**Unit 1: Information Risk Management: Definitions, Standards and Approaches**

**In this unit we shall:**

* Review a number of common definitions of Information Risk Management.
* Review some common Information Security Management Concepts.
* Discuss the Risk Management Process.

**On completion of this unit, you will be able to:**

* Discuss the various definitions of risk.
* Explain how to assess, qualify and mitigate risks.
* Describe various approaches to quantify and qualify risks.
* List common risk standards and select the appropriate one(s) for a given situation.

**Reflection**

A company's IT risk management, often known as "information security risk management," comprises of the policies, processes, and technologies it employs to minimize risks from hostile actors and to eliminate information technology vulnerabilities that adversely influence data security (Securityscorecard.com. et al., 2019).

Risk management is the process of recognizing risk, evaluating risk, and reducing risk to an acceptable level. Organizations utilize risk assessment, the first phase of the risk management approach, to establish the scope of the possible threat, vulnerabilities, and risk associated with an information technology (IT) system (N.I.S.T. et al., 2020), (Kull, T.J. et al., 2008), (Ritchie et al., 2007).

ISO 27000, a series of standards, is perhaps the most well-known standard for the comprehensive management of information security. Particularly, ISO 27001:2013 is a risk-based standard for information security management systems. It embraces a global perspective of business, process, people, and technology risks, and senior management is actively engaged in the whole process of risk mitigation. In this regard, it offers an effective foundation for implementing an enterprise-wide risk management system (Cyberwatching. et al., 2018).

Commonly there are four types of risk management which is given below.

1. Risk acceptance
2. Risk transference
3. Risk avoidance
4. Risk reduction

**References:**

Securityscorecard.com. (2019). What is IT Risk Management? A Complete Guide | SecurityScorecard. [online] Available at: <https://securityscorecard.com/blog/what-is-information-risk-management>.

SP800, N.I.S.T., 30. Risk management guide for information technology systems. National Institute of Standards and Technology Special Publication, pp.800-30.

Kull, T.J. and Talluri, S., 2008. A supply risk reduction model using integrated multicriteria decision making. IEEE Transactions on Engineering management, 55(3), pp.409-419.

Ritchie, B. and Brindley, C., 2007. An emergent framework for supply chain risk management and performance measurement. Journal of the Operational Research Society, 58(11), pp.1398-1411.

Cyberwatching. (2018). Relevant Standards for Cybersecurity Risk Management. [online] Available at: https://cyberwatching.eu/relevant-standards-cybersecurity-risk-management.