

Information Security Metrics and Targets Setting: A Review of literature and Best Practices

Innocent Chibueze Atasi¹

¹(IT Audits, G2GFM Management Solutions Limited, Nigeria)

Abstract:

Background: Performance measurement is indispensable in today's world. Huge amount of time and efforts could be put into planning, policies development and process implementation, however, if we are not able to objectively decipher whether or not we are making progress, as expected, then it will be difficult to ascertain the status of the system. How do we measure progress in information security?

This paper clearly outlines the importance of information security metrics in industry. A number of security metrics, associated key performance indicators and targets have been presented to contribute to performance measurement and improvement activities. What cannot be measured, cannot be improved, hence the need to establish sound security metrics.

Methodology: A survey of 5 companies in Nigeria's banking sector was conducted and data received was analysed to ascertain the extent of adoption of security metrics and to understand what targets were considered. 3 out of the 5 companies were ISO 27001 certified and the other 2 were not.

Results: Results show that ISO 27001 certified organisations possess a robust performance framework and included most of the very important metrics in their programme.

Conclusion: This paper has presented sound security metrics that could be used by organisations, regardless of type, size, location and activities, for better, improved security systems. A good number of organisations can consider setting their targets along the lines proposed in this paper. This will indeed guarantee an exponential increase in performance levels, ensuring that organisations achieve business objectives.

Key Word: Metrics, Information Security, Indicators, Security Performance

Date of Submission: 03-10-2026

Date of Acceptance: 12-10-2026

I. Introduction

All over the world, advancement in technology, increasing cyberattacks, changing customer expectations, regulatory pressures, increasing economic constraints continue to affect the performance of organisations' security systems. In fact, the advent of more sophisticated artificial intelligence systems, internet of things (IoT) and other emerging technologies has not prevented systems for failures or security underperformance. More efforts to digitalize systems does not sufficiently absolve it from exposure to cyber threats.

Organisation's performance can be monitored and managed more effectively regardless of changes in our threat landscape. Organisations with well-defined security metrics stand better chance of performing better or at least meeting security and business objectives. Security metrics show progress or results of efforts associated with the establishment and implementation of system controls. A number of organisations have not duly outlined key security metrics that could inform stakeholders regarding the effectiveness and performance of their systems.

Huge amount of time and efforts could be put into planning, policies development and process implementation. However, if we are not able to objectively decipher whether or not there is progress, as expected, then it will be difficult to ascertain the status of the system. It is worthy of note that many opportunities for improvement are identified from performance management programs and activities, hence the need to have clearly defined security metrics. Other benefits include: enhanced compliance, justification for investments, enhanced resource allocation, reduction of waste, time optimization, informed decision making and sustainability.

Security metrics adoption could also improve commitment and sense of responsibility with regard to the maintenance of the information security management system¹. They are effective tools for measuring security strength and system levels as well as their resilience or readiness to address security issues. Considering our evolving threat landscape, it is imperative that actors have the right security metrics in place to validate their efforts. To improve our ability to understand, control and better defend our systems, we need to define and apply security metrics².

Security metrics should be structured or designed to address important aspects of the organisation's management system, feed into corporate strategy and serve as business enablers.

Gartner² defines security metrics as quantifiable measurements, based on security objectives, ensuring that services are delivered and data processed. How can we understand the state of our systems without defining security metrics?

Security metrics possess certain properties or attributes. According to Ioan³, security metrics should possess properties such as correctness and effectiveness, ability to indicate lead or lag situations or conditions, alignment with security and business objectives, qualitative and quantitative properties. Gori, et al.⁴ also mentioned attributes of security metrics: well-defined, progressive and reproducible. They went on to state that to clearly define or identify security metrics, it is important to establish a framework for classification, as they considered four distinct types: defense metrics, vulnerability metrics, attack metrics and situation metrics.

Emad, et al.⁵ also outlined thirteen properties of a good security metric, ahead of the five properties mentioned by Ioan³ and three properties mentioned by Gori, et al.⁴ The thirteen properties are: objective, quantifiable, cost effective, repeatable, reproducible, verifiable, meaningful, auto collected, consistent, easy to understand, efficient, feasible and comparable. They identified all the relevant properties from selected sources, all cited in their work and then compared them to each element of the SMART (Specific, Measurable, Actionable, Relevant, and Timely) criteria⁵.

The usefulness of security metrics cannot be over emphasized. They can be used to ascertain the quality of a system, compare performance with other systems and take actions-based and well-informed decisions geared towards maintenance and continual improvement of the system. Security metrics help organisations find answers to the following questions:

- Are we where we are supposed to be?
- How secure are our systems?
- Where are we not doing enough?
- How do we compare with others?
- How do we make all stakeholders understand if we are making progress or not?

ISO 27001:2022 Standard⁶ is an international standard for information security, published by International Organisation for Standardisation in October 2022, adopted by many organisations worldwide captured management clauses and Annex A – security controls from which security metrics could be derived. Security controls were classified into four categories: 37 organisational, 8 people, 14 physical and 34 technological controls⁶.

Ioan³ mentioned four classes of security metrics: metrics supporting control objectives, performance metrics, metrics defined by Centre for internet security (CIS) and metrics imperatives for information security. Rana and Abbas¹ puts it as strategic security metrics, security management metrics and operational security metrics. A publication by Yussuf, Syed and Mark⁷ outlined eight classes of security metrics: intelligence-driven defence metrics, resilience metrics, red and blue teaming metrics, vulnerability assessment metrics, penetration testing metrics, risk assessment metrics, indicators of attacks (IOAs) metrics and indicators of compromise (IOCs) metrics. Diverse classifications of security metrics mentioned by Rana⁸ are: Center for internet security (CIS) classification, classification based on business imperatives for information security and metrics supporting control objectives.

Emad, Iryna, Vitor and Allan⁵ also outlined categories of security metrics based on SMART principles: system vulnerabilities, defence power, situation, etc. The S.M.A.R.T. and PRAGMATIC methods are more about selecting metrics and which principles should be embraced when a metric is constructed. PRAGMATIC is an acronym for predictive, relevant, actionable, genuine, meaningful, accurate, timely, independent, and cheap⁹.

Serhii, et al.¹⁰ outlined aspects of security metrics that can significantly affect the assessment of critical infrastructure – secrecy level of information resources, regulatory concerns, evaluation of financial and computational costs and extent of provision of security services.

It is also worthy of note that Ansar and Khalifa¹¹ developed a model for information security metrics determination and implementation based on the following domains: information security governance, resource management, data protection, threat management, incident management, network security, system security, application security and monitoring analysis, with a view that they were derived at strategic, tactical and operational levels.

Good security metrics should be seamlessly collected by automated means, consistently measured and better expressed as a percentage or cardinal number. Efficiency, objectivity and consistency should be known values of metrics.

Based on the aforementioned research efforts and personal industry experiences, security metrics will be presented with reference to domains of information security as effective security metrics can be derived from

them. The domains considered in this paper are: technical vulnerabilities management, network security, incident management, Identity and access management, end-point security, Awareness and education, change management and data protection, resource management and risk management^{1,2,3,4,5,6,7,8,9,10}.

1. Technical Vulnerabilities Management metrics

Proposed Metrics and Key Performance Indicators: Frequency of assessments, Number of vulnerabilities identified but not reported, Number of vulnerabilities not appropriately classified, Number of tools used for assessment, Percentage of vulnerabilities not remediated within a defined period, Percentage of patch not tested, Percentage of patch tested but not deployed, Percentage of systems and applications without current patch, Mean time to remediate vulnerabilities, Percentage of vulnerabilities without patch, Retest success rate, Percentage of asset scope or category not captured in the assessment

2. Network security metrics

Proposed Metrics and Key Performance Indicators: Number of outdated policies on the firewall, Number of policies not enforced, Number of rules without formal approval, Mean time to detect an anomaly, Mean time to respond to an anomaly, Mean time to resolve an incident, Percentage of expired network access requests with active status on the system, Frequency of network access reviews, Percentage of successful attacks, Percentage of successful redundancy tests, Percentage of inactive network security agreements, Percentage of unresolved network security incidents, Percentage of unauthorised devices on the network, Network tools lifespan index, Number of parameters or indicators not captured by the network monitoring tool dashboard

3. Incident management metrics

Proposed Metrics and Key Performance Indicators: Number of incidents not reported, Number of incidents not properly classified, Mean time to respond to incidents, Mean time to resolve incidents, Number of incidents not resolved

4. Identity and access management metrics

Proposed Metrics and Key Performance Indicators: Frequency of access rights reviews, Number of dormant accounts, Percentage of rights escalation, Percentage of systems that are not MFA (multi-factor authentication) enabled and enforced, Percentage of exited staff with active accounts, Number of utility accounts that are not linked to a particular individual or group of people, Number of privileged accounts without authorization, Number of accounts that have exceeded approved duration of access.

5. End-point security metrics

Proposed Metrics and Key Performance Indicators: Percentage of devices not enrolled, Percentage of devices that have not completed full scan, Percentage of devices without full disk encryption, Number of devices that violate policies, Mean time to respond to threats, Mean time to resolve threats, Frequency of scan, Number of devices with obsolete application, Percentage of devices with unhealthy status, Mean tolerable device inactive period

6. Awareness and education metrics

Proposed Metrics and Key Performance Indicators: Number of awareness sessions not completed, Percentage of awareness programme not completed, Number of phishing simulations not completed, Phish-prone rate, Number of policy violations, Percentage of policy acknowledgements, Percentage of information security domains not included in the awareness programme.

7. Change Management

Proposed Metrics and Key Performance Indicators: Number of unapproved changes, Number of failed changes, Number of changes not properly classified, Percentage of change requests without roll-back plans, Percentage of changes deployed without post-implementation review, Percentage of emergency changes without required documentation

8. Data protection

Proposed Metrics and Key Performance Indicators: Number of devices not enrolled in the Data Leakage Prevention (DLP) solution, Number of DLP policies not enforced, Percentage of non-compliances from regulatory audits, Percentage of awareness programme not completed, Percentage of unmasked data categories, Frequency of data access reviews, Percentage of applications deployed without data protection impact assessment (DPIA), Number of data breaches, Number of information classification violations, Number of unauthorised devices processing personal data

9. Resource Management

Proposed Metrics and Key Performance Indicators: Number of trainings completed, Percentage of needs not covered by the current budget, Number of devices that has exceeded end of life (EOL), Number of fire drills conducted, Number of personnel available per function, Percentage of obsolete assets not properly disposed, Mean time to respond, Mean time to resolve.

10. Risk Management

Proposed Metrics and Key Performance Indicators: Number of risks unidentified, Percentage of risks identified and not treated, Frequency of risk reviews, Number of risk owners not involved, Percentage of risks above the acceptance level.

II. Methodology

A survey of 5 companies in Nigeria's banking sector was conducted and data received was analysed to ascertain the extent of adoption of security metrics and to understand what targets were considered. 3 out of the 5 companies were ISO 27001 certified and the other 2 were not.

The survey questionnaire captured metrics defined by the author in the domains outlined above – technical vulnerabilities management, network security, incident management, identity and access management, end-point security, awareness and education, change management, data protection, resource management, risk management. Feedback from 5 institutions were analysed.

A survey of 5 companies in Nigeria was conducted to obtain information about security targets based on the security metrics and KPIs outlined above. 3 out of the 5 companies were ISO 27001 certified and the other 2 (companies 4 and 5) were not. See results below:

Table 1: Survey of Security Targets

Domain	Metric/KPI	Targets				
		Company 1	Company 2	Company 3	Company 4	Company 5
Technical Vulnerability Management	Frequency of assessments	Annually	Annually	Monthly	Annually	N/A
	Number of vulnerabilities identified but not reported	Less than 3	Less than 5	0	N/A	N/A
	Number of vulnerabilities not appropriately classified	0	0	0	0	0
	Number of tools used for assessment	5	3	Greater than 5	N/A	1
	Percentage of vulnerabilities not remediated within a defined period	5%	5%	5%	N/A	N/A
	Percentage of patch not tested	0	0	0	10%	10%
	Percentage of patch tested but not deployed	0	0	0	N/A	N/A
	Percentage of systems and applications without current patch	10%	Less than 5%	5%	10%	N/A
	Mean time to remediate vulnerabilities	1 month	2 weeks	1 week	1 month	N/A
	Percentage of vulnerabilities without patch	10%	10%	N/A	N/A	N/A
	Retest success rate	95%	N/A	100%	70%	N/A
	Percentage of asset scope or category not captured in the assessment	10%	N/A	0%	N/A	N/A
Network Security	Number of outdated policies on the firewall	0	0	0	0	0
	Number of policies not enforced	0	0	0	0	0
	Number of rules without formal approval	0	0	0	0	0
	Mean time to detect an anomaly	30 mins	1 hour	30 mins	15 mins	30 mins
	Mean time to respond to an anomaly	1 hour	1 hour	1 hour	1 hour	1 hour
	Mean time to resolve an incident	6 hours	1 – 3 hours	3 hours	1 hour	1 hour
	Percentage of expired network access requests with active status on the system	0	0	0	0	0
	Frequency of network access reviews	Annually	Quarterly	Monthly	Annually	Annually
	Percentage of successful attacks	0	0	0	0	0
	Percentage of successful redundancy tests	100%	100%	100%	N/A	N/A
	Percentage of inactive network security agreements	0	0	0	0	0
	Percentage of unresolved network	5%	5%	0%	10%	5%

	security incidents					
	Percentage of unauthorised devices on the network	0	0	0	N/A	N/A
	Network tools lifespan index	N/A	0.85	0.9	N/A	N/A
	Number of parameters or indicators not captured by the network monitoring tool dashboard	0	0	0	0	0
Incident Management	Number of incidents not reported	Less than 2	0	0	0	0
	Number of incidents not properly classified	N/A	0	0	N/A	N/A
	Mean time to respond to incidents	1 hour	1 hour	1 hour	1 hour	1 hour
	Mean time to resolve incidents	6 hours	1 – 3 hours	3 hours	1 hour	1 hour
	Number of incidents not resolved	Less than 10	Less than 10	Less than 5	5	7 – 10
Identity and Access Management	Frequency of access rights reviews	Annually	Quarterly	Monthly	N/A	N/A
	Number of dormant accounts	Less than 5	0	0	N/A	Less than 5
	Percentage of rights escalation	5%	5%	5%	N/A	N/A
	Percentage of systems that are not MFA (multi-factor authentication) enabled and enforced	0	10%	0	5%	N/A
	Percentage of exited staff with active accounts	0	0	0	0	0
	Number of utility accounts that are not linked to a particular individual or group of people	0	0	0	0	0
	Number of privileged accounts without authorization	0	0	0	0	0
	Number of accounts that have exceeded approved duration of access	5%	5-10%	0	0	N/A
End-Point Security	Percentage of devices not enrolled	0	0	0	0	0
	Percentage of devices that have not completed full scan	0	0	0	0	0
	Percentage of devices without full disk encryption	0	0	0	0	0
	Number of devices that violate policies	10%	5%	1%	N/A	10%
	Mean time to respond to threats	1 hour	1 hour	1 hour	1 hour	1 hour
	Mean time to resolve threats	6 hours	1 – 3 hours	3 hours	1 hour	1 hour
	Frequency of scan	Daily	Daily	Daily	Daily	Daily
	Number of devices with obsolete application	0	0	0	0	0
	Percentage of devices with unhealthy status	0	0	0	0	0
	Mean tolerable device inactive period	30 days	7 days	15 days	30 days	30 days
Awareness and Education	Number of awareness sessions not completed	0	0	0	0	0
	Percentage of awareness programme not completed	0	0	0	0	0
	Number of phishing simulations not completed	0	0	0	0	0
	Phish-prone rate	10%	N/A	5%	10%	N/A
	Number of policy violations	0	0	0	0	0
	Percentage of policy acknowledgements	100%	100%	100%	100%	100%
	Percentage of information security domains not included in the awareness programme	50%	70%	25%	N/A	N/A
Change Management	Number of unapproved changes	0	0	0	0	0
	Number of failed changes	10	7	3	5	7
	Number of changes not properly classified	1	0	0	0	0
	Percentage of change requests without roll-back plans	0	0	0	0	0
	Percentage of changes deployed without post-implementation review	5%	10%	0%	10%	10%
	Percentage of emergency changes without required documentation	0	0	0	0	0
Data Protection	Number of devices not enrolled in the Data Leakage Prevention (DLP) solution	0	0	0	0	0
	Number of DLP policies not enforced	0	0	0	0	0
	Percentage of non-compliances from regulatory audits	5%	5%	0%	0%	0%

	Percentage of awareness programme not completed	0	0	0	0	0
	Percentage of unmasked data categories	40%	50%	15%	30%	50%
	Frequency of data access reviews	Annually	Quarterly	Monthly	Annually	Annually
	Percentage of applications deployed without data protection impact assessment (DPIA)	0	5%	0	0	10%
	Number of data breaches	0	0	0	0	0
	Number of information classification violations	0	0	0	0	0
	Number of unauthorised devices processing personal data	0	0	0	0	0
Resource Management	Percentage of trainings completed	100%	90%	90%	85%	100%
	Percentage of needs not covered by the current budget	20%	0%	20%	N/A	N/A
	Number of devices that has exceeded end of life (EOL)	N/A	10%	5%	N/A	20%
	Number of fire drills conducted per year	1	2	2	1	0
	Number of personnel available per function	5	More than 5	Not less than 10	20	10
	Percentage of obsolete assets not properly disposed	0	0	0	0	0
	Mean time to respond	1 hour	1 hour	1 hour	1 hour	1 hour
	Mean time to resolve	6 hours	1 – 3 hours	3 hours	1 hour	1 hour
Risk Management	Number of risks unidentified	0	0	0	0	0
	Percentage of risks identified and not treated	10%	10%	5%	5%	N/A
	Frequency of risk reviews	Annually	Quarterly	Monthly	Annually	Annually
	Number of risk owners not involved	0	0	0	N/A	N/A
	Percentage of residual risks above the acceptance level	20%	20%	10%	20%	20%

*N/A means not available

III. Results and Discussion of Results

The total Number of KPIs considered was 86 as shown in table 1. The five companies sampled subscribed to a good number of KPIs and indicated that they set targets, also highlighted above.

Figure 1 below showed the number of security targets per company:



Figure 1: Number of security targets per company

From Figure 1, it can be seen that Company 3 subscribed to 85 KPIs and company 5 subscribed to 64 KPIs out of 86 KPIs presented by the research instrument. From the data table shown, it was also observed that Company 3 set the best targets.

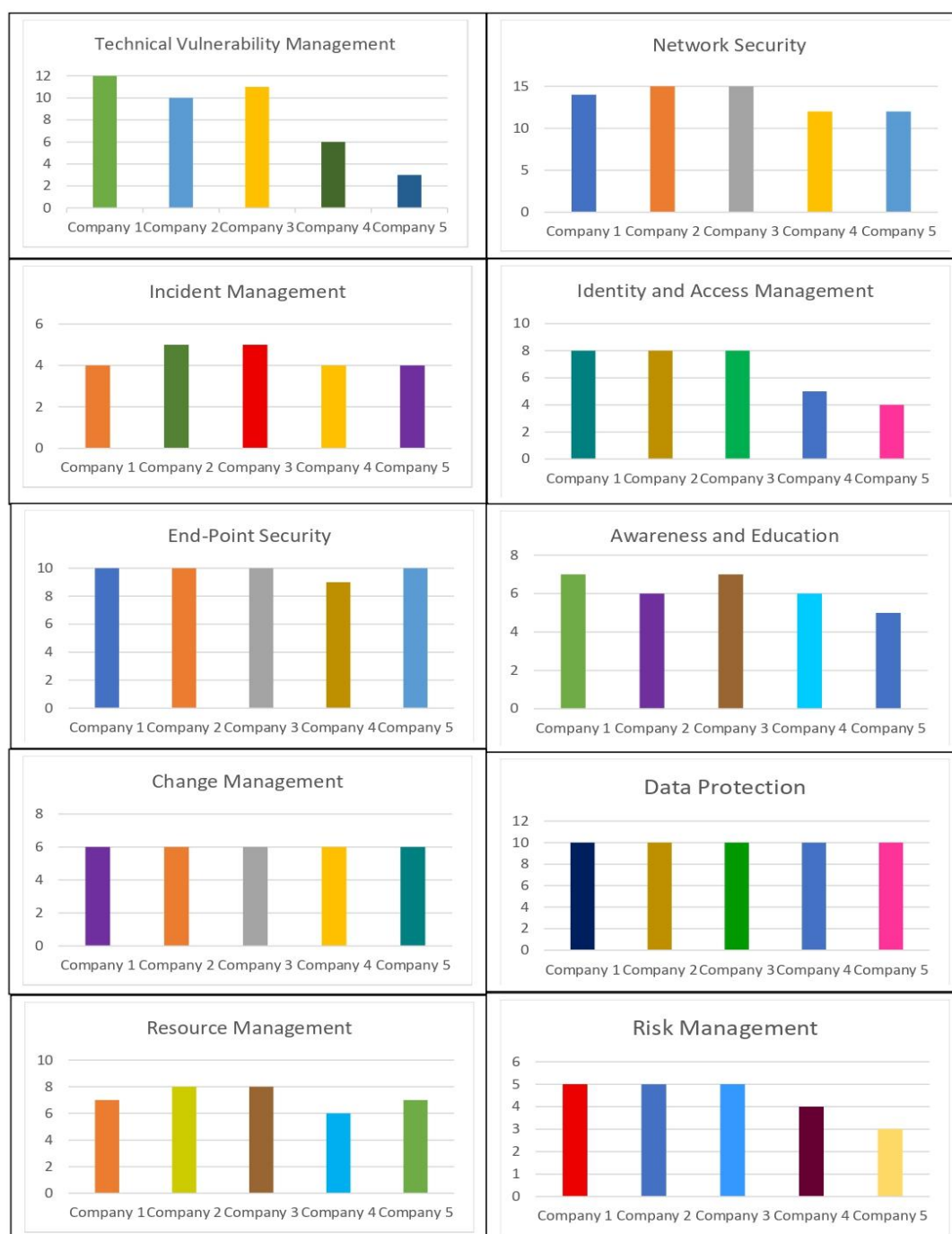


Figure 2: Domain by Domain KPI and company response

From Figure 2 above, Network security has the highest number of KPIs. Change Management domain captured equal number of responses from the 5 companies. Also, change management and data protection domains had KPIs that were fully subscribed by the companies. KPIs associated with incident or threat response and resolutions were fully subscribed by the 5 companies.

IV. Conclusion

This paper has presented sound security metrics that could be used by organisations, regardless of type, size, location and activities, for better, improved security systems. A good number of organisations can consider setting their targets along the lines proposed in this paper. This will indeed guarantee an exponential increase in performance levels, ensuring that organisations achieve business objectives.

References

- [1]. Rana, K., & Abbas, A. (2016). Security metrics and the risks: An overview. *International Journal of Computer Trends and Technology*, 41(2), 106–112.
- [2]. Gartner. (n.d.). Security metrics. <https://www.gartner.com/en/information-technology/glossary/security-metrics>.
- [3]. Ioan, A. (2020). Mobile security metrics. *International Journal of Innovative Science and Research Technology*, 5(4), 1225–1229.
- [4]. Gori, G., Rinieri, L., Melis, A., Al Sadi, A., Callegati, F., & Prandini, M. (2024). A systematic analysis of security metrics for industrial cyber-physical systems. *Electronics*, 13(7), Article 1208.
- [5]. Sherif, E., Yevseyeva, I., Fernandes, V. B., & Cook, A. (2024). The smart approach to selecting good cyber security metrics. *Journal of Internet Services and Information Security*, 14(4), 312–330.
- [6]. International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ISO/IEC Standard No. 27001:2022).
- [7]. Ahmed, Y., Naqvi, S., & Josephs, M. B. (2019). Cybersecurity metrics for enhanced protection of healthcare IT systems. In 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT) (pp. 1–9). IEEE. <https://doi.org/10.1109/ISMICT.2019.8744003>.
- [8]. Ahmed, R. K. A. (2016). Overview of security metrics. *Software Engineering*, 4(4), 59–64. <https://doi.org/10.11648/j.se.20160404.11>
- [9]. Joonas, F & Tapio, F (2023). Technical performance metrics of a security operations center. *Computers & Security*, 135(103529), 1–14.
- [10]. Yevseiev, S., Milov, O., Opirskyy, I., Dunaievska, O., Huk, O., Pogorelov, V., Bondarenko, K., Zviertseva, N., Melenti, Y., & Tomashevsky, B. (2022). Development of a concept for cybersecurity metrics classification. *Eastern-European Journal of Enterprise Technologies*, 4(4), 6–18. doi.org
- [11]. Daghour, A., & Mansouri, M. (2024). Hierarchical models of information systems security metrics. *Engineering, Technology & Applied Science Research*, 14(6), 17761–17768. doi.org.

About the author

Innocent Chibueze Atasie is an IT Audit and Assurance Leader who has provided services across countries in Africa, Middle East, USA and Australia. He holds C|CISO, CISA, CRISC, CDPSE, CISM, CDPO certifications, 15 ISO certifications, a fellow of over 4 reputable institutions. He is the Chief Executive of G2GFM Management Solutions Limited. He holds BEng and MSc Degrees from University of Nigeria and University of Lagos. Research interests are in the areas of Information Security, IT, privacy and cloud security. He is the winner of Rron Islami Award for the MSECB Auditor of the Year 2025 for Africa.