yet lose important evidence. It may maintain reliable systems but lack an independent reporting route for concerns involving senior management. The investigation itself may be handled well, while the same weakness later appears in another unit. Strength in one domain is therefore not used to offset weakness in another.

Reading Maturity

Each domain is therefore read on its own maturity scale. Maturity reflects how far the relevant arrangements have developed into something the organisation can depend on. In simple terms, the four levels – Reactive, Defined, Managed, and Embedded – distinguish between working out a response after a complaint arrives, having that response written down, knowing that it works, and keeping it ready between incidents.

It shows how an organisation's readiness moves from an event-driven response to an established organisational capability.

Reactive	Defined	Managed	Embedded
The response is assembled after the matter surfaces.	A documented response route exists.	The route has operated, and its use can be demonstrated.	Readiness is maintained and improved between incidents.

The levels apply separately to each of the four domains. An organisation may have a tested route for escalating a complaint and still handle evidence poorly. It may be able to appoint specialists quickly but have no process for checking whether earlier recommendations actually worked. The FRMM preserves these differences instead of reducing them to one overall score.

> "The Forensic Readiness Maturity Model (FRMM) assesses these practical conditions. It complements FAIS by helping the Professional understand the organisational environment in which the engagement will be carried out."

A higher level also does not mean that every person will perform well. Similarly, a Reactive organisation may contain an experienced individual who handles the matter effectively. The model looks at what the organisation can depend on, even when particular individuals are unavailable.

The earlier procurement complaint helps illustrate how this works. During scoping, the Professional also considers how well the organisation can support the investigation.

The FRMM assessment therefore does more than describe the organisation. It helps the Professional decide how the engagement should be planned and where additional safeguards may be required.

Using FRMM Alongside FAIS

FRMM and FAIS serve related purposes. However, FRMM is particularly useful during scoping, when the mandate, reporting arrangements, access requirements and expected support are being settled. FRMM approaches the engagement from the other side. The FAIS principally governs what the Professional must do. FRMM evaluates whether the organisation is ready to support the environment in which that work has to be done.

The relationship should therefore be seen as complementary, not as a formal cross-mapping of two frameworks.

A few connections illustrate the point as described in figure 2 below.

1

What the Professional finds

- The audit committee has authority to commission the engagement, but the separate route for matters involving senior management has never been tested.
- Forensic specialists and internal coordinators are available, but the organisation has not tested how they would work together.
- Relevant emails have been copied, but the organisation cannot demonstrate how they were extracted or who had access to them.
- Earlier recommendations were marked as closed without checking whether the corrective measures had worked.

2

What the Profile shows

- Governance, Recognition and Escalation is **Defined.**
- Investigation Capability is **Defined.**
- Evidence and Analytical Reliability is **Reaction.**
- Remediation and Organisation Learning is **Reactive.**

3

What changes in the engagement

- Original records must be secured.
- Existing extracts must be verified against their sources.
- The reporting and escalation route must be confirmed.
- The scope may need to extend to other divisions where the same weakness could exist.

FIGURE 2 FRMM READINESS AND SELECTED FAIS TOUCHPOINTS

Illustrative Connections. FRMM is not part of FAIS.

FRMM READINESS AREA	ILLUSTRATIVE FAIS TOUCHPOINTS
1. Governance, Recognition and Escalation	■ FAIS 110 Nature of Engagement ■ FAIS 210 Engagement Objectives ■ FAIS 220 Engagement Acceptance and Appointment ■ FAIS 250 Communication with Stakeholders
2. Investigation Capability	■ FAIS 230 Using the Work of an Expert ■ FAIS 310 Planning the assignment ■ FAIS 340 Conducting Interviews ■ FAIS 350 Review and Supervision
3. Evidence and Analytical Reliability	■ FAIS 320 Evidence and Documentation ■ FAIS 330 Conducting Work Procedures ■ FAIS 410 Applying Data Analysing ■ FAIS 420 Evidence Gathering in Digital Domain
4. Remediation and Organisational Learning	■ FAIS 510 Reporting Result ■ FAIS 610 Quality Control

The connections above are illustrative. FRMM is not part of FAIS and does nor replace compliance with any applicable Standard.

The relationship between FRMM and FAIS becomes clearer during an actual engagement. Suppose the Professional may begin with a clear objective. But if the organisation's governance arrangements are uncertain, it may still be unclear who can approve a change in scope or direction.

Similar difficulties may arise during the planning phase of FAIS. The engagement plan may assume that certain records and internal support will be readily available. If the organisation, however, cannot provide them, the timetable and approach may have to change. Another checkpoint is evidence and analysis. The Professional may follow the relevant FAIS requirements, but poor handling of records could require substantial reconstruction before the analysis can begin.

Finally, when the engagement reaches the reporting stage, a sound report does not automatically lead to corrective action. The FAIS guides the Professional's reporting responsibilities. The final FRMM domain considers what the organisation does after the findings are communicated. This includes remediation, follow-up and carrying relevant lessons to other parts of the organisation.



> "In simple terms, the four levels – Reactive, Defined, Managed, and Embedded – distinguish between working out a response after a complaint arrives, having that response written down, knowing that it works, and keeping it ready between incidents."

Readiness Before the Warning Light

At cruising altitude, a flight crew decides how to manage an emergency without waiting for a warning light. This is because responsibilities are assigned in advance, checklists are available, and difficult situations are rehearsed in simulators. The crew may never face that exact emergency during a real flight. Yet the response has been practised because decisions made under pressure cannot depend entirely on improvisation.

Forensic readiness follows the same principle. While FAIS gives the professional the discipline to conduct the engagement, FRMM examines whether the organisation is prepared to support that work. When the Monday morning complaint arrives, the reporting route, available capability and evidence practices are no longer matters confined to policy. They begin shaping the investigation immediately. FRMM helps the organisation test these arrangements before an allegation arises and helps the Professional understand them when one does. The allegation itself may be unexpected, but the response should already be familiar. After all, the best time to test it is while the warning light is still off.

References

- *Association of Certified Fraud Examiners. (2026). Occupational fraud 2026: A report to the nations. https://www.acfe.com/report-to-the-nations*



- *Englbrecht, L., Meier, S., & Pernul, G. (2020). Towards a capability maturity model for digital forensic readiness. Wireless Networks, 26(7), 4895–4907. https://doi.org/10.1007/s11276-018-01920-5*
- *Institute of Chartered Accountants of India, Digital Accounting and Assurance Board. (2025). Compendium of Forensic Accounting and Investigation Standards (revised 2025). https://resource.cdn.icai.org/75009daab030723.pdf*
- *Rowlingson, R. (2004). A ten-step process for forensic readiness. International Journal of Digital Evidence, 2(3), 1–28.*
- *Tan, J. (2001, July 17). Forensic readiness [Technical report]. @stake, Inc.*

Author may be reached at durgesh.pandey@gmail.com and eboard@icai.in