**Topic:** InfoTech importance in strategic planning

**Question:**

What do you think were the critical factors that fueled the need for IT governance? In what ways did ISO affect the standards for network security?

**Instructions:**

* Need only 2 Responses including APA references excluding textbook for other student posts
* Minimum 150 words for each response (use uploaded document to see other student posts)
* Provide extensive additional information on the topic
* Explain, define, or analyze the topic in detail
* Provide an outside source (References) that applies to the topic, along with additional information about the topic or the source (please cite properly in APA)
* Textbook attached
* No plagiarism please

**Initial Post 1:**

IT Governance is an organized procedure to guarantee that organizations use their IT investments suitably to ensure that the subsequent activities, whether projects, programs, or events that they support, are done appropriately and accomplish the ideal outcomes. IT Governance offers a component to coordinate the IT plan with the corporate strategy. In adopting a conventional structure, then they can convey quantifiable results toward objectives achievement (Ali, Nor, Abdullah, & Murad, 2014). The structured plan frequently contemplates the interests of partners and the prerequisites of employees and the techniques that embrace them. IT Governance gives a component for correlating the IT plan with the business strategy. IT Governance is a significant piece of corporate governance. The critical factors that fueled the requirement for IT Governance are as per the following.

* The governance structure refers to the administration structure of their organization, just as how it permits the decision-making procedure of the organization and guarantees coordinated, reliable improved performance in the administration of services (Amali, Mahmuddin, Ahmad, & Katili, 2018). Most enterprises, as of now, have a sort of governance set up. For instance, a typical territory of management incorporates taking care of tasks and arrangement of undertakings.
* Communication and readiness ought to be planned, exhaustive, and illustrative and reproduced to quicken the usage of authoritative administration procedures and assets.
* Roles and responsibilities in the association, when organizations characterize, archive, and dole out jobs and obligations inside their governance structure, precise desires are set for the employees who doled out specific roles. Precise desires make individuals effective (Amali et al., 2018).
* Culture is another factor, and In each association, culture is unique. Therefore, an association should address the social changes in an all-around imparted and planned manner. Change compromises a few people in the organization, whereas some may never show signs of change. (Ali et al., 2014)

These days, because of the expansion of digital assaults, associations have begun actualizing the ISO 27001 standard. Thus, it is smarter to be stable and steady to protected from attacks. ISO will give thorough directions on the security ramifications of the administration, activity, and the utilization of data management systems and the linkages (Tatiara, Fajar, Siregar, & Gunawan, 2017). refers to the assurance of associated gadgets just as to the administration of the security, network applications/offices, and network clients. Notwithstanding the security of information transmitted using communications links. In an accompanying manner, ISO influences the standards for network security in an organization.

* It assists with characterizing how associations ought to accomplish quality network specialized security structures, plans, and usage that will guarantee network security proper to their business surroundings, utilizing a reliable way to deal with the planning, architecture, and execution of network security (Tatiara et al., 2017).
* Provides direction on an organized procedure to distinguish and investigate network security risks and consequently characterize network security control necessities, including those ordered by appropriate data security strategies.
* It provides an outline of the controls supporting network specialized security structures and related technical controls, just as non-technical controls, in addition to other technical restrictions that not exclusively identified with network security (Kao, 2017).
* Serves as an establishment for definite proposals on overall network security, and it covers the issues of hazard, engineering, techniques, control measures in the organization.

These standards tied in with assisting with overseeing data security as well as help to recognize and bring lawbreakers to equity (Lewis, 2019). For instance, ISO offers rules that depict procedures and standards appropriate to different sorts of examinations, including unauthorized access, information debasement, and system crashes as well as some other digital inspection.

**Initial Post 2:**

Organizations have prepared their checklist when it comes to the implementation of information governance (IG) programs. Most of the organizations are pursuing profitability, business agility, and other features through their IG programs. One of the main drivers for having IG programs is to gain deeper insights related to the procedures and processes securely. IG programs also are used for unlocking the information potential in various business areas. Even though not directly related to network security, IG has helped the organizations in decreasing their discovery and litigation expenses. In general, organizations would spend enormous amounts and numerous months for creating valuable information (Mooradian, 2018). Once the information is subject to threats of losses, businesses have to retain the information through the discovery process. IG teams and programs have helped the organization to develop e-Discovery programs enabling relevant information to be accessed and identified more easily. Offering up-to-date information to the business clients and automated categorization of the defined procedures will create procedures needed for defensible destruction of the information. Auditing can also be done effectively amidst growing regulatory changes. It will be possible to retain the records in an automatic manner, which is integrated with the record retention process. This step can help in decreasing the risks related to businesses. It is possible through the IG for knowing the legacy data, which can no longer be useful for the organization. Through the effective IG, it would be possible for identifying the systems and applications which have become obsolescence (InfoGov, 2017).