

Additional Information of Assessment:-

The Security Audit Assessment is designed to help organizations assess weaknesses in their current IT security environment. It will help identify processes, resources, and technologies that are designed to promote good security planning and risk mitigation practices within your organization.

After you complete the Assessment, we suggest you go through the report and decide whether you want to go through a thorough security audit.

Business Risk Profile

Understanding how the nature of your business affects risk is important in determining where to apply resources in order to help mitigate those risks. Recognizing areas of business risk will help you to optimize allocation of your security budget.

Defense-in-Depth

The "Defense-in-Depth" (DiD) concept refers to the implementation of layered defenses that include technical, organizational, and operational controls. This assessment is based on accepted standards and best practices to help reduce risk in IT environments.

Reports

You will receive a full-length report that describes your company's security posture, based on your answers, and provides industry-recognized best practices and recommendations for achieving those practices.

Areas of Analysis

With the Security Audit Assessment we evaluate your organization's security practices in such areas as Infrastructure, Applications, Operations, and People.

The following table lists the areas that are included in our security risk assessment.

Business Risk Profile	Importance to security
Business Risk Profile	Understanding how the nature of your business affects risk is important in determining where to apply resources in order to help mitigate those risks. Recognizing areas of business risk will help you to optimize allocation of your security budget.
Infrastructure	Importance to security
Perimeter Defense	Perimeter defense addresses security at network borders, where your internal network connects to the outside world. This constitutes your first line of defense against intruders.
Authentication	Rigorous authentication procedures for users, administrators, and remote users help prevent outsiders from gaining unauthorized access to the network through the use of local or remote attacks.
Management & Monitoring	Management, monitoring, and proper logging are critical to maintaining and analyzing IT environments. These tools are even more important after an attack has occurred and incident analysis is required.
Workstations	The security of individual workstations is a critical factor in the defense of any environment, especially when remote access is allowed. Workstations should have safeguards in place to resist common attacks.
Applications	Importance to security
Deployment & Use	When business-critical applications are deployed in production, the security and availability of those applications and servers must be protected. Continued maintenance is essential to help ensure that security bugs are patched and that new vulnerabilities are not introduced into the environment.
Application Design	Design that does not properly address security mechanisms such as authentication, authorization, and data validation can allow attackers to exploit security vulnerabilities and thereby gain access to sensitive information.
Data Storage & Communications	Integrity and confidentiality of data is one of the greatest concerns for any business. Data loss or theft can hurt an organization revenue as well as its reputation. It is important to understand how applications handle business critical data and how that data is protected.
Operations	Importance to security
Environment	The security of an organization is dependent on the operational procedures,

	<p>processes and guidelines that are applied to the environment. They enhance the security of an organization by including more than just technology defenses. Accurate environment documentation and guidelines are critical to the operation team's ability to support and maintain the security of the environment.</p>
Security Policy	<p>Corporate security policy refers to individual policies and guidelines that exist to govern the secure and appropriate use of technology and processes within the organization. This area covers policies to address all types of security, such as user, system, and data.</p>
Backup & Recovery	<p>Data backup and recovery is essential to maintaining business continuity in the event of a disaster or hardware/software failure. Lack of appropriate backup and recovery procedures could lead to significant loss of data and productivity.</p>
Patch & Update Management	<p>Good management of patches and updates is important in helping secure an organization's IT environment. The timely application of patches and updates is necessary to help protect against known and exploitable vulnerabilities.</p>
People	Importance to security
Requirements and Assessments	<p>Security requirements should be understood by all decision-makers so that both their technical and their business decisions enhance security rather than conflict with it. Regular assessments by a third party can help a company review, evaluate, and identify areas for improvement.</p>
Policies and Procedures	<p>Clear, practical procedures for managing relationships with vendors and partners can help protect the company from exposure to risk. Procedures covering employee hiring and termination can help protect the company from unscrupulous or disgruntled employees.</p>
Training and Awareness	<p>Employees should be trained and made aware of how security applies to their daily job activities so that they do not inadvertently expose the company to greater risks.</p>