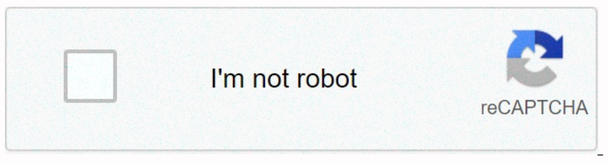


Continue

# Information security site visit checklist

Published 19th December 2019 by Shanna Nasiri • 4 minutes reading today's complex and diverse network and data security environment. There are hundreds of pieces for security systems and all those pieces need to be looked at individually and in their entirety to ensure they not only work well for your organization, but are also secure and do not pose a security threat to your company and your data or your customer data. Risk management and risk assessment are important parts of this process. Data loss and data breaches harm your organization and can create or destroy companies, especially if a breach causes other organizations to lose confidence in your ability to keep your data and their data private. For this reason, it is very important that you conduct regular audits of your environment. There are hundreds of items that can be included in the cybersecurity audit checklist. Here are some broad categories and ideas that include many important cybersecurity threats: Management Company security policies in place Security policies written and enforced through computer software training and hardware asset lists Data classified by use and sensitivity Established chain of employee training data ownership on phishing, handling suspicious emails, social engineering hackers Password training and law enforcement training on dealing with strangers in the workplace Training on carrying data on laptops and devices other and ensure the security of this data All security awareness training passes and is signed ensuring that all employees not only understand the importance of security but also active guardians for security Ensuring that the Secure Bring Your Own Device (BYOD) plan is put in place Business practice plan Emergency response and cybersecurity Determine all possible sources of business disruption cybersecurity Risk Plan to reduce business interruption and security breachEs Emergency disaster recovery plans in place Alternative locations to conduct business in case of emergency or disruption Redundancy and restoration pathways for all important business operations Are you testing your restoration and redundancy plans? It staff hardening plans Automatic system hardening on all operating systems on servers, routers, workstations, and gateways Management patches automatic security mailing list software? Regular security auditing and penetration testing Anti-virus software installed on all devices with automatic updates A systematic review of log files and backup logs to ensure there are no Remote Plan errors in place, as well as policies regarding remote access Physical security key servers and network equipment Have a secure and remote backup solution Make sure the keys to the network are in a secure location Keeping the computer visible Using in the case of a computer Perform regular checks Preventing unauthorized users from entering server space or even in work station areas The camera monitoring system key card system is required Secure data policy area in place and ensure users understand policies through training Safe bins and shredders to prevent dumpster diving Secure data Encryption is enabled wherever necessary Secure laptops, mobile devices, and storage devices Allows automatic wiping of lost or stolen Devices Secure Sockets Layer (SSL) in place when using the Internet to ensure secure data transfer Secure email gateway ensures scheduled security data external penetration testing regularly to ensure your staff does not miss Something that scans these types of data to make sure they're safe and stored properly There are three levels of security in the organization. Information Security or InfoSec covers everything and refers to information processes and technologies designed to protect any kind of sensitive data and information either in print or electronically from unauthorized access. Cybersecurity is a subset of InfoSec and deals with protecting internet-connected systems including hardware, software, programs, and data from potential cyberattacks. It protects the integrity of the network from unauthorized electronic access. Cybersecurity is the practice of defending your organization's networks, computers, and data from unauthorized digital access, attacks, or corruption by implementing processes, technologies, and practices. There are many advanced threats that target multiple organizations and it is critical that your infrastructure is secured at all times to prevent full-scale attacks on your network and risk exposing your company's data and reputation. Network Security is a subset of cybersecurity and deals with protecting the integrity of any network and data sent through devices within that network. We discuss Network Security in other blog entries. This blog also includes a Network Security Audit Checklist. Governance Framework When creating an information system security program, start with the right governance structure and management system software. There are many articles on this website about what governance frameworks are, but frameworks are set up to ensure that security strategies align with your business goals. Governance aligns business security and information, so teams can work together efficiently. It also defines everyone's roles, responsibilities, and accountability and ensures that you meet compliance. CIA Model When security experts create policies and procedures for effective information security programs, they use the CIA Model (confidentiality, integrity, and availability) as guidance. Components of the CIA Model are Confidentiality, Integrity, and Availability. Confidentiality: Ensure that information is not accessible to unac authorities—usually by enabling encryption—available in a variety of Integrity: Protects data and systems from by an un authorized person; ensure that the data has integrity and does not change between the time you created it and the time the data arrived on the intended party. Availability: Ensures that authorized persons can access information when necessary and that all hardware and software is retained and updated when necessary. The CIA model has become the standard model for keeping your organization safe. These three principles help build a set of security controls to preserve and protect your data. About Other Cybersecurity Audit Checklists There are many cybersecurity checklist sources that you can find on the Internet. Some companies are happy to provide their checklists and others charge for them. Some just charge an email subscription in hopes of selling other products and services on the way. It really doesn't mean to start taking some of these security checklists because they are a great place to start developing yourself, because you really need to create your own checklist. No one else has the same network, device, and software configurations that you have. That canned list is just a ballpark idea of how you should check your security, as will be included in this document. For your checklist to be effective, you need to take a basic checklist or checklist collection, put it together, and then add specifics to your environment. Also, as the organization is constantly changing, you will make changes to it over time. ZenGRC can help streamline the process of creating and updating security controls for your information, related objects such as risks, threats, and vulnerabilities, as well as auditing and assessment tasks. You can attend a new security class that will give you ideas to add to your checklist. Or you can buy a new firewall or some new anti-virus software that will make you rethink how you do certain aspects of your checklist. You can also decide that you want to outsource your security checks, although even if you do that, you will want to have your own checklist and compare it to what your outsourcing consultant uses to make sure that they have covered all bases as well as add things from their checklists to yours. Do officers have a Guard Card they have? Is the uniform clean & Neat? Do officers need new uniforms? If so what size and are they hard or soft? Are Postal Orders clear and concise? Is the officer knowledgeable post order? Do you provide the exact amount of training needed to be knowledgeable with the site? Is IIPP included in the Post Order? IIPP site specifics? Are all officers aware of what IIPP means? Do all officers sign contracts with IIPP? Do you know who your Branch Manager is? How often do your Branch Managers and other Supervision visit the site? Do you feel you have the support you need from Management or other office staff? Otherwise what can we do to provide the support you need? When you have a work-related problem that is brought to the Manager or other supervisor they handle on time? If you can't give an example of when this happened? How is your timesheet delivered? Are you trained on how to fill out timesheets correctly? Are you getting paid properly? If not &; payroll correction is required how often does it happen & is the correction done on time? Is there a known Danger of Salvation? If so they have been reported? Do you know what a miss is? If so, you report it to your Management? Management?