**Blog Post**

The five terms selected from the “ISO/IEC Standard 27000 Section 3 Terms and Definitions” are the following ones (ISO, 2018): 1) **audit**; 2) **competence**; 3) **confidentiality**; 4) **continual** **improvement**; 5) **information system**.

**Auditing** is essential to ensure that all processes, data, methods, and results are documented systematically and comprehensively for the information system to be fully controlled, secured, and, thus, reproducible in its lifecycle (ISO, 2018). Internal teams in the organisation should be educated on the value of proactively documenting their procedures and findings via a centralised platform (Haqaf & Koyuncu, 2018) that is approved by the organisation, thus securely storing information of the information system being built progressively, before an external audit can take place.

**Competence** is key to achieving business goals (ISO, 2018) with security in mind and, thus, it can be the best preventative measure to overcome cyber security attacks within an organisation; in fact, it ensures that the workforce is equipped with the theoretical knowledge and practical skills to fulfil business requirements (Koohang *et al*., 2020) by placing security at the core of both software design and development stages. Along with this fundamental concept, **confidentiality** is an attitude that should be instilled in the company culture since its inception, thus safeguarding the organisations and their clients’ information (ISO, 2018), such that they are not disclosed to unauthorised third parties (Aminzade, 2018).

**Continual improvement** is a fundamental mindset that can improve the performance of individuals and teams (ISO, 2018), as well as the quality and the security of the features in the applications being developed and deployed. Individuals should be trained to recognise the value of continual improvement (Haqaf & Koyuncu, 2018; AlGhamdi *et al*., 2020) as a means for improving themselves in their careers, as a part of their team/s in the organisation, and to ensure that security-related best practices are strictly adhered to drive sustained organisational success.

**Information systems** are all applications that handle information or data (ISO, 2018); thus, it is of paramount importance to secure such information throughout its layers and lifecycle from an architecture standpoint (Hameed & Arachchilage, 2021). The workforce should be trained to architect secure information systems from design to development, deployment, and support.

**References**

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

Aminzade, M. (2018) Confidentiality, integrity and availability–finding a balanced IT framework. *Network Security* 2018(5): 9-11.

Hameed, M. A., & Arachchilage, N. A. G. (2021) The role of self-efficacy on the adoption of information systems security innovations: a meta-analysis assessment. *Personal and Ubiquitous Computing* 25(5): 911-925.

Haqaf, H., & Koyuncu, M. (2018) Understanding key skills for information security managers. *International Journal of Information Management* 43: 165-172.

ISO (2018) ISO/IEC Standard 27000 Section 3 Terms and Definitions. Retrieved from <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en>.

Koohang, A., Nowak, A., Paliszkiewicz, J., & Nord, J. H. (2020) Information security policy compliance: leadership, trust, role values, and awareness. *Journal of Computer Information Systems* 60(1): 1-8.