**Cybersecurity Audit Checklist**

* With the rapid development of the modern technology, the cyber threats towards the data security have risen up massively. However, when it comes to the current network systems & data systems, there is a massive diversity within those environments. Due to the complexity of the modern systems, each & every section needs to be given much attention individually. It’s a huge responsibility of the network & security engineers to consistently monitor the functionality of the security aspect of their systems.
* According to the current industry standards, it has become mandatory for any organization to conduct a proper risk assessment procedure within the organization. Usually, when a data breach happens, an organization goes through a massive number of losses such as financial losses, customer losses, loss of confidence etc.
* So, it has now become very crucial for an organization to perform regular audits of the organizational environment. When it comes to the cybersecurity audit checklists, there are massive number of broad categories that need to be given attention. Following are some of the main highlighting cybersecurity threats & categories that may crucially affect towards the entire security infrastructure of an organization.

|  |  |  |
| --- | --- | --- |
| **Cybersecurity Audit Checklist** | | |
| **Category Name** | **Checklist** | **Readiness** |
| 1. **Management** | Company security policies in place |  |
| Security policies written and enforced through training |  |
| Computer software and hardware asset list |  |
| Data classified by usage and sensitivity |  |
| Established chain of data ownership |  |
| 1. **Employees** | Awareness training on handling situations like phishing, social engineering etc. |  |
| Password training and enforcement |  |
| Training on dealing with strangers in the workplace |  |
| Training on carrying data on laptops and other devices and ensuring the security of the data |  |
| Ensure that Secure Bring Your Own Device **(BYOD)** plans are in place |  |
| Ensuring that the employees have gained both the theoretical & practical knowledge from the awareness training program |  |
| 1. **Business Practices** | Emergency and cybersecurity response plans |  |
| Determine all possible sources of business disruption cybersecurity risk |  |
| Having proper plans in place to reduce business disruptions and security breaches |  |
| Emergency disaster recovery plans in place |  |
| Alternative locations for running business in case of an emergency or total disruption |  |
| Redundancy and restoration paths for all critical business operations |  |
| Performing regular check-ups on the restoration and redundancy plans |  |
| 1. **IT-Related Staff** | System & OS hardening plans |  |
| Automated system hardening on all the servers, routers, workstations, and gateways |  |
| Automated software patch management |  |
| Security mailing lists |  |
| Conducting Regular security audits and penetration testing |  |
| Anti-virus software installed on all devices with auto-update feature enabled |  |
| Systematic review of log files and backup logs to make sure there are no errors |  |
| Having remote plans & policies in place regarding the remote access |  |
| 1. **Physical security** | Lock the necessary servers and network equipment properly |  |
| Have a secure and remote backup solution |  |
| Ensure that the keys for the network are in a secure location |  |
| Keep computers visible |  |
| Use physical locks on computer cases |  |
| Perform regular inspections |  |
| Prevent unauthorized users from entering the server room or in the workstation areas |  |
| Implementing a security camera monitoring system |  |
| Implementing a keycard system for high-security areas |  |
| Implement necessary data security policies in place & make sure the users fully aware of those policies |  |
| Secure trash dumpsters and paper shredders to prevent dumpster diving |  |

|  |  |  |
| --- | --- | --- |
| 1. **Secure Data** | Application of proper encryption mechanisms when required |  |
| Secure laptops, mobile devices and storage devices |  |
| Enable automatic wiping feature on lost or stolen devices |  |
| Implement Secure Sockets Layer (SSL) in place when using the Internet to ensure secure data transfers |  |
| Implement secure email gateways ensuring data is emailed securely |  |
| 1. **Active Monitoring & Testing** | Perform regular monitoring of all aspects of security |  |
| Regularly scheduled security testing |  |
| Conduct external penetration testing to ensure that the staff has covered all the aspects of security |  |
| Scanning for data types to make sure they are secure and properly stored |  |