Project #4: Audit Policy and Plans

[Author’s name]

[Institute’s name]

Project #4: Audit Policy and Plans

**Executive Summary**

The higher management of red Clay Renovations company is interested in successfully established the approach of information technology considering the application of proper cybersecurity systems. The technological forms of “smart home” and “Internet of Things” are adopted by the company to successfully updating its business services effectively and efficiently. The increasing trend of technology application made it essential for the company to appropriately document a security policy ensuring the prospect of a significant auditing domain. The approach of documented policy for IT needs to be effectively aligned with IT security policy compliance, facets of audit plans for policy awareness. Furthermore, the development of the audit plan in case of IT security policies is also one mandatory practical measure to ensure the successful form of the overall security plan of the company. The perspective of employee compliance evaluation is also critical to recognize suitable grounds in case of domains of audit plan documentation. Detailed documentation of the audit plan for the Red Clay Renovations company is also vital to enhance the awareness level of all employees. this form of understanding eventually helps them to meet the standards of IT security compliance. Proper implementation of the company’s security controls is only possible when IT security policies are easily understandable for all the employees.

**Issue Specific Policy for IT Security Policy Compliance Audits**

**Purpose**

The central purpose of the auditing IT security policy compliance in the case of Red Clay Renovations company is to develop a successful form of compliance audits considering the domain of overall IT security policy. It is one core responsibility of the stakeholders to ensure proper documentation of IT security policies needs to be successfully aligned with the overall IT security policy developed in the case of Red Clay Renovations company. The aim of developing and executing various IT security policies is to enhance the understanding level of all workers considering the importance of information security for the company. A detailed review of IT security policies in the form of a compliance audit is a mandatory condition to analyze the practical organizational approach to ensure the application of regulatory guidelines.

**Scope**

The policy-relevant to IT security policy compliance audits apply to the functioning of all the employees under the broader domain of internal audit plan set by the higher management of Red Clay Renovations company.

**System Overview**

A brief description of the organization’s system approach is a necessary step to recognize the actual requirements of information security and compliance system. Information Technology Security Program (ITSP) by the organization of Red Clay Renovations company is the focal aspect of consideration. When it comes to the identification of system category in case of an organization’s information security, it is established its position as the domain of “moderate level” under the standards of FIPS 199/200 and specifications provided by NIST SP 800-53 Revision 4.

           The main functions in the case of an organization’s system are mainly characterized as accounting & finance, customer relations, human resources, marketing, corporate management, and information technology services. The current status of the system is defined as the operational prospect considering the domain of Systems Development Lifecycle. It is noteworthy to mention that currently, the organization is not focusing to upgrade the system referring to the feature of major developments.

**Responsibilities/Requirements**

           Detailed documentation of required responsibilities is an important step to meet policy goals and objectives in the desired manner. The perspective of requirements in the form of audit policy relevant to various aspects of consideration that requires necessary attention (Hayes, 2003). The main responsibilities or roles under the domain of IT security compliance audit policy.

* Successful consideration of standards of audit practice is an essential step for the auditors to attain desired outcomes from the audit program. The team of auditors is responsible for developing, maintaining, and successfully managing the entire paradigm of the internal IT security audit program.
* Audit standards set by Information Standard Organization (ISO) follow in case of an information security audit program in case of the information system of Red Clay Renovations Company.
* Confidentiality is one prominent policy issue that needs to be a focus on the proper development of the audit plan for the company’s information security system. All the auditors are strictly restricted to never share important internal organizational information with unauthorized entities for the sake of any purpose (Goodyear, Goerdel, Portillo, & Williams, 2010). Confidentiality standards need to be aligned with the data protection for the organization as the primary aspect of consideration.
* Proper consideration of security controls in an organizational setting is a necessary condition to provide relevant security assurance. The broad idea of security controls actively linked with the protection of information assets and ensure data privacy. The phenomenon can also be observed in case of proper preservation of integrity and reliability of data by focusing on essential standards, policies, and regulations.
* One of the key objectives is to timely assess and report all forms of threats and vulnerabilities concerning the unexpected items and specific circumstances. Moreover, the purpose of evaluation can never be achieved without the delivery of engagement to all the shareholders and defines the actual objectives and scope of the audit process.
* The responsibilities of auditors further enhance when it comes to sharing findings and recommendations to the relevant entities after the execution of the complete procedure of internal audit in the organization. This approach only appeared when it is requested by the shareholders to attain the necessary advice by the audit team.
* Another critical aspect relevant to the practical idea of information security audit policy is to successfully enforce the objectives of proper integrity. It is critical to ensure complete protection of data in the forms of accuracy and completeness. Information should not be damaged by any unauthorized entity.

**The Option of Compliance Audit as Internal Audit**

           The practical approach of compliance audit can be used by the organization to meet the objectives of an internal audit (Gao, 1991). This plan of audit linked with the adoption of a specific form of regulations and standards to timely identify all the security risk factors and adopt necessary measures.

**Compliance Audit Checklist**

* Identification of non-compliance aspects in the form of workers’ practices within an organizational setting.
* Obtain necessary evidence to determine specific features of irregularities during the audit process.
* Application of necessary action plans and strategies assigned to the relevant authorities.
* Proper documentation of all the observations and formulated suggestions accordingly
* Accurate validation of the entire audit program is a necessary step to determine the authenticity of the auditing within an organizational context.

**Audit Plan for IT Security Policy Awareness and Compliance (Employee Survey)**

***Questions about Awareness of Key Policies***

1. Is Email can be used as a simple and protective way to convey important organizational information?
* Agree
* Strongly agree
* Neutral
* Disagree
* Strongly disagree
1. Are you able to timely recognize an issue concerning to IT security program of the organization?
* Agree
* Strongly agree
* Neutral
* Disagree
* Strongly disagree
1. What is the major source of risk when it comes to the application of the information security program in your department?
* Improper system applications
* Human error
* The threat of viruses
1. Is it mandatory for you to lock access to your workstation?
* Yes
* No
1. Do you have an understanding of all the protocols when it comes to using personal devices within an organizational setting?
* Yes
* Partially Yes
* No

***Questions about Awareness of Personal Responsibilities regarding Compliance***

1. Do you use personal electronic devices for work purposes?
* Yes
* Sometimes yes
* No
1. Do you successfully apply all the standards of IT security you learned through training?
* Yes
* No
1. Do you agree that it is okay to allow someone else to use your working system?
* Yes
* Unsure
* No
1. Are you ensuring proper back-up of important organization’s data?
* Yes
* No
1. Do you believe is it okay to open different web links when it comes to completing the organization’s tasks?
* There is no problem with it
* I am unsure
* No

**Audit Plan for IT Security Policies Audit (Documentation Assessment Strategy)**

Comprehensive planning and development in the form of documentation assessment strategy are important to offer a significant form of IT security policies audit plan (*Winnipeg.ca,* 2008). This consideration aims to estimate and prioritize risks considering different operations of the Red Clay Renovations company. The approach of compliance relevant to three main and interrelated factors. These aspects are defined as the consideration of assets at risk, the magnitude of the threat, and the vulnerability of the system in case of dealing with the information security threat.

**Background Information on the Policy**

A detailed examination of the existing form of audit policy in case of an organization’s information security program is a necessary measure to propose better strategies of compliance in the future. The assessment of the current audit domain of the organization revealed that audit policy is owned by the Chief Information Officer (CIO) to successfully assess all the reports and successfully established audit findings. The central focus of current audit domains within an organization setting is to consider the importance of technology infrastructure when it comes to determining the effectiveness and suitability of the company’s application of security controls. The broad idea of IT security policy considering the importance of employees’ awareness of IT security policies and the proper compliance with these policies.

**Application of Compliance Audit**

Different practical options can be used by the audit team to ensure better outcomes from the approach of the IT security policy audit program. Different ways can be used to obtain the necessary information to meet the standards of the audit plan. Interview management is one option to collect necessary information about the potential risk of data theft or any form of misconduct. Critical analysis of the entire system and IT infrastructure is also mandatory in the organizational scenario. Additionally, a critical review of relevant documentation also helps to identify the potential IT security hazards.

* Exploration of all the valuable assets is first to step to ensure the successful realization of potential risk. The facets of valuable assets are recognized under the domains of servers, websites, information technology instruments, and the contact information of clients.
* A timely examination of potential risks in case of IT security is one of the first steps to meet the objectives of the audit compliance program. Moreover, it is also essential to determine the potential consequences that can be appeared in case of data security risks. These consequences are mainly established as data loss, the insignificant performance of system or application, legal complications, and inability to meet the organization’s objectives.
* Exploration of all the potential hazards and their aligned level is also an essential approach to successfully handle the situation of vulnerability of the IT security program. This form of application is a vital step to develop and deliver better recommendations under the spectrum of IT security audit process.

In concluding remarks, it is vital to indicate that the active role of the CIO is immensely crucial to timely deliver assessment policies and program to other stakeholders. This form of consideration ultimately helps to propose necessary solutions in case of ensuring a better form of IT security within an organizational setting.

**References**

#### Gao.gov. (1991). How to Get Action on Audit Recommendations? Retrieved from

#### https://www.gao.gov/special.pubs/p0921.pdf

Goodyear, M., Goerdel, H., Portillo, S., & Williams, L. (2010). Cybersecurity management in the states: The emerging role of chief information security officers. *Available at SSRN 2187412*.

Hayes, B. (2003). Conducting a Security Audit: An Introductory Overview. Retrieved from Symantec.Connect website: https://www.symantec.com/connect/articles/conducting-security-audit-introductory-overview

####  Winnipeg.ca (2008). Assessment of Information Security Awareness. Retrieved from https://www.winnipeg.ca/audit/pdfs/reports/ITSecurityAwareness.pdf