

Future-Proof Your Strategy

Having a proactive fraud strategy is essential for organizations to stay ahead of increasingly sophisticated threats, designed to support efforts to prevent, detect, respond to, and recover from fraud before significant damage occurs.

1. Response

- Assemble an independent investigation team and define investigation goals.
- Preserve all evidence and avoid impulsive actions that could compromise the investigation.
- Contain and isolate the threat.

2. Recovery

- Eradicate threats and restore systems from clean backups or by re-imaging, helping to ensure all vulnerabilities are patched.
- Refine the investigation plan as new findings emerge and communicate this with stakeholders.
- Effectively and efficiently gauge your internal controls.

4. Detect

- Implement proactive data monitoring and analytics (e.g., Payment Risk Analytics) to target high-risk areas.
- Promote and act on tips by maintaining a formal program for receiving, investigating, and resolving tips.
- Conduct regular risk assessments, vulnerability scans, and penetration testing.

3. Prevent

- Provide regular fraud training to personnel and empower them to report concerns without fear of retaliation.
- Strengthen internal controls, including segregation of duties and updated policies.
- Establish anonymous reporting hotlines (e.g., IntegraReport) to encourage a culture of communication.
- Embed cyber resilience in every layer of your organization.



End-to-End Fraud Risk Support From Forvis Mazars

Helping you tackle today's challenges head-on with an experienced team.



[Analytics](#)



[Forensics](#)



[Cybersecurity](#)



[Payment Risk Analytics](#)



[IntegraReport](#)



[Internal Audit](#)

Proactive Data Monitoring

53%

large organizations

19%

small organizations

Despite its effectiveness, only 53% of large organizations and 19% of small organizations use proactive data monitoring.