gug

by Asd Ihi

Submission date: 04-Jul-2021 01:03PM (UTC-0400)
Submission ID: 1615593089
File name: order_770639_1.docx (27.49K)
Word count: 1328
Character count: 7347

Audit Policy and Plans

Student Name

Due Date

Executive Summary

Every organization's IT security and regulatory compliance are critical. A company's crucial data is always at risk of being interfered with; as a result, it is necessary to protect the company's crucial data by implementing network security processes and performing regular upgrades and checks to maintain proper performance. Because non-compliance with security and regulatory requirements can cause big penalties, enterprises must monitor regulatory compliance audit procedures(Senft et al., 2016). Red Clay Renovations is operational in terms of technology and employees, which is critical to the company's success. Red Clay Renovations needs to put in place auditing standards that will enable the company's IT professionals to keep track of any vulnerabilities to figure out what the present and potential dangers are. Compliance measures are laid down to prevent the company from losing valuable information about the company, leading to further loss in profits(den Butter et al., 2012). To ensure compliance during the audit, Red Clay Renovations must meet all security and compliance requirements.

Specific Policy for IT Security Policy Compliance Audits

Audits can be done on-site, remotely, or a combination of both. The audit procedure may fluctuate depending on the audit level that is required. The following steps will be included in the audit, commonly known as Red Clay Renovations:

- Having a meet-up with the IT manager to tell the audit levels.
- IT Policies and Procedures are being reviewed.
- Compliance reports of the Red Clay Renovations and its security
- Making an after-action report that identifies all issues and offers solutions to any bad discoveries

- Assist the customer in developing and implementing a plan to reduce the risks.
- Go over the places that need to be updated.
- Prepare a final report after examinations.

Auditors should observe RCR's security policy for handling sensitive information. Sensitive information should be encrypted, and auditors should use "bring your own device" policies. If the audit report contains sensitive data, it should be handled with care and kept in a secure area accessible only to the auditors. To ensure that data access to RCR's system is protected and only used for auditing purposes, the auditor should sign a non-disclosure agreement.

To maintain confidentiality and data integrity, the companies employee must understand who has access to given networks at a given time. It is mandated that people's Personally Identifiable Information (PII) should not be publicized; RCR recognizes this mandate and bars even the company employees who have no use in accessing the data. RCR values the privacy of all its stakeholders, and this policy is specifically made to keep off the third party from accessing the data.

Audit Plan for IT Security Policy Awareness Compliance

The audit plan consists of four processes: preparing an audit, working with the auditors, and implementing the auditor's recommendations to fill in the gaps in the procedures and processes. The audit would help identify the security gaps in Red Clay's Security policies and ensure that employees understand the policies and do not put the organization's data at risk. The IT awareness security levels depended on several levels depending on the employee position. Many of them are not informed about cybersecurity threats; however, they are aware of their

cybersecurity policies. Employees at the entry-level are unaware of the threats that the company may face. Despite their lack of preparedness, most company employees are confident that the company is prepared for any threat that could come their way.

Employees have a responsibility to follow the state laws, federal laws, international rules, and the company rules in the Employee's handbook on privacy. Every Employee is expected to follow all of the regulations outlined in this policy and to seek clarification from the IT department if they have any issues. According to Scott-Douglas, the effort of implementing and maintaining a cybersecurity policy aids a company's shift from ineptitude to knowledge(Trozzo, 2019). To improve the employees' IT security awareness, the employees need security training to keep them updated. In addition, during the employee onboarding process, the organization should engage in IT security training. The employees need to note that the attackers are interested in the company's data and the Employee's data. To protect their data, they need to understand the basics of cybersecurity and follow the already existing company's security rules.

Audit Plan for IT Security Policies Audit

Every day, customers entrust businesses with their Personally Identifiable Information (PII). Customers may be hesitant to give their personal information to a corporation that has been featured in practically every news outlet due to a breach of information. This is all the more reason for Red Clay Renovations to regularly protect its data by training personnel and informing them of the ramifications of the company's data breach. Customer happiness is important to Red Clay Renovations because it is expected to get the attention of new clients if present customers are good with the company's level of data security. Red Clay Renovations will benefit from installing Security Awareness and Training Policy and Procedures, Security Awareness Training,

Role-Based Security Training, and Security Training Records to have the finest IT auditing for the company's internal system.

The Audit Approach

1. A data collection plan

   Data intended to be collected are:

   - Data on the company's IT system's security, including whether it is updated or not. For example, whether or not the organization has updated anti-virus software.
   - The individual roles of people in the company
   - The Employee's understanding of the system security
   - Evidence that the IT system satisfies the operational needs.

   How the data will be collected

   - Direct interviews
   - On-phone interviews
   - Testing
   - Mail questionnaires
   - Conducting online surveys

2. Document Review

   The following papers will be checked to make sure that Red Clay Renovations' IT security is updated and that it is operational:

   - System Security Plan (SSP)
   - Plan Of Action and Milestone (POAM)
   - Security Assessment Report (SAR)

3. Some of the survey questions that were asked include

   This document contains a set of questions that must be asked to determine Red Clay Renovations' IT security posture

   - What is your position in the organization, and what are your responsibilities?
   - Can you share, or have you ever shared your password with someone?
   - Do you understand what phishing is and ways to recognize when it is taking place?
   - How often are IT systems in the company audited?
   - Do you know of the existing company IT team?
   - Can you describe your computer as secure?
   - How do you know if an intruder attacks a computer?
   - Does your computer have a firewall in it?
   - Are all the necessary services running?
   - Is your anti-virus updated?

Red Clay Renovations' executives have put in place security plans and policies that will help the company meet its standard requirement of obtaining certifications for its operations and identify any vulnerabilities and provide countermeasures to ensure a secure environment for data storage, processing, and transmission. IT auditing should be considered by any firm that relies on technology to operate its operations. Information security, business continuity, mobile device usage, software and hardware management, and social media risk are just a few of the concerns that may prompt companies to conduct an IT audit.

Organizations must never disregard information security since the data in their IT systems is a valuable asset that must be safeguarded at all costs. Because the cost of dealing with

information being illegally accessed by an unauthorized person is so high, businesses take the necessary precautions to ensure that data is always protected. This will encourage firms that rely largely on technology, such as Red Clay Renovations, to audit their IT systems to ensure that security safeguards are current.

References

den Butter, F. A. G., Liu, J., & Tan, Y.-H. (2012). Using IT to engender trust in government-to-business relationships: The Authorized Economic Operator (AEO) as an example. *Government Information Quarterly*, *29*(2), 261–274. https://doi.org/10.1016/j.giq.2011.05.004

Senft, S., Gallegos, F., & Davis, A. (2016). *Information Technology Control and Audit*. CRC Press.

Trozzo, E. (2019). *The Cyberdimension: A Political Theology of Cyberspace and Cybersecurity*. Wipf and Stock Publishers.

gug

ORIGINALITY REPORT

24%	1%	1%	24%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to University of Maryland, University College Student Paper	24%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		