Engineering and Technology Journal e-ISSN: 2456-3358

Volume 10 Issue 12 December-2025, Page No.-8004-8013

DOI: 10.47191/etj/v10i12.03, I.F. – 8.482

A Holistic Approach for Insider Threat Assessment and Mitigation

Fatai A. Akinsola[1], Francisca N. Ogwueleka[2], Uche M. Mbanaso[3]

[1,3]Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria

[2]Department of Computer Science, University of Abuja, Abuja-FCT, Nigeria

ABSTRACT: In recent times, insider threats have become one of the most complex and persistent cybersecurity challenges to manage, primarily because insiders are trusted and have legitimate access to organisational systems and data. Both public and private organisations face considerable risks of financial losses, data breaches, operational disruptions, and reputational damage resulting from malicious or negligent insiders. This study introduces the All-inclusive Threat and Organisational Mitigation (ATOM) Framework, a comprehensive and adaptable model designed to understand, detect, and mitigate insider risks through an integrated, layered, and structured approach. Unlike traditional strategies that focus narrowly on individual or technical factors, the ATOM framework aligns security measures with organisational objectives, governance policies, and regulatory compliance requirements. It emphasises proactive protection of sensitive digital assets and advocates a holistic approach that combines human behaviour analysis, technical monitoring, and organisational resilience. The framework provides practical tools and insights that assist organisations in anticipating, assessing, and counteracting insider threats more effectively. It also explores innovative analytical and technological methods to enhance detection, prevention, and response capabilities. The framework underscores the importance of proactive monitoring of human behaviours, vulnerabilities, and indicators of insider threats to close cybersecurity gaps and strengthen the resilience of critical systems and information. Additionally, the work is currently examining artificial intelligence (AI)-driven adaptive deception techniques that generate convincing fake data to mislead and monitor insider behaviour, while carefully considering associated ethical considerations.

KEYWORDS: Insiders, risk, privacy, vulnerabilities, zero-trust, cyber asset

1. INTRODUCTION

The rise in cybercrime and insider threat incidents has been fueled by increasing digitisation, widespread automation, and the shift to remote and hybrid work (Hoffmann, 2020). These technological advancements, while beneficial, have expanded the digital attack surface, leading to more frequent and costly cyberattacks worldwide (Global Cybersecurity Outlook, 2022). Cyber threats take many forms, including data breaches, hacking, identity theft, ransomware, and phishing, with serious social and economic consequences that can disrupt individuals, organisations, and entire societies (Agrafiotis et al., 2018).

Organisations face insider threats for various reasons, ranging from employee dissatisfaction and workplace conflicts to personal gain, sabotage, or retaliation (Subhani, 2021). Insider threats can be as damaging as external attacks, often leading to severe financial and reputational harm (Max, 2018). The growing prevalence of insider incidents underscores the urgent need for cohesive, pragmatic strategies to manage these risks effectively. Organisations must adopt comprehensive prevention and detection measures that consider both the human and technological dimensions of security.

Insider threats are particularly challenging because perpetrators operate from within, using legitimate access to exploit organisational vulnerabilities in people, processes, and technology. They often possess deep knowledge of systems and controls, allowing them to bypass safeguards and compromise sensitive assets. Even under zero-trust architectures, which enforce strict authentication and authorisation, insiders still retain privileged access and can exploit non-technical weaknesses, such as human or procedural gaps (ISACA, 2021). Not all insider incidents are malicious, as many stem from negligence or human error (Thompson, 2020). Therefore, combating insider threats requires a multi-layered strategy combining technical defences, behavioural monitoring, training, and cultural awareness to detect, prevent, and mitigate both intentional and accidental breaches.

2. THE ANATOMY OF INSIDER THREATS

There are reasons to worry about insiders, whether intentional or unintentional. Understanding the various insider types enables security practitioners to identify threat origins and motivations and to determine where to focus prevention and mitigation efforts. The different insiders that represent a significant threat include:

a. **Unintentional Insider:** Employees who unintentionally cause harm due to ignorance or carelessness rather than malice (Al-Mhiqani et al.,

2020). They include negligent insiders, who mishandle sensitive data, and complacent insiders, who ignore security practices like password updates. Such individuals are often exploited through phishing or social engineering (Greitzer et al., 2019; Singleton, 2021).

b. **Traitors: T**hese are insiders who deliberately misuse their access privileges to harm the organisation. They have deep system knowledge and act in their own self-interest or with malicious intent (Al-Mhiqani et al., 2020; Homoliak et al., 2019).
c. **Masqueraders:** External attackers who steal legitimate insider credentials to impersonate employees and perform malicious activities. Unlike traitors, they lack insider knowledge but exploit stolen identities for unauthorised access (Liu et al., 2018).
d. **Insider Agents:** Employees who collaborate with external actors to carry out attacks against their organisation by providing insider access or information to aid outsiders in attacking their organisations (Rama, 2023).
e. **Departing Employees:** Staff leaving voluntarily or involuntarily who may steal or leak sensitive information for personal advantage, revenge, or to aid future employment (Ostendorf, 2023).
f. **Ex-Employees:** Former workers who left on bad terms and may act out of resentment or revenge, posing risks through retained access or insider knowledge (Al-Mhiqani et al., 2020).
g. **Supply Chain Insiders:** Third parties such as vendors, contractors, support contractors, and suppliers with authorised access who can endanger organisational systems or data. Outsourcing and shared privileges can weaken controls and heighten insider threats (Boakye-Gyan, 2021).

3. THE ROLE OF TRUST IN INSIDER THREAT MANIFESTATIONS

Insider threats undermine organisational trust, which is the cornerstone of any secure and functional system and workplace (Rafae et al., 2025). Organisations inherently rely on trust when granting employees, contractors, customers and partners authorisation to sensitive information, systems, and resources. Such authorisation implies a degree of trust (Kim et al., 2020). This trust assumes that individuals will use their privileges responsibly and in alignment with the company's policies and security goals. However, when an insider misuses this access either intentionally or unintentionally, it undermines the very foundation upon which the organisation's security posture and collaborative culture are built.

Trust provides the foundation of confidence that enables individuals, businesses, and governments to participate safely in digital interactions and transactions (Uche & Dandaura, 2021). It is noteworthy that the sense of betrayal that accompanies insider incidents often extends beyond the immediate damage, affecting morale, team dynamics, and the organisation's overall perception of safety. Moreover, the breach of trust caused by insider threats has wide-ranging implications that extend beyond financial or operational losses. Once violated, trust is exceedingly difficult to restore, leading to increased scrutiny, stricter internal controls, and a culture of suspicion that can hinder productivity and openness. It is noteworthy that increased job security is associated with greater organisational loyalty, which, in turn, reduces the likelihood of trust violations (Safa & Abroshan, 2025). Employees may begin to feel less valued or unnecessarily monitored, creating an environment of fear rather than collaboration. Thus, insider threats are not merely security incidents but breaches of confidence that challenge the integrity of human relationships within an organisation, emphasising the need for balanced security measures that protect assets while preserving mutual trust and employee dignity.

4. TAXONOMY OF INSIDER THREATS

The consequences of insider threats often manifest in various harmful outcomes, reflecting the different ways insiders can exploit their legitimate access to compromise organisational assets. Some of these outcomes include:

i. Data Theft: This is a case of malicious insiders using the access they have to steal sensitive data such as customer information, intellectual property, or business secrets in order to sell for profit-making or use to their benefit or gain a competitive advantage (Rakhi et al. 2025)
ii. Fraud: This involves falsification of financial records or misuse of sensitive information to steal money from the organisation. Examples include an insider obtaining and retaining information such as debit/credit card details for fraud and identity theft; modifying information without authorisation for one's own interest, and altering financial records or diverting funds (CERT, 2018; Thompson, 2020)
iii. Sabotage: Sabotage refers to malevolent, deliberate or harmful actions perpetrated by insiders such as an employee, partner, contractor, or vendor with authorised access to the organisation's information assets in order to damage the organisation's systems, infrastructure, reputation, or operations (Chauhan, 2024).
iv. Espionage: This is also known as spying. It is a situation in which an insider is hired by other organisations, foreign agents, or the government to collect confidential information without the company's knowledge or consent, typically for military, political, or economic advantage (Collins et al., 2016).

The common types of attacks organisations are concerned with are shown in Figure 2.

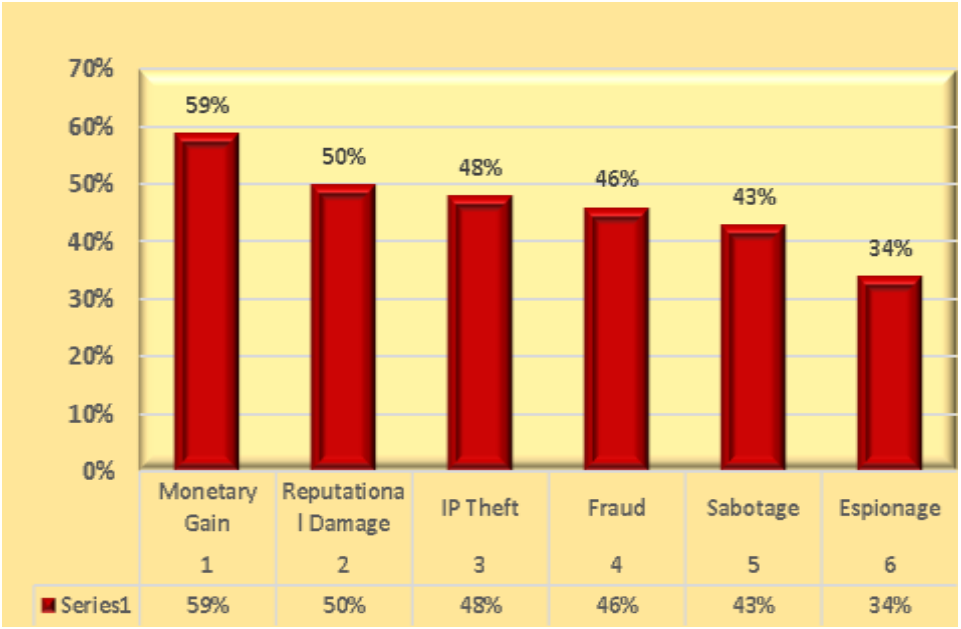

Figure 1: Percentage of insider attacks (Source: www.cybersecurity-insiders.com 2023 Insider Threat Report)

5. RELATED WORK

Insider attacks have grown in frequency and sophistication, prompting researchers to propose diverse frameworks and strategies for detection and mitigation. Scholars such as Modini et al. (2020) and Balakrishnan (2015) emphasise that managing insider threats requires a comprehensive, multi-faceted approach supported by top management, clear policies, and well-defined procedures. An effective insider threat program should not only detect and prevent attacks but also ensure timely response and recovery. This holistic approach underscores the importance of integrating organisational, technical, and human factors into insider threat management.

Recent studies have expanded on this by proposing innovative and technology-driven solutions. Rakhi et al. (2025) and Inayat et al. (2024) highlight the use of behavioural anomaly detection, privilege access management, and AI/ML-based monitoring, while Clifton (2024) and Chauhan (2024) introduce structured frameworks that combine proactive risk management, employee profiling, ethical oversight, and training. These models commonly enable real-time monitoring, behavioural analysis, and adaptive access control, collectively strengthening organisational resilience against insider threats.

Earlier contributions, such as those by Pureti (2022), Sauer (2022), and Alsowail & Al-Shehari (2022), emphasise the need for multi-stage, taxonomy-based frameworks. These works focus on understanding insider motivations, applying biometric and asset-based prevention, and developing cyclical processes that cover the entire employee lifecycle—from recruitment to exit. Other authors, including Boakye-Gyan (2021) and Subhani et al. (2021), emphasise best practices such as leadership involvement, awareness programs, behaviour monitoring, and tailored mitigation policies. Together, these approaches highlight the interplay between technology, policy, and human behaviour in reducing insider risk.

Foundational studies from 2012 to 2018 laid the groundwork for current models. Bilusich et al. (2018) introduced a layered "security-in-depth" approach, while Gamachchi & Boztas (2018) and Max-Alexander (2018) applied hybrid frameworks integrating analytics, anomaly detection, and behavioural insights. Earlier frameworks by Haran (2016), Gelles (2016), Nurse et al. (2014), and Montelibano et al. (2012) emphasised governance, ethical considerations, organisational culture, and holistic architecture across multiple enterprise layers. Collectively, the literature reveals a shared consensus that insider threat mitigation demands a layered, adaptive, and organisation-wide strategy that blends technical defences with behavioural monitoring, continuous training, and a strong security-aware culture.

6. THE FRAMEWORK

From the foregoing, implementing controls to mitigate insider threats while focusing on individual factors or scope (e.g., technical monitoring) is insufficient to avert a wide range of insider incidents (Alsowail & Al-Shehari, 2021). Thus, an All-Inclusive Threat & Organisational Mitigation (ATOM) framework was proposed to help organisations manage insider threat holistically. Additionally, the proposed framework considered issues that must be determined when planning, establishing, implementing and maintaining an insider threat program. The framework is akin to Bilusich et al. (2018), which supported customisation of security for organisations based on their unique requirements. Since insider attacks are committed by trusted individuals who exploit their authorised permissions to organisational assets, the framework accounts for the level of trust organisations

place in employees relative to specific permissions on assets to determine suitable controls to mitigate insider threats. Industry frameworks and best practices were reviewed to identify processes, capabilities, and controls that could be leveraged to build a comprehensive framework for managing insider threat risks (Kara, 2021). Figure 2 shows the components of the proposed ATOM framework.

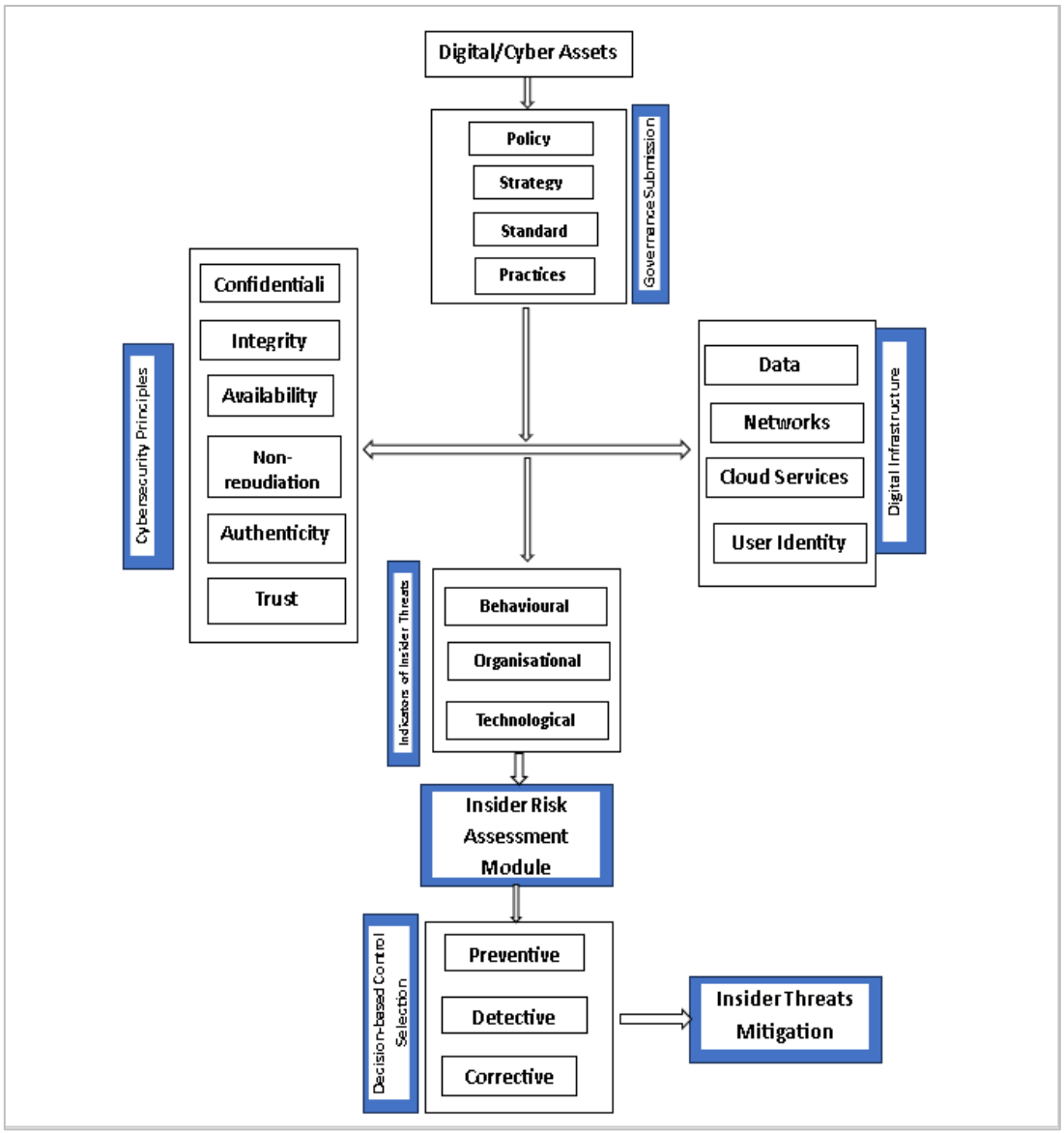

Figure 2: High-Level Structure of the ATOM Framework for Insider Threat Detection and Management (Source: Authors**)**

The framework consists of six components to detect, prevent or mitigate attacks on digital assets. The components of the framework are: governance and oversight; cybersecurity principles or goals; digital infrastructure; vulnerabilities and indicators of insider threats; insider risk assessment; and decision-based selection and mitigation of insider threat controls. Each component is explained in the following sections:

6.1 Governance and Oversight

The first step to establishing a lasting, sustainable insider threat program is to establish a governance and oversight structure (Kara, 2021). The organisation should develop a comprehensive insider threat management framework by establishing and updating policies that define acceptable behaviour, establishing monitoring and reporting practices and ensuring compliance. It should adopt a formal strategy or standardised approach to manage insider threats effectively, clearly define roles and responsibilities for all stakeholders, including executive management, the steering committee, security professionals, and users. Organisations are also expected to set performance expectations. Additionally, an insider threat incident response plan should be developed to cover all stages from detection and evaluation to containment, eradication, escalation, and response, while considering potential legal and human resource implications.

6.2 The Goals of Cybersecurity

For cybersecurity measures to be relevant, it must to achieve six goals. These goals are confidentiality, integrity, availability, authenticity, non-repudiation and trust.

Confidentiality ensures that private or sensitive data is not disclosed to unauthorised individuals or systems, safeguarding privacy and preventing misuse (Aslan et al., 2023). Privacy, as a related concept, gives individuals control over what personal information is collected, stored, transmitted or shared. Integrity, on the other hand, focuses on maintaining the accuracy, completeness, and consistency of data throughout its lifecycle, ensuring that only authorised users can modify information or systems. It guarantees that both data and systems remain authentic, reliable and perform their intended functions without unauthorised interference.

Availability ensures that systems and information are accessible to authorised users whenever needed, which requires eliminating single points of failure and detecting issues promptly. Complementing these are authenticity and non-repudiation. Authenticity verifies that data or communication is genuine, while non-repudiation ensures that parties cannot deny their actions, thereby supporting accountability and auditability.

Trust, on the other hand, underpins all these principles by representing confidence in the reliability, integrity, and authenticity of systems and entities. In digital environments, trust ensures users can rely on systems to operate securely and ethically. However, insider threats breach this trust by exploiting authorised access to compromise confidentiality, integrity, or availability, highlighting the need for strong governance and secure practices to maintain digital trust.

6.3 Digital Infrastructure

Digital infrastructure refers to the physical and software-based devices needed to process and share digital products and services from one point to another. As society and industries have become increasingly intelligent and interconnected (Schmitt, 2023), the need to focus on the protection of modern technologies such as cyber-physical systems, communication networks, mobile devices, the internet of things (IoT), cloud services, and user identity, among others, will continue to rise. The ever-increasing dependence on digital infrastructure and emerging technologies will continue to shape the world we live in, transforming companies, countries, and entire societies. The continued digitisation of the world economy comes with increased security risks due to an expanding attack surface (Schmitt, 2023). Nevertheless, how do we secure digital infrastructure from malicious insiders? The answer is not straightforward, nor does a one-size-fits-all solution exist. Nevertheless, organisations must take steps to achieve resilience by implementing measures to protect cyber assets from malicious insiders.

6.4 Organisational Vulnerabilities and Indicators of Insider Threats

The fourth component of the framework involves understanding the organisational vulnerabilities and indicators of insider threats. Insider threat actors, such as espionage, sabotage, theft, and terrorism, can cause significant damage to organisations (Bedford, 2018). Reducing organisational vulnerabilities and tracking indicators of insider threats to enable proactive countermeasures can significantly improve the management of insider threats. Knowledge of technical, organisational or behavioural indicators is fundamental to identifying insider threats. Technical indicators, such as unusual access patterns or data transfers (Maasberg, 2015), and organisational indicators such as inadequate hiring practices or job instability (Greitzer, 2019), combined with behavioural indicators, like workplace deviance (Bedford, 2018) can create a comprehensive profile of potential risks. One of the most significant security challenges in the cyber world is insider threat since attackers from within the organisation have more privilege and legitimate access to the assets compared to attackers from outside (Al-Mhiqani et al., 2018).

6.5 Insider Risk Assessment

The fifth component of the framework involves risk assessment based on detected indicator of insider threat. Organisations can identify their assets and develop strategies to protect them from malicious insiders through the conduct of risk assessments. The concept of risk varies in interpretation and significance to organisations (Akinrolabu et al., 2019). Therefore, the risk management and risk assessment approach vary for each organisation and will to a large extent be based on their predisposition, in-house expertise, and risk appetite. There are a number of popular risk assessment and management frameworks such as ISO/IEC 27005, ISO/IEC 31000 and NIST 800-30, with broad applicability. These frameworks come with high level guidelines that need to be tailored to specific need of each organisation (Akinrolabu et al., 2019). Applying a risk assessment will enable an organisation to know the types of data it stores, processes and transmits. It allows organisations to know who uses the data and where it is stored.

6.6 Decision-based Insider Threat Control Selection

The last and the sixth component involves selection of risk-based controls to mitigate the threat of insider threat. These controls can be preventive, detective or corrective as the case may be (Kara, 2021). Bilusich et al. (2018) proposed and applied a risk-based framework to assist security professional to determine the relative security effectiveness of different controls. The framework allows decision makers to prioritise security investment and to provide an accountable method to balance investment in controls based on the indicator (e.g. behavioural, organisational or technical) and vulnerability or the insider activity they are dealing with. Kara (2021)

supported a risk-based approach with a focus on key risk indicators (KRIs) or specific organisational vulnerabilities when establishing an insider threat program.

Table 1: A Summary of the components of the ATOM framework

Framework Component	Purpose and Applicability
Governance and Oversight for Insider Threat	Purpose: Establish leadership responsibility, policies, and accountability structures Application to Insider Threats a) Define roles and responsibilities for insider threat management. b) Create insider threat programs (ITPs) with cross-functional teams (HR, Legal, Security, IT). c) Implement policies related to acceptable use, data access, and whistleblower protection. d) Ensure regular audits and board-level reporting on insider risk incidents.
Digital Asset Identification	Purpose: Identify and classify digital assets that could be targeted. Example include data, network, cloud services, user identity, etc.) Application to Insider Threats: a) Identify crown jewels (e.g., intellectual property, customer data, source code). b) Tag and classify sensitive assets based on confidentiality, integrity, and availability. c) Map asset access permissions and usage patterns.
Cybersecurity Goals	Purpose: Align security initiatives with organisational goals. Application to Insider Threats: d) Define confidentiality, integrity, availability, authenticity, non-repudiation and trust goals specifically for insider scenarios. e) Ensure goals reflect both business operations and threat landscape. f) Understand the business impact if an insider misuses legitimate access.
Indicators of Insider Threat	Purpose: Identify early warning signs or risk factors of insider behaviour Application to Insider Threats: a) Monitor digital footprints or anomalies in systems or networks that suggest an insider with authorised access may be misusing or preparing to misuse their access. b) Search for human actions, attitudes, or emotional responses that may signal someone is at risk of misusing their authorised access c) Look for vulnerabilities within the system that may increase the risk of insider threat activity
Insider Risk Assessment	Purpose: Evaluate the likelihood and impact of insider threats. Application to Insider Threats: a) Conduct threat modelling for insider scenarios. b) Use an appropriate framework e.g. NIST, ISO 27005, ISO 31000 standard. (e.g., risk matrices, scoring). c) Consider business context: what would be the cost of a leak, fraud, or system downtime?
Decision-Based Insider Threat Control Selection	Purpose: Choose and implement controls based on risk insights. This can be preventive, detective and corrective controls. Application to Insider Threats: a) Select layered controls: technical (e.g., DLP, access controls), administrative (e.g., policies), and physical (e.g., access restrictions). b) Tailor controls to threat types and user roles. c) Include deterrence (e.g., warnings, training), detection (e.g., logging, alerts), and response (e.g., automated lockouts).

7. APPLYING THE FRAMEWORK ON INSIDER THREAT INCIDENTS

To validate the use of the framework in detecting and preventing insider threat breaches. The six modules of the framework were applied to the four insider threat incidents: data theft, fraud, sabotage, and espionage. Figure 3 demonstrates how each of the six components can be applied horizontally to address the four breaches. On the other hand,

it also shows how each of data theft, fraud, sabotage, and espionage can be mitigated across the six modules in a downward trajectory. Figure 3 shows the components of the framework and how associated modules can be applied to detect and mitigate insider threats.

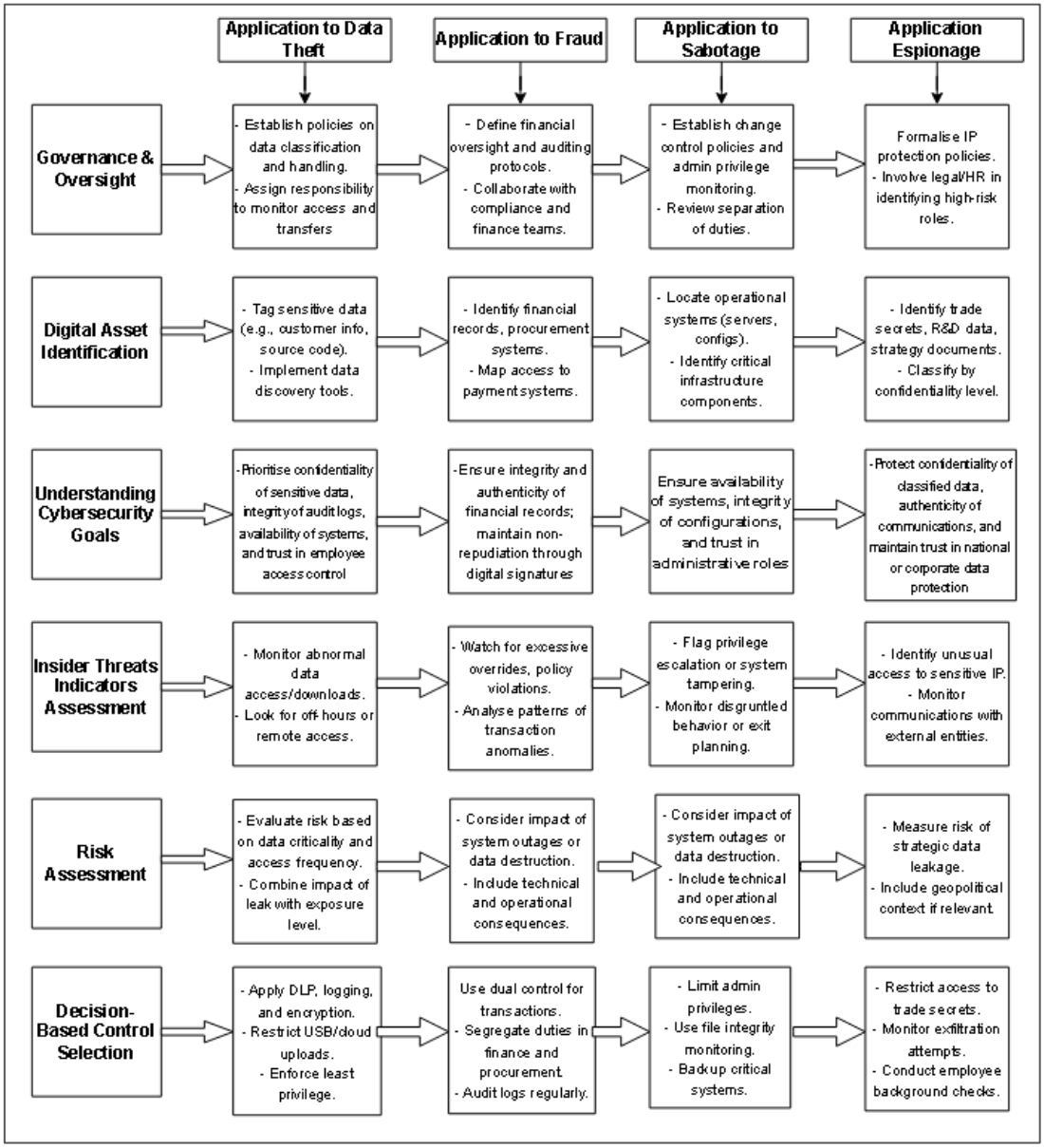

Figure 3: Application of the Framework to Insider Threat Cases

In the previous sections, we illustrated the components of the framework and their applicability in real-life situations. Table 2 summarises the components of the framework and identified relevant digital assets, cybersecurity goals, indicators of insider threats, level of risk and the corresponding controls that can be applied to mitigate associated risks.

Table 2: A summary of applying the framework on insider threat breaches

Insider Threat Type	Key Assets	Cybersecurity Goals	Indicators	Risk	Control
Data Theft	Customer records, Employee data, IP, source code	Confidentiality, Integrity & Trust	Unusual file download, large downloads, off-hours access	High	DLP, logging, PAM, MFA

Fraud	Financial data, accounting systems	Integrity, Authenticity, & Non-repudiation	Override logs, unusual transactions, policy violation.	Medium to High	Automated alerts, Segregation of duties, transaction limits, audit trail, and log review.
Sabotage	Operational systems, config files	Availability, Integrity, Trust	Excessive privilege use, Disgruntled behaviour, system tampering	High	Admin control monitoring, backups, activity monitoring, and change controls
Espionage	Trade secrets, R&D files	Confidentiality & Authenticity, Trust	Multiple access attempts, external communication, criminal association, job hunting while employed	Very High (Critical)	NDA enforcement, data exfiltration monitoring, network segregation.

8. CONCLUSION

One of the most significant challenges facing public and private organisations today is data leaks or breaches caused by insider attacks. Since insiders have privileged access to the organisation's information resources, preventing insider threats requires a deliberate, multifaceted approach. First, a thorough assessment of the characteristics of insiders, whether intentional or unintentional, was considered to help cybersecurity professionals develop effective detection and prevention strategies. Second, the research examined the relationship between trust and insider threats, illustrating how perceptions of trust influence employee behaviour and can either deter or enable insider threat actions. The damaging consequences of insider threats, which often lead to various adverse outcomes, were highlighted. Therefore, there is an increasing need for an integrated, comprehensive framework for insider threat detection and mitigation. Previous research addressed some individual factors, but a broader, integrated, and multi-layered approach has been overlooked. To address this, the proposed framework consolidates all relevant factors into a single, unified model. It adopts a multi-tiered approach that links governance and oversight, digital asset identification, cybersecurity objectives, vulnerability and threat indicator evaluation, insider risk assessment, and risk-based control selection. The framework has been demonstrated through applications that illustrate how it can mitigate the four major types of insider threats: data theft, fraud, sabotage, and espionage. Case studies with real-life insider threat incidents confirm the framework's suitability. Future research should explore AI-enabled deception techniques capable of generating false data to mislead and monitor potential insider activities, while carefully managing ethical concerns.

REFERENCES

1. Akinrolabu, O., Nurse, J. R., Martin, A., & New, S. (2019). Cyber risk assessment in cloud provider environments: Current models and future needs. Computers and Security, 87, 101600.
2. Alsowail, R. A., & Al-Shehari, T. (2022). Techniques and countermeasures for preventing insider threats. PeerJ Computer Science, DOI 10.7717/peerj-cs.938Alsowail RA & Al-Shehari T. (2021). A multi-tiered framework for insider threat prevention. Electronics. 10(9):1005, pp 1-30, DOI 10.3390/electronics10091005.
3. Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity, 4(1), Vol. 4, Issue 1, pp. 1 - 4.
4. Al-Mhiqani, M. N., Ahmad, R., Zainal Abidin, Z., Yassin, W., Hassan, A., Abdulkareem, K. H., & Yunos, Z. (2020). A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations. Applied Sciences, 10(15), 5208, 1-41.
5. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333. Pp 1-42. https://doi.org/10.3390/electronics12061333
6. Bedford, J. (2018). Organisational vulnerability to intentional insider threat. (Doctoral dissertation, University of Southern Queensland). https://www.researchgate.net/publication/304345269 Accessed 24 July, 2024.
7. Boakye-Gyan, K. (2021). An Approach to a Comprehensive Framework for Insider Threat (Doctoral dissertation, Capitol Technology University).
8. Bilusich, D. A. N. I. E. L., Chim, L. E. U. N. G., Nunes-Vaz, R. A., & Lord, S. (2018). There is no single solution to the 'insider'problem but there is a valuable way forward. WIT Transactions on Engineering Sciences, 121, 135-146.
9. Chauhan, K. (2024). Insider Threats Mitigation: Role of Penetration Testing. arXiv

preprintarXiv:2407.17346. https://www.researchgate.net/publication/382527078

10. Clea Ostendorf (2023), 11 Real-Life Insider Threat Examples, https://www.code42.com/blog/insider-threat-examples-in-real-life/ assessed on May 20, 2024
11. Clifton, A. (2024). Strategies for Insider Threat Mitigation and Detection (Doctoral dissertation, Walden University).
12. Gamachchi, A., Sun, L., & Boztas, S. (2018). A graph-based framework for malicious insider threat detection. https://arxiv.org/abs/1809.00141
13. Gelles, MG (2016). Insider Threat: Prevention, Detection, Mitigation, and Deterrence, Butterworth-Heinemann, https://www.researchgate.net/publication/268687978 Accessed August 15, 2024.
14. Global cybersecurity outlook (2022) insight report https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.
15. Greitzer, F. L. (2019). Insider threats: It's the HUMAN, stupid! NCS '19: Proceedings of the Northwest Cybersecurity Symposium, 1–8. doi:10.1145/3332448.3332458
16. Haran, M. H. (2016). Framework Based Approach for the Mitigation of Insider Threats in E-governance IT Infrastructure. International Journal of Scientific Research, 3(4), 5-10.
17. Hoffmann, R., Napiórkowski, J., Protasowicki, T., & Stanik, J. (2020). Risk based approach in scope of cybersecurity threats and requirements. Procedia Manufacturing, 44, 655-662.
18. Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight into insiders and it: A survey of insider threat taxonomies, analysis, modelling, and countermeasures. ACM Computing Surveys (CSUR), 52(2), 1-40.
19. Inayat, U., Farzan, M., Mahmood, S., Zia, M. F., Hussain, S., & Pallonetto, F. (2024). Insider threat mitigation: Systematic literature review. Ain Shams Engineering Journal, 103068. Accessed on May 15, 2025.
20. ISACA Whitepaper (2021). A Holistic Approach to Mitigating Harm from Insider Threats. https://www.isaca.org/resources/white-papers/a-holistic-approach-to-mitigating-harm-from-insider-threats on July 25, 2025.
21. Kara Nagel, (2021). Establishing a Foundation and Building an Insider Threat Program.
22. Kim, A., Oh, J., Ryu, J., & Lee, K. (2020). A review of insider threat detection approaches with IoT perspective. IEEE Access, 8, 78847-78867.
23. Liu, L.; De Vel, O.; Han, Q.-L.; Zhang, J. & Xiang, Y. (2018). Detecting and Preventing Cyber Insider Threats: A Survey. IEEE Commun. Surv. Tutor. 1397–1417.
24. Liu, J. (2020). "The Impact of Cloud Computing on Insider Threats: A Comprehensive Review." Future Generation Computer Systems, 108, 146-155.
25. Maasberg, M., Warren, J., & Beebe, N. L. (2015). The dark side of the insider: detecting the insider threat through examination of dark triad personality traits. In 2015 48th Max Alexander, C. I. S. M., & CRISC, C. (2018). Protect, Detect and Correct Methodology to Mitigate Incidents: Insider Threats. https://www.isaca.org/resources/isaca-journal/issues/2018/volume- 3/protect-detect-and-correct-methodology-to-mitigate-incidents-insider-threats. Accessed June 28, 2025.
26. Modini, J., Vanzomeren, M., Fowler, S., Joiner, K., & Lynar, T. (2020). Rising to the Challenge of Insider Threats for Middle Powers. Academic Conferences International Limited. 92 http://dx.doi.org/10.34190/ICCWS.20.131
27. Nurse, J. R. C., Buckley, O., Legg, P., Goldsmith, M., Creese, S., Wright G. & Whitty, M. (2014) Understanding insider threat: A framework for characterizing attacks. Retrieved from https://www.cs.ox.ac.uk/files/6576/writ2014_nurse_et_al.PDF.
28. Pureti, N. (2022). Insider Threats: Identifying and Preventing Internal Security Risks. International Journal of Advanced Engineering Technologies and Innovations, 1(2), pp.98-132.
29. Rafae, A., Aiche, A., & Erritali, M. (2025). Mitigating insider threats: a trust-based security framework for energy grid plants with dynamic authentication and role-based training. Cluster Computing, 28(15), 1000. https://link.springer.com/article/10.1007/s10586-025-05652-y
30. Rakhi, S., Sampada, H. K., Balodi, A., Shobha, P. C., & Kumar, R. (2025). Insider Threat Detection and Prevention: New Approaches and Tools. Emerging Threats and Countermeasures in Cybersecurity, 241-262.
31. Rama K. (2023). The Different Types of Insider Threats and How to Stop Them. https://www.securonix.com/blog/stop-insider-threats/. Viewed 31 August, 2024.
32. Safa, N. S., & Abroshan, H. (2025). The Effect of Organizational Factors on the Mitigation of Information Security Insider Threats. Information, 16(7), 538.
33. Schmitt, M. (2023). Securing the Digital World: Protecting smart infrastructures and digital industries with Artificial Intelligence (AI)-enabled malware and intrusion detection. Journal of Industrial Information Integration, 36, 100520.
34. Singleton, C. (2021). X-force threat intelligence index (Tech. Rep.). Armonk, NY: IBM.

https://www.cybersecurity-insiders.com/portfolio/2023-insider-threat-report-gurucul/

35. Subhani, A., Khan, I. A., & Zubair, A. (2021). Review of insider and insider threat detection in the organizations. Journal of Advanced Research in Social Sciences and Humanities, 6(4), 167-174.
36. Thompson, N. (2020). A unified classification model of insider threats to information security.In 31st Australasian Conference on Information Systems (pp. 1-4). https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1018&context=acis2020
37. Uche M. Mbanaso & Emmanuel Dandaura (2021). Mastering Cybersecurity for Professionals & Practitioners. Center for Cybersecurity Studies, Nasarawa State University, Keffi, 3rd Edition.