Security Audits: Health Body Wellness Center

Name

Institution

Security Audits: Health Body Wellness Center

Business Objectives

The primary objective of the Health Body Wellness Center (HBWC) Office of Grants Giveaway (OCG) is to support and promote advances in the usefulness and quality of hospital grants or donations by way of federally supported evaluation, information sharing, and research. Healthy Body Wellness Center achieves this by using the Small Hospital Tracking System (SHGTS) that assists in tracking the small hospital grants given. The grants are assigned to a given hospital within a period of one month, during which if not utilized in all are “rotated” to another hospital (Davis, 2013). The system is used to track the grants delivered then follows the donations through all hospital facilities. For purposes of documentation, a weekly report is availed to the executive officer and a monthly briefing done before the report is generated.

Guiding Security Principle

Healthy Body Wellness Center tracks any first delivery of funds through five hospital facilities. For intensive security purposes, pertinent information is also tracked with only an executive staff allowed to assign grant funds. At the same time, the requirement that specifies that all grants must be completed is another security principle that pushes all recipients of the grants to complete their allocations before receiving another grant. If not exhausted, HBWC assigns the balance to another hospital facility. Thus HBWC ensures that the grants given out are exhaustively used.

Business Process and Justifications

The entire business process entails a risk assessment strategy that identifies threats and vulnerabilities. Additionally, the process entails any likelihood of a vulnerability being exploited, any countermeasures placed with the aim of mitigating the risk and the possibility of having a residual risk. The process is wholly dedicated to underscoring possible risk assessment activities that WTE plans to undertake in the period in which OGG takes up its security measures in addition to the risk exposures. The process is critical to the scenario since it will help in understanding the level of commitment and practical evaluation of the procedural activities during the entire process. According to Abbasi, Sarker and Chiang, (2016) in any business information system framework, it is important to apply the process at all stages of the project scope to widen the scope and success of the risk mitigation efforts within the organization and its corresponding activities. The process is critical in its inclusion within the system as it will no doubt help in countering any unintended forthcoming action and activity within the processes. Of particular interest are confidentiality, availability and integrity, also known as the CIA triangle. CIA triangle is a security model developed to offer guidance on information security strategies within an enterprise. Thus, the model has a direct impact on business operations regarding information processing and handling. For instance all threats, risks and vulnerabilities within an organization are weighed against their ability to compromise the principles of CIA triad. It means that all security policies, strategies, and operations must reflect the basis and framework of CIA triad. CIA triad will therefore directly impact a company’s decision processes, success rates in information management and information frameworks to employ while managing the information system.

Information Systems

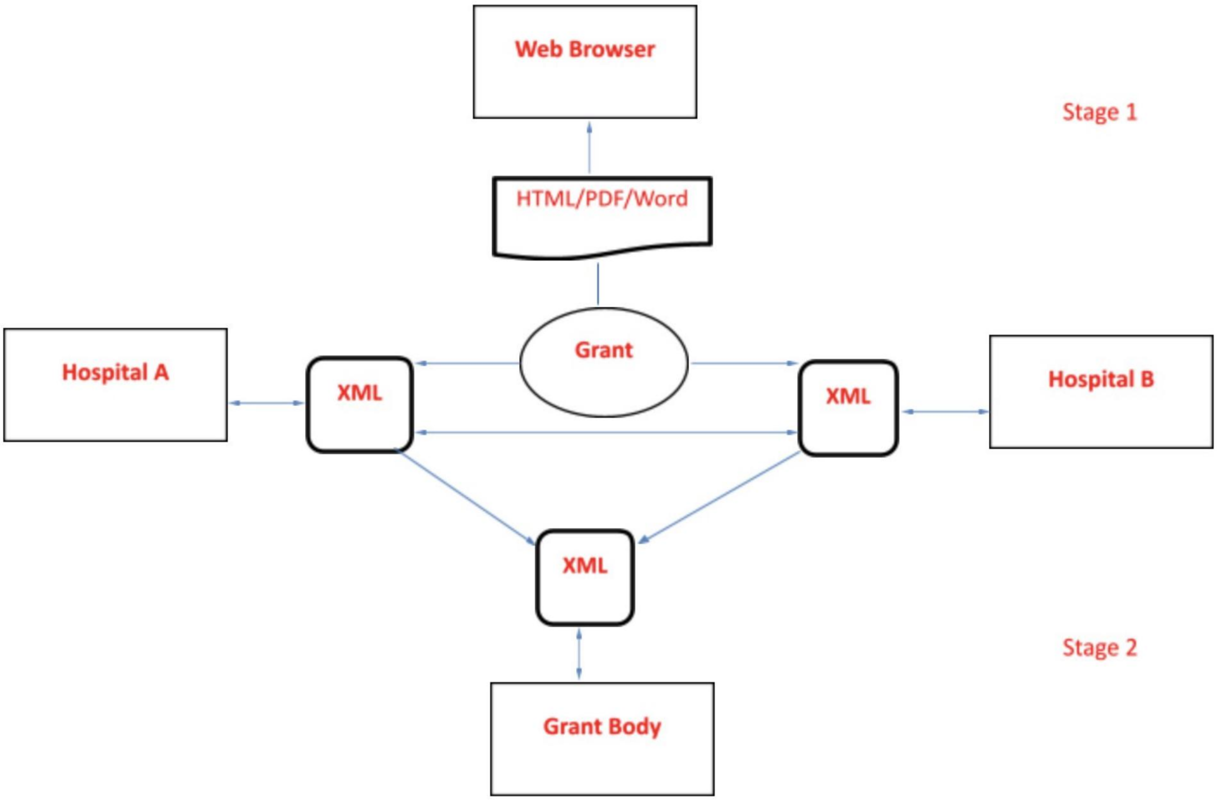
The primary purpose of the information system is to help in decision making through use of raw data gathered from the processes. At the same time, the information system will play a significant role in supporting outlined processes in carrying out precise procedural analysis entailed in business activities. The main features of the information system within the ISMS plan will include software (the Microsoft Access), hardware (computer components), data, procedures (the processes), people, and communication between the various departments involved in the risk assessment plan and scope. On the other hand, PDCA or the plan-do-check-actor plan-do-check-adjust refers to an iterative management methodology in a business operation meant to control and have a continuous improvement on products and processes. Adopting PDCA would thus improve major business processes and operations by way of streamlining the business waste-reduction cycle. The cycle entails a binding commitment to unceasing improvement that is aimed at having a positive effect on productivity. Besides driving improvement, the cycle helps in the implementation of changes that are consistent with the broader objective of "performance drive-outcome." It thus helps in adopting an improvement culture within an organization leading to a culture of excellence.

Duties of the Information System

According to Pearlson, Saunders and Galletta (2016) the primary function of the information system within the scope plan is to manage data storage and process. At the same time, its principal role is to support the key features of the organization that involve communication organization, record keeping, data analysis, and decision making. The inclusion of the information system within the ISMS plan will help in making accurate reporting, faster decision making, and efficient use of resource allocation (Davis, 2013). Further, the inclusion of information system will help in general visualization that will go a long way in enabling analysis and making of better decision making considering the large amount of information that the system may handle at a given time. Additionally, Pearlson et al., (2016) noted that the inclusion of the system will help in predicting future patterns of events while at the same time, considering historical data in the account.

IT Infrastructure

According to Abbasi, Sarker and Chiang (2016) an IT infrastructure entails all of the enterprise networks, hardware, software data centers, and facilities. They are the equipment's used in developing, testing, operating, monitoring, managing, and or supporting information technology services within an organization. Within the ISMS plan, various IT components will be applicable. According to Pearlson et al., (2016) within the IT infrastructure, data flows from one component to another considering the general IT components' layout and configuration. Within the ISMS plan, data will take the typical path from personnel to the IT hardware's, into the processing configuration and finally to the display or storage components. The data flow within the infrastructure will take the input-output flow in which data will be input into the system, processed, and given out as processed output. The diagram below is a typical data flow arrangement that can apply within the ISMS structure and information system.



The structure is a typical simple flow of information from various information system components that entail personnel, hardware, software, and parts involved in passing information from one location to another.

Additional Risks

Data safety is a critical component of any information management. One of the most outstanding risks not addressed in the organization towards implementation of the ISMS plan are chances of an external attack that include viral attack, worms, hacker, or system breakdown. According to Pearlson et al., (2016) a viral attack is often damaging to data within a system. Failure to create a backup or have anti-virus in place may expose data within the system to damage and or structural changes. Abbasi, Sarker and Chiang (2016) maintained that system security is thus critical towards ensuring that data is protected and secured from an external attack that includes unauthorized access by hackers or personnel who may change or damage data or information flow within the system structure.

Recommendation

It is important to have in place security measures that include strong passwords within the system to bar unauthorized access in addition to keeping the information offices out of bound for unauthorized personnel (Pearlson et al., 2016). At the same time, it is critical to ensure that only knowledgeable persons access and use the IT infrastructure within the premises holding the hardware components of the ISMS IT plan. Installation of antivirus is also critical towards prevention of a viral attack such as boot sector viruses, web scripting virus, multipartite virus, resident virus, and direct action virus. These can easily be avoided by way of installing an up to date anti-virus in the system with the ability to prevent and discard any potential danger to the information system.

References

Abbasi, A., Sarker, S., and Chiang, R. H. (2016). Big data research in information systems: Toward an inclusive research agenda. *Journal of the Association for Information Systems*, *17*(2), I.

Davis, J. L. (2013). *Healthy Body Wellness Center Office of Grants Giveaway Small Hospital Grants Tracking System: Initial Risk Assessment*. We Test Everything LLC.

Pearlson, K. E., Saunders, C. S., and Galletta, D. F. (2016). *Managing and using information systems, binder ready version: a strategic approach*. John Wiley & Sons.