Week 4 - Module Project: Security Plan Section 4: Compliance and legal standards

IT controls, compliance and audit plan are very essential for every organization in today's world if the organization wants to thrive and be a success considering security and control breaches around the world. As businesses rely heavily on technology, and any organization without the correct and the required measures, policies and standards, the said business or the organization is highly likely to be attacked, as such the organization is bound to fail. We will consider few or some of the internationally recognized standards, policies and measures for our IT controls and audit plans which in turn, will help us stop, mitigate or transfer some of the common and unknown risks in our environment. It will be a combination of COBIT, ITIL, COSO and the rest if the known standards and framework.

Having said that, we will go ahead and adopt these IT controls and Audit plans for our organization and business with a focus on;

1. IT Governance Component
2. Control Component

IT Governance Component

IT Governance basically offers the framework for aligning IT plan with that of the business. Having that framework, business will be able to yield measurable results in the direction of realizing their strategies and goals. An agreed program also considers investors' benefits into account and considers the requirements of employees and the procedures they ought to follow. In all, IT governance is an essential component of the general enterprise governance.

Now, under the IT Governance, there are many areas we are going to look at or consider. These are;

- **Policies & Standards** – Classification of risk administration is it's an identified / amended method or deterrent / alleviated method. With this knowledge, we will know the way internal process are controlled with the environment.
- **Processes & Guidelines** – classification of methods which are being followed by the business and technology role for the subsequent components of governance;
    - Hazard Valuation of the business, technology and purposes of the business.
    - Observation and process of dealing with information security requirement.

- Observation and the process of dealing with the internal control efficiency for application systems and security of the network.
- "Business continuity management, disaster management, and availability, security, and recoverability of key systems"
- Operative provision "(SLA) of network, operating systems, applications, and help desk/issue management".

- **Organizational edifice of the Information Technology** - Ask of business and IT management on the view if IT has adequate possessions to succeed and control technology all over the organization. Recognize if technology roles are rooted in business procedures, a centralized purpose, subcontracted purpose, or assorted accomplished with portions centralized, rooted, and subcontracted.

- **Legal Compliance** - Recognize by what means legal requirements are achieved in the technology processes. Regulate at what time legal elements (e.g., HIPAA) are recognized, revised, and are held responsible within IT processes.

- **Risk Management** - Classify the well-known controls of how recognized dangers and risk are managed. Investigate whether rules and measures address well-defined risk parts. Investigate if IT supervision roles are recognized to manage clarified risk areas and the way managerial and decision-making management are well-versed of risks, controls, and control efficiency outside external/internal audit assessments.

- **Awareness** – Find out if adequate consciousness on the policies and standards all over the organization is present and supports the organization and IT purposes. We also need to find out if IT efficiently communicate policies and standard to employees of the organization.

Control Component

According to the **COSO** model, internal control can be said of a procedure, achieved by an organization's board of directors, management and other staffs, intended to offer practical guarantee of the accomplishment of purposes three classifications below:

- Usefulness and productivity of operations
- Consistency of financial reporting
- Submission with appropriate laws and regulations

Under the control components, we are also going to pick few or some of the required points or areas and discuss as part of the over all plan and strategy of compliance and IT controls.

- **Procedures** - Classify the way procedures are kept and accessed by employees who ought to follow them. Recognize if procedures are protected to avert unintentional access or exposures.
- **Align Business and IT** - Classify if there is a high 'accept risk' rate for past and older technology and a high explanation rate for 'cost prohibitive' control enhancement areas.
- **Testing of Control Component –** At this stage, we will design a dedicated means of testing the internal control based on the audit plan for the organization. So, there are few evidence we will require from the IT management.
    - Standard procedures, measures, and description of present risks, extenuating controls, and monitoring status.
    - Papers of IT and corporate evaluations of security for users, privilege users, and third-party happenings.
    - Business endurance approach, backup management, and clearly stated incident management together with testing and reporting.
    - Administration of modification controls as well as proof of identity, testing, approval, execution, and overall cost relationships (e.g., trending on symptoms, increasing costs, interfaced and/or security impacts).
- **Control Efficiency** – there are also few steps at this stage which will help us to assess the control usefulness.
    - Assessment of the drive and aims of the control.
    - Indication of the existence of the control.
    - Indication of the control operating as envisioned.
- **Administration of Assessment of Risk** - The assessment of risk supposed to be insistent and continuing as the business, controlling and technology changes are insistent and continuing. Risk assessment supposed to be rooted into business and IT procedures.

Certification is one of the important areas in IT controls and Auditing. This is because, is it seen basically that, once a certain standard and requirements have been met, the organization has at least the basic knowledge and compliance in the said industry. Due to this, we will follow the needed

process, regulations and the needed requirement to be certified and recognized in the industry which in turn will contribute to the benefits of the business and be in line with the vision of the organization.

With the above IT control and audit plans, I believe the organization in general is in for business and will achieve it's over all mission and contribute to the development of the nation while it recommendations IT controls and audit will be of benefit to its clients.

References:

Kim Lindros July 31, 2017. What is IT Governance? A formal way to align IY & Business strategy. Accessed online (February 6, 2019). https://www.cio.com/article/2438931/governance/governanceit-governance-definition-and-solutions.html

Kate Riley, CISA, September 2010, IT Governance and Control Framework Audit Plan. Accessed online (February 6, 2019). https://www.resourcenter.net/images/AHIA/Files/2010/AnnMtg/Handouts/E5_ReferenceMaterials.pdf

Sharise Cruze, October 28, 2016. What are the five components of COSO framework? Accessed online (February 7, 2019). https://info.knowledgeleader.com/bid/161685/what-are-the-five-components-of-the-coso-framework

Kirk Rehage, Steve Hunt, Fenando D. Nikitin, Global Tecnology Audit Guide (GTAG 11) – Developing the IT Audit Plan. Accessed online (February 7, 2019). https://chapters.theiia.org/montreal/ChapterDocuments/GTAG%2011%20-%20Developing%20the%20IT%20Audit%20Plan.pdf

Ernst & Young, Insights on governance, risk and compliance. February 2013, Ten Key IT considerations for internal Audit. Assessed online (February 7, 2019). https://www.ey.com/Publication/vwLUAssets/Ten_key_IT_considerations_for_internal_audit/%24FILE/Ten_key_IT_considerations_for_internal_audit.pdf