SmallSEOTools

PLAGIARISM SCAN REPORT

Words	595	Date	January 26,2020
Characters	4100	Exclude Url	

0%	100%	0	31
Plagiarism	Unique	Plagiarized Sentences	Unique Sentences

Content Checked For Plagiarism

Security in the Modern World (Quantifying the Security Risk of an Enterprise) In recent years, the telecommunication industry has witnessed significant growth with the increasing omnipresence of communication devices, and inception and development of new technologies such as IoT (Internet of Things), which have led to a substantial augmentation in interconnectivity. However, these developments have also exposed a glaring concern – the security risks and vulnerabilities which accompany them. Security risk management is an ongoing process to identify and manage these risks, followed by implementation of plans to mitigate them. It assigns relative priorities for mitigation plans and implementation. Thus, a risk assessment framework is needed for categorizing and sharing information about the security risk IT infrastructure. Vulnerabilities and the Security Framework Assessing vulnerabilities is a major task in any organization. Vulnerability analysis is a part of the risk assessment process. It focuses on methods for identifying vulnerabilities, and implementing suitable protection plans to maintain a certain standard of network security. In order to regulate the risk assessment process, a uniform and unanimous configuration is requisite. A security framework is a holistic structure for risk assessment. It is used to evaluate security capabilities across industry standards by using tools to identify shortcomings in controls, score the level of IT risk and prioritize rectification and repair. Even natural calamities like earthquakes, floods and fire are included in the list of risks, as these can impact the organization’s assets and its physical structure. Security Risk Assessment Security Risk Assessment is the process of evaluating the security risks of an organization to ascertain the required countermeasures. To be effective, risk assessment must be a continuous process. The motive is to identify the threats and vulnerabilities that could affect the privacy, integrity and accessibility of the system. The assessment is done at the early stages of product development, and is later modified as changes occur in the information asset and its environment. The process involves assessment and analysis of all assets and processes related to the system. It can be divided into three categories: 1. High level Assessment, which is applied to systems at design phase in order to identify risks before implementation. 2. Comprehensive Assessment, which is used to assess a particular constituent system and to gather feedback for improvement. 3. Pre-Production Assessment, conducted on new information systems before they are rolled out. An Insight into Modern Risk Assessment Tools - LUCIDEUS SAFE SAFE (Security Assessment Framework for Enterprise) is an AI and ML based platform which performs enterprise-wide cyber risk assessment and quantifies organizational security. It is a dynamic cyber risk assessment platform which integrates with the existing IT infrastructure and security tools deployed within an organization. It performs real time assessment both at a macro (enterprise-wide) and a micro (asset-wise) level to allow an organization to visualize, track and enhance their cyber risk posture. Key features of the platform include: • MACRO LEVEL ASSESMENT: Using 2500+ controls encompassing over 15+ global compliances, SAFE assesses the entire IT stack and provides a comprehensive security score from 0 to 5 • MICRO LEVEL ASSESSMENT: Provides a 360 degree view of technology-wise security posture, which is then further funneled down to an individual asset’s level. • REAL-TIME ASSESSMENT: Enables the organization to receive a synchronous, live assessment of their assets. • HACK SIMULATION: Virtually simulates attacks to evaluate the organization’s cyber-defense system against known hacks. • AUTO PATCHING: Allows easy remediation of vulnerability and configuration controls following changes in a control process. • COMPLIANCE MANAGEMENT: Provides a real-time analysis of the system in comparison to the global compliance framework.

Sources	Similarity