The Institute of Internal Auditors Malaysia

Technical Newsletter

Issue 3/2026
2 March 2026

Cybersecurity, Data Integrity & Fraud : The New Risk Triangle for Internal Auditors

The Institute of Internal Auditors Malaysia

Technical Newsletter

Issue 3/2026
2 March 2026

FRAUD HAS GONE SYSTEM-ENABLED. ASSURANCE STILL THINKS IN SILOS

Fraud has not changed its nature but its terrain has evolved in today's digital environment. People still commit fraud because of pressure, opportunity and rationalisation but where opportunity now arises and how fraud is executed have shifted dramatically. Nowadays, fraud rarely begins with forged documents or manual overrides. It begins with a login, a compromised identity, a poorly governed dataset. Yes, a system designed for efficiency, not resilience.

For decades, internal auditors have been trained to look for fraud in processes, approvals and reconciliations. Whilst this approach had probably worked in yesterday's largely manual world, the recent digital transformations that swiped across corporations have quietly changed the mechanics of fraud. A stolen credential can grant access that bypasses layers of formal approval. Poorly governed master data can be manipulated without triggering exceptions. Inadequate logging or short log retention can erase the trail before suspicions even arise. Fraud, in other words, has become system-enabled.

This has profound implications for internal auditors. While fraud risk, cybersecurity and data governance are often managed as separate disciplines, modern fraudsters exploit technology to span all three domains simultaneously. Therefore to remain effective, IA must learn to see them as a single, interconnected risk landscape.

The Institute of Internal Auditors Malaysia

Technical Newsletter

Issue 3/2026
2 March 2026

ONE CONVERGING RISK SURFACE : CYBERSECURITY × DATA INTEGRITY × FRAUD

To be effective today, IA needs to understand how the CIA Triad, data governance principles and the Fraud Triangle form a single risk ecosystem.

- **Cybersecurity** provides the technical guardrails, commonly framed through the CIA Triad — Confidentiality, Integrity and Availability. Frameworks such as NIST CSF and ISO/IEC 27001 emphasise identity management, access control, monitoring and system resilience. These are not just IT safeguards, they directly influence whether fraud opportunity exists.

- **Data integrity and governance** determine what can be changed, who is accountable, and whether changes are visible. Standards such as DAMA-DMBoK, COBIT 2019, ISO 8000 and ISO 38505-1 highlight data ownership, lineage, quality and stewardship as prerequisites for trust in information.

- **Fraud risk**, grounded in the Fraud Triangle and reinforced by ACFE Fraud Tree and COSO Fraud Risk Management Guide, explains the human drivers - Pressure, Opportunity and Rationalisation.

The connection is straightforward but often overlooked:

- Cybersecurity weaknesses create opportunity by allowing unauthorised or excessive access.
- Data governance weaknesses enable execution and concealment by allowing data to be altered without detection or traceability.
- Human pressure and rationalisation activate the fraud once opportunity exists.

Fraud does not sit neatly in any one of these domains. It emerges at their intersection. This is the new risk triangle internal auditors must learn to navigate.

The Institute of Internal Auditors Malaysia

Technical Newsletter

Issue 3/2026
2 March 2026

THE BLIND CORNERS : WHERE CYBER MEETS DATA MEETS FRAUD

Modern fraud rarely announces itself through obvious red flags. Instead, it unfolds quietly across systems.

(Real Case Examples)

1. A compromised identity remains one of the most powerful fraud enablers. This was evident in the 2023 **MGM Resorts cyberattack**, where threat actors used social-engineering techniques to gain access through legitimate employee credentials. Once inside, systems treated the attackers as authorised users, allowing them to disrupt operations and access sensitive information. The incident highlights how identity compromise enables high-impact outcomes that traditional control testing struggles to distinguish from legitimate activity.

2. A second blind corner lies in the manipulation of master data. For example, vendor records, bank account numbers and pricing tables are the control points that determine where money flows. If an attacker alters a single field, every downstream process can be subverted. Privilege escalation within ERP systems allows fraudsters to create fake vendors or redirect payments despite of approval workflows and SoD requirements appeared fully compliant. When the source of truth is corrupted, internal controls become a façade.

Modern intrusions are also increasingly anti-forensic. Attackers understand how monitoring works, and they work around it. In the **MOVEit mass exploit** of 2023, threat actors deleted traces of their access, delaying discovery and giving themselves a longer window to weaponise stolen data. When system logs are disabled or altered, even the most sophisticated monitoring tools cannot detect what has already happened.

3. The 2023 leak of vaccination records from the **i-Sihat system** placed citizens' most sensitive personal details at risk. Vaccination records containing IC numbers and personal identifiers were leaked online thus risk exposure to fraudulent loan applications, medical claim scams, or extremely convincing social-engineering attacks.

All the above cases represent a convergence of cyber gaps, data weaknesses and human intent, where IA is least equipped if it continues to operate in silos

THE NEW REALITY : WHAT IA MUST DO DIFFERENTLY

Addressing this new reality does not require IA to become cybersecurity specialists or data engineers. It does, however, require a fundamental shift in how auditors interpret opportunity within the Fraud Triangle.

1. Read the Fraud Triangle through a digital lens because Opportunity is increasingly shaped by identity and access controls embedded within systems, including:

- Identity and Access Management (IAM) design and governance
- Privilege escalation pathways
- Multi-Factor Authentication (MFA) coverage and enforcement
- Use of shared or generic accounts
- Data modification rights within critical systems
- Gaps in logging, monitoring and alerting

A Fraud Risk Assessment that does not explicitly consider these digital dimensions of opportunity is, by definition, incomplete.

2. IA should treat cybersecurity principles not as purely technical safeguards, but as core fraud controls. This requires evaluating how systems prevent, enable or conceal unauthorised activity by examining:

- The design and enforcement of authentication mechanisms
- Segregation of Duties embedded within system roles and workflows
- Governance over APIs and system-to-system integrations
- Endpoint hygiene, including device security and access discipline
- Incident Response capabilities, particularly speed of containment and evidence preservation

Frameworks such as the NIST Cybersecurity Framework, ISO/IEC 27001, and the CIS Critical Security Controls provide clear, practical guidance that IA can leverage without becoming cybersecurity specialists.

The Institute of Internal Auditors Malaysia

Technical Newsletter

Issue 3/2026
2 March 2026

3. Data governance determines whether fraud can be detected, investigated and proven. IA should therefore assess the integrity of data controls by examining:

- Clear data ownership and accountability
- Master data workflows and approval mechanisms
- Data lineage and traceability across systems
- Metadata quality, including completeness and accuracy
- Exception handling and override pathways

Frameworks such as DAMA-DMBoK, ISO 8000, ISO 38505-1, and COBIT give IA a common language and measurable criteria to assess these areas holistically.

4. Rather than focusing solely on control design, IA should adopt attacker-pathway thinking by asking three simple but powerful questions:

- "Can someone break in?" - identity strength, privileged access governance, endpoint security
- "If they can, what can they change?" - data integrity controls, master data governance, transaction rules, audit trails
- "If they change it, will anyone know?" - fraud monitoring effectiveness, log correlation, behavioural anomaly detection

To assess whether controls would withstand real-world threats, IA can further stress-test key controls by simulating scenarios such as credential compromise or master data manipulation.

KEY TAKE-AWAYS

1. The Fraud Triangle still explains why fraud happens. The CIA Triad explains how digital opportunity is created. Data governance determines whether fraud is visible, traceable and provable. None of these models is sufficient on its own.

2. In a digital organisation, compromised identity produces clean transactions. Poorly governed data provides the perfect hiding place. Weak logging erases accountability. The challenge is that these controls are not integrated across the pathways attackers exploit.

3. Cybersecurity may determine who gets in, data governance determines whether IA can trace what the fraudsters did. For internal auditors willing to embrace this integrated view, the challenge is significant and so is the opportunity to redefine the value of assurance.

Author: Javen Khoo Ai Wee, CIA, CISA, AAIA, CFE, ISC² CC
CMIIA Membership No. 211787

REFERENCES:

1. *(https://www.wsj.com/articles/mgm-resorts-cyberattack-social-engineering-11695112984) MGM Resorts cyberattack (WSJ, 2023) – compromised identity*

2. *(https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a) MOVEit mass exploit (CISA, 2023) – anti-forensics & data exfiltration*

3. *(https://vgh.pth.mybluehost.me/2023/02/audit-mysejahtera-data-breach-affected-three-million-users/) i-Sihat data exposure (audit/media) – data integrity & downstream fraud*