The Strategic Importance of Information Assurance in Combating Modern Cyber Threats

Rusalyn A. Ubay[1]; Akdam T. Omaron[1]; Al-Hadzrim M. Gajir[1]; Alzyver S. Kadil[1]; Nadzmar R. Arakama[1];
Rosemilyn H. Humam[1]; Garfaiza S. Jamasali[1]; Nelhata H. Talib[1]; Abdurasul M. Insam[1]; Alnizar J. Hussin[1];
Shernahar K. Tahil[2]; Nureeza J. Latorre[3]
[1]Department of Information Technology, Student, College of Computer Studies, Mindanao State University-Sulu, Philippines
[2]Department of Computer Science, Faculty, College of Computer Studies, Mindanao State University-Sulu, Philippines
[3]Dean, College of Computer Studies, Mindanao State University-Sulu, Philippines

Abstract:- In recent years, there has been no end to the types of modern cyber security threats. Information assurance (IA) is a strategic mandate for organizations increasingly reliant on digital technologies. Such needs are confidentiality, integrity, availability, authenticity, and nonrepudiation (NTR), which are also discussed in this study. While the NIST Cybersecurity Framework, ISO 27001, and COBIT have been examined elsewhere by academia, this research seeks to understand theories and look at these established frameworks under actual practice. It investigates IA's basic technologies and apparatus, such as firewalls, intrusion detection/prevention systems, encryption, and vulnerability scanners. Realizing human factors' serious role in security breaches, this paper stresses the importance of security awareness training, dealing with social engineering attacks, and encouraging a security-conscious corporate culture. It also considers the challenges and opportunities IA faces when applied to digital transformation technologies like cloud computing, mobile devices, and the Internet of Things (IoT), pointing out ways of securing these technologies. Finally, monitoring and assessing IA programs are essential through key performance indicators (KPIs), risk assessment methodologies, and security audits to ensure that adjustments are kept in line with deployed threats and business targets. By taking an all-round and forward-looking approach to IA, any organization can fully use its information assets, maintain normal business operations, and press on untroubled by the ever-evolving range of cyber threats.

Keywords:- *Information Assurance, Cyber Threats, Cybersecurity Frameworks, Digital Transformation.*

I. INTRODUCTION

In today's hyper-connected world, information security has been placed at the forefront because data drives innovation and is also a prime mover of economic growth. Across all industries, from multinational corporations and government agencies to non-profits of faiths or charity levels, organizations increasingly rely on digital technologies for their operations, communications, and service provision [1]. Yet as that reliance grows, vulnerability does too, causing higher risks for damage from cyber threats, which can compromise entire sectors' most valuable assets and disrupt operations. It is no longer enough to hope no one breaks into your system; now, four levels of vigilance are needed to defend against external attacks [2]. The need for strong information assurance (IA) has become a strategic necessity rather than merely an IT issue alone. This is further highlighted by the increasing sophistication and frequency of cyberattacks, which are no longer restricted to the random depredations of individuals but may well involve international criminal syndicates or even nation-state actors deploying substantial resources and expertise to achieve their ends [3]. Information assurance is a comprehensive approach to the protection of information assets, specifically those assets' confidentiality, integrity, availability (CIA), authenticity, and nonrepudiation. It involves a full spectrum of security measures, from technical safeguards such as firewalls and intrusion detection systems to administrative controls like policies, procedures, and training programs [4]. IA is not just about keeping unauthorized persons out of your data; it's also concerned with managing risk, ensuring compliance with regulations, and promoting a culture of security consciousness throughout the entire organization. In an age where cyberattacks are sophisticated and commonplace, information assurance provides a comprehensive framework for addressing the various dangers that organizations face. This encompasses more than just responses to threats that have already occurred, such as incident recovery and response plans: it also entails dealing with them before they materialize in other ways- through measures like threat intelligence gathering, vulnerability assessments on systems, and security awareness education for all members of staff alike.

The reason for helping them with that is data. A breached file can inflict huge financial damages, shame your reputation, and impose legal liabilities. For instance, when customer data is lost, an organization may be hit with heavy regulatory fines, severe lawsuits, and lowered consumer trust. In addition, well-orchestrated intellectual property theft can throttle innovation and ruin competitive advantage. Organizations can reduce this risk using robust IA measures and ensure the continuity of their business systems. It is a key contributor to maintaining operational efficiency [5]. Denial-of-service attacks, for example, can take the life of an Online Service and shut down essential infrastructure, resulting in heavy financial losses operationally. Besides its role in maintaining a low rate for prolonged periods, a well-constructed set of IA safeguards--can guarantee the availability of services and systems for uninterrupted functioning. This is particularly crucial in healthcare, finance, and energy; few breaks will not result in extensive loss [6].

In addition to its protective function, IA is an important digitization driver. Traditionally, security has been about protecting users or keeping things private. However, with the rise of cloud computing and ever more mobile devices, it is increasingly the data owner that bears the risk. Moreover, customers want more access to their information online than ever before. IA lays the groundwork for secure innovation, giving businesses an opportunity to use these technologies while mitigating associated risks [7]. By incorporating safety considerations in the design and implementation of new systems and processes, enterprises can confidently carry out the phases of digital transformation. In addition, IA boosts confidence and trust among stakeholders. Consumers, partners, and investors are increasingly concerned about the security of their data. However, by demonstrating a real commitment to IA, groups can build trust with stakeholders and improve relations. IA is no longer just a matter of technology. It's a strategic necessity for the success of organizations in an era when everything is digital [8]. Proactivity, comprehensiveness, and integration with business aims are all called for IA, reflecting the current threat environment at every turn.

II. THE EVOLVING LANDSCAPE OF CYBER THREATS

The lure of making money has attracted large numbers of cyber gangs into this lawless and fast-changing business environment. It has also provided a major threat to both people and organizations. Unorganized lone cyber thug no longer carries out the same type of cybercrime. It has developed into various advanced crime operations conducted by well-organized syndicates, drug lords using electronic commerce, and even political groups rallying behind the Internet's name. The motivation, membership goals, and modus operandi of each category vary. However, in such a dynamic environment, understanding the changing landscape of information assurance is paramount. A big problem today is ransomware when an attacker encrypts the target company's key data and demands that its management pay off a ransom [9]. This has evolved from simple, scattergun attacks into concentrated offensives on valuable organizations. Hospitals, schools, and infrastructure are places no one thought would be taken this way. Another trend is supply chain attacks: Cybercriminals mess with a software or hardware component intended for broader networks. For example, the SolarWinds breach infected many government agencies and corporations.

Moreover, the proliferation of artificial intelligence systems and Internet of Things (IoT) devices adds new vulnerabilities. Artificial intelligence algorithms can be tricked into producing biased or incorrect results, and the inherent security holes in IoT devices make them easy targets for hackers. These networked devices can be used to launch large-scale DDoS attacks or to get private data. The growth of cryptocurrencies has also made cyberspace a more fertile breeding ground for crime by providing attackers with a means of laundering stolen money and evading detection [10]. There are many reasons for conducting such attacks. Organized criminal groups are usually financially motivated, whereas state actors might steal intellectual property, sabotage vital infrastructure, or carry out espionage. Activists, too, can't be lumped together: some are motivated by political or social aims, using cyberattacks to further their cause or uncover wrongdoing. This tangled web of motives and actors underlines the need for a comprehensive, flexible approach to information assurance. By understanding how cyber threats are changing, organizations can prepare well in advance--and take effective measures to mitigate risks when they happen. This will safeguard their valuable assets while ensuring that business continues as usual.

III. CORE PRINCIPLES AND FRAMEWORKS OF INFORMATION ASSURANCE

Core principles are foundations for building up Information Assurance. These principles lay out the key objectives of IA and how they contribute to overall security. Information is kept confidential to ensure that sensitive information is transmitted only to authorized individuals. These principles are meant to prevent unauthorized disclosure. Data integrity guarantees the correctness and trustworthiness of data. Data is kept intact so that it cannot be altered or otherwise modified without authorization [11]. Data are protected from deletion or being overwritten for the same reasons: selfish purposes like profit-making or inappropriate closed systems. The user is entitled to access information unavailable elsewhere. The provision of this service for a user keeps his operation running smoothly. This is called availability. Authenticity lets you establish the truth of who or what you are dealing with. Authentic information is legitimate information. Finally, nonrepudiation makes it impossible for a party to deny participating in a process. Without nonrepudiation, there would be no accountability.

Organizations typically lean on well-structured frameworks and standards that provide guidance and best practices to make IA implementations effective. The NIST Cybersecurity Framework, produced by the National Institute of Standards and Data Technology, is a comprehensive collection of standards, guidelines, and best practices that lay out the issues associated with managing cybersecurity risks. It offers organizations a flexible, adaptable framework tailored to their needs and risk characteristics (profile) [12]. ISO 27001, an internationally recognized standard for Information Security Management Systems (ISMS), is a methodical means of managing sensitive information. It specifies what an organization has to do to establish, implement, and maintain an ISMS (information security management system) on an ongoing basis. Control Objectives for Information and Related Technologies (COBIT), developed by ISACA, is a framework for IT governance and management that offers comprehensive controls and guidance in managing IT risks and aligning with business objectives. It provides organizations a structured approach to efficiently using IT resources to realize their goals. By implementing these frameworks and standards, organizations can lay a solid foundation for their IA programs, ensuring their security is comprehensive and consistent with the industry's best principles [13]. These frameworks supply a route map for carrying out security controls, managing risks, and ensuring compliance with relevant legislation – all of which finally eventuate in a robust security posture.

IV. KEY TECHNOLOGIES AND TOOLS FOR INFORMATION ASSURANCE

Given that no technology can defend against every threat and safeguard all information assets, information assurance relies on a truly diverse arsenal of technologies and tools to be effective [14]. Often, such tools will be our first line of defense throughout the attack window. They both deal with preventing attacks (averting them at or just below the network boundary, respectively) and responding to them (either manually or, increasingly, automatically). Firewalls, for instance, act as the gateway that controls all network traffic and prevents external access to internal systems. They examine incoming and outgoing network connections, blocking those that fail to meet fixed security rules. Intrusion detection and prevention systems (IDPS) take this further by actively monitoring network traffic for anomalous patterns or malicious activity [15]. They can alert security personnel or even take remedial action to block or mitigate threats in real time as they occur.

Encryption is a foundational technology for ensuring the confidentiality and integrity of data. It turns the data into an unreadable format that unauthorized individuals cannot read or use. Encryption can be applied to data at rest, like files on a hard drive and data in motion, such as information transmitted over a network DLP, or data loss prevention solutions that aim to prevent sensitive data from flowing beyond the organization's boundaries [16]. They examine and govern data movements, while also preventing sensitive information--for example, credit card numbers or intellectual property--from being sent or stored without authorization.

Security information and event management (SIEM) technology systems provide a central platform for collecting, analyzing, and correlating security logs and events from various sources across the network [17]. This gives security teams an overall assessment of security status, helps them recognize potential threats, and allows them to respond more effectively when trouble starts. Vulnerability scanners automate the process of identifying weaknesses in systems and applications. They scan for known vulnerabilities, configuration mistakes, and outdated software to provide useful information that can be used to prioritize patching and remediation efforts. These technologies and tools form the practical basis for a robust IA framework.

They enable the implementation of security controls, the monitoring of threats, and protection against unauthorized access. IA represents an unhappy triangle: it could be broken through unauthorized use, disclosure, or destruction. Yet, to provide a safety valve against tomorrow's threats, organizations should look for any emerging tools that can aid in their efforts to maintain a secure posture.

V. HUMAN FACTORS IN INFORMATION ASSURANCE

Although technical measures are essential for its assurance, the human element is often overlooked when it comes to cybersecurity and is usually the key factor to boot. This way, even the most robust defensive measures can be severely compromised due to an individual's accident, negligence, or malice. We needed to understand and deal with this point just as we had to do in trying to make an impervious security strategy. Security awareness training often involves on-site participant interaction [18]. This educates the people in places at risk of conventional attack and forges positive relationships. Successful programs for fostering security awareness go further than simply telling employees about the company's policies. They start out by cultivating a security-minded mindset. Employees need to be trained to distinguish between common techniques employed by social engineering attackers, such as attempts to acquire sensitive information from staff through phishing emails and fraudulent impersonations [19]. This is potentially devastating to the entire enterprise or organization. The ploys employed by cybercriminals in forging significantly reduced credit card transactions and grabbing individuals' login credentials at a near 100% return rate include phishing emails and fake Web sites.

Creating a culture of full security awareness in the organization is vital. This entails developing the attitude that "I am responsible for any threat, and so are my colleagues and subordinates." Communicating constantly with people about security matters, giving them regular performance feedback, and encouraging secure practices through incentives will all help create a highly valued and high-use security environment. Access control, watching what users are doing, and ethical behavior will all make these things less likely. Human factors should be included in the IA arena to tackle the inner problems more harmful than anything external threats can cause. Employees motivated by money or revenge can occasionally throw the entire enterprise out of kilter. As a result of training, cultural change, and proactive programs aimed specifically at human factors, we were able to prevent a great many potential security breaches and thereby increase the overall efficiency of our security strategy. This approach points out once more that technology cannot protect safety by itself. The responsibility for this lies with management and operational personnel in every corner of these systems, who will not let genuine information security be gained at such a price.

VI. INFORMATION ASSURANCE IN THE AGE OF DIGITAL TRANSFORMATION

The spread of cloud computing, mobile terminals, and interconnected devices (so-called indicative Things) has led to a paradigm shift in the way organizations operate today. However, the new transformation has also brought about all kinds of obstructions and complications for information assurance. For instance, cloud computing is scalable and cost-effective but raises questions about the security and privacy of data shared in such environments. Organizations need to consider their security measures from cloud service providers when evaluating these risks [20]. They must also ensure that their data meets all requirements set forth by themselves or other parties- in particular, legally competent third-party organizations authorized to regulate specific fields (such as finance or health care). Mobile devices are portable and connected by nature, which brings a whole new set of security issues. The loss or theft of such a device may result in data breaches. Sensitive information is often sent via public Wi-Fi networks, making it vulnerable to interception and theft. Implementing strong authentication mechanisms, device encryption, and mobile device management solutions is crucial for securing these devices and protecting organizational data [21]. With its myriad of interconnected devices, the attack surface of the Internet of Things (IoT) is constantly expanding. Security features on IoT devices are often weak or absent altogether, providing numerous opportunities for hackers to take advantage. Breached IoT devices can be used to infiltrate other systems and steal proprietary information; even hijacked systems so strongly associated with critical infrastructure are affected by this state. Securing the IoT requires a comprehensive approach: for the devices to be designed securely, good identification must give way to stricter passwords and other access controls on every level; otherwise, regular firmware updates will also have to get into gear.

However, digital transformation also holds the key to improving the information assurance landscape. Cloud computing platforms may provide organizations with advanced security features and capabilities they could not readily acquire. Mobile devices offer access to corporate resources from any location--thus enhancing productivity and flexibility. The IoT yields valuable data for security monitoring and analysis that can aid in the early detection, localization, and termination of any threat [22]. In order to master the intricacies of digital transformation, organizations need to take a proactive and adaptive approach to IA. It entails adopting robust security controls into their cloud environments, mobile devices, and interconnected devices and formulating all-encompassing strategies for safeguarding information that factor in the unique challenges of this dynamic, integrated environment. By incorporating safety into the very fabric of digital transformation activities, organizations will be able to draw forth advantages from such lands of technology while keeping the hazards to a minimum.

VII. MEASURING THE EFFECTIVENESS OF INFORMATION ASSURANCE PROGRAMS

Implementation of information assurance programs does not call for a single step-by-step approach. They do require constant observation and examination to ensure the continuous success of the program. With continuously changing cyber threats, proactivity is essential, and it is constantly measuring its potential ability to mitigate risk while simultaneously adapting to these ever-evolving challenges. Assessing the effectiveness of IA programs incorporates multiple tools and techniques to measure performance, highlight areas for improvement, and make consistent improvements [23]. Key performance indicators of the IA program will, therefore, measure quantifiable metrics to demonstrate whether the program is accomplished. The KPIs could be how successful phishing attacks were prevented, the time taken to detect and respond to the security incidents, and the percentage of completion by employees of security awareness training. By establishing clear KPIs and regularly tracking them, organizations can gain valuable insights into the strengths and weaknesses of their IA program. Risk assessment methodologies are crucial to identify and prioritize the risks. Regular risk assessments help organizations understand their vulnerabilities, assess the likelihood and impact of potential attacks, and allocate resources appropriately to mitigate the most critical risks [24]. Depending on the organization's specific needs and risk appetite, various methodologies, such as quantitative and qualitative risk assessments, can be used.

Security audits offer an independent and objective assessment of an organization's security posture. Internal security audits or those conducted by third-party experts include all-round reviews of security controls, policies, and procedures. Security audits help detect loopholes in security implementation, verify compliance with relevant regulatory bodies, and provide improvement suggestions [25]. By integrating these approaches, tracking KPIs, making risk assessments, and conducting security audits, organizations can establish a holistic view of the efficacy of their IA program. Through continuous monitoring and evaluation, organizations are best equipped to change security measures according to emerging threats, optimize resources, and ensure that an IA program is in synch with changing business needs [26]. Overall, this dynamic process provides a stronger and more agile security posture; organizations will be better armed to manage the dynamic, morphing threat environment.

VIII. CONCLUSION

In conclusion, this exploration of information assurance underscores its critical role as a strategic imperative in the face of ever-evolving cyber threats. The dynamic landscape of these threats, ranging from sophisticated ransomware attacks to the exploitation of AI and IoT devices, demands a comprehensive and adaptive approach to safeguarding information assets. Embracing the core tenets of IA – confidentiality, integrity, availability, authenticity, and nonrepudiation – and relying on widely used frameworks, such as the NIST Cybersecurity Framework and ISO 27001, enables organizations to have a robust basis for the security posture. Effective IA requires a multi-faceted approach, both for technology and human factors. While implementing essential tools such as firewalls, intrusion detection systems, and encryption technologies is important, equal attention must be given to the human side by providing the required security awareness training, bringing up a security-conscious culture, and reducing insider threats. Moreover, the moving part in digital transformation requires proactive approaches to securing one's cloud environments, mobile devices, and IoT networks. COBIT

An IA program's final and crucial aspect is continuous monitoring and evaluation. The use of key performance indicators, risk assessments, and security audits ensures that an organization's IA initiatives are constantly in tune with the ever-changing threats and business objectives. An iterative process of evaluation and adaptation is necessary to maintain a resilient security posture against changing challenges. Information, a very precious asset in today's globalized world, must be protected. The cyber risk mitigation process for organizations would be successful only when they treat IA as a strategic priority and take an overarching, proactive, and adaptive approach.

REFERENCES

[1]. Tahil, S. K., Alibasa, J. T., Tahil, S. R. K., Marsin, J., & Tahil, S. S. K. (2023). Preserving and Nurturing Tausug Language: The Bahasa Sug Mobile Learning Application Tool for Enhancing Mother Tongue Development for Toddlers. *International Journal of Learning, Teaching and Educational Research*, *22*(11), 18-35.

[2]. Abduhari, E.S., Shaik, T.C., Adidul, A.B., Ladja, J.H., Saliddin, E.S., Adin, A.J., Rumbahali, F.A., Sali, A.B., Jemser, J.M., & Tahil, S.K. (2024). Access Control Mechanisms and Their Role in Preventing Unauthorized Data Access: A Comparative Analysis of RBAC, MFA, and Strong Passwords. *Natural Sciences Engineering and Technology Journal*, *5*(1), 418-430. https://doi.org/10.37275/nasetjournal.v5i1.62

[3]. Rios, B. (2015). Cybersecurity Expert: Medical Devices Have ‘A Long Way to Go’. *Biomedical Instrumentation & Technology*, 49(3), 197-200. https://doi.org/10.2345/0899-8205-49.3.197

[4]. Leśkow J. (2024). Introduction to special issue on the Russian-Ukrainian war: Effects on global cybersecurity and digital infrastructure. *Applied Cybersecurity & Internet Governance (ACIG)*, 3(1): 1–4.

[5]. Deng, J., Zhao, L., Yuan, X., Tang, Z., Guo, Q. (2021). Research on the Role-Based Access Control Model and Data Security Method. In: Tian, Y., Ma, T., Khan, M.K. (eds) Big Data and Security. ICBDS 2020. Communications in Computer and Information Science, vol 1415. Springer, Singapore. https://doi.org/10.1007/978-981-16-3150-4_8

[6]. Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva papers on risk and insurance. Issues and practice*, *47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

[7]. Clark-Ginsberg, A., & Slayton, R. (2019). Regulating risks within complex sociotechnical systems: Evidence from critical infrastructure cybersecurity standards. *Science and Public Policy*, *46*(3), 339-346.

[8]. Ray, A., & Cleaveland, R. (2015). Security assurance cases for medical cyber-physical systems. *IEEE Design & Test*, *32*(5), 56-65.

[9]. Seng N. (2024). Cybersecurity regulation—types, principles, and country deep dives in Asia. *Int Cybersecurity Law Rev*, 5(3): 387–411.

[10]. González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures. *Sensors*, *21*(14), 4759.

[11]. Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology*, *21*(1), 2-35.

[12]. Hamill, J. T., Deckro, R. F., & Kloeber, J. M. (2022). Evaluating information assurance strategies. In *Handbook of Scholarly Publications from the Air Force Institute of Technology (AFIT)*, *1*, 3-32.

[13]. AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & security*, *99*, 102030.

[14]. Tahil, S.K. (2024). Integrating Computer Science in Basic Education Curriculum: Enhancing Innovation and Sophistication for Global Competitiveness. *International Journal of Learning, Teaching and Educational Research*. 23(8), 203-221. https://doi.org/10.26803/ijlter.23.8.11

[15]. Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, *71*(8), 939-953.

[16]. Patel, A. U., Williams, C. L., Hart, S. N., Garcia, C. A., Durant, T. J. S., Cornish, T. C., & McClintock, D. S. (2023). Cybersecurity and Information Assurance for the Clinical Laboratory. *The journal of applied laboratory medicine*, *8*(1), 145–161. https://doi.org/10.1093/jalm/jfac119

[17]. Dunn Cavelty, M. (2018). Cybersecurity research meets science and technology studies. *Politics and Governance*, *6*(2), 22-30.

[18]. Chowdhury, N., & Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, *40*, 100361.

[19]. Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & security*, *56*, 1-27.

[20]. Zhao Z, Hsu C, Harn L, Xia Z, Jiang X, Liu L. (2024). Lightweight ring-neighbor-based user authentication and group-key agreement for internet of drones. *Cybersecurity*, 7(1).

[21]. Awang H, Mansor NS, Zolkipli MF, Malami STS, Mohd Zaini K, Yau TD. (2024). Cybersecurity awareness among special needs students: The role of parental control. *Mesopotamian Journal of CyberSecurity (MJCS)*, 4(2), 63–73.

[22]. Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future generation computer systems*, *92*, 178-188.

[23]. Caramancion, K. M., Li, Y., Dubois, E., & Jung, E. S. (2022). The missing case of disinformation from the cybersecurity risk continuum: A comparative assessment of disinformation with other cyber threats. *Data*, *7*(4), 49.

[24]. Shukla A., Katt, B., Nweke, L.O., Yeng, P.K., & Weldehawaryat, G.K. (2022). System security assurance: A systematic literature review. *Computer Science Review*, Vol 45,100496, https://doi.org/10.1016/j.cosrev.2022.100496

[25]. Heaton, J., & Parlikad, A. K. (2019). A conceptual framework for the alignment of infrastructure assets to citizen requirements within a Smart Cities framework. *Cities*, *90*, 32-41.

[26]. A. Y. Al Hammadi, C. YeobYeun and E. Damiani (2020). Novel EEG Risk Framework to Identify Insider Threats in National Critical Infrastructure Using Deep Learning Techniques. *2020 IEEE International Conference on Services Computing (SCC)*, 69-471, https://doi.org/10.1109/SCC49832.2020.00071