CybrHawk
Transforming Cybersecurity

CYBRHAWK
SECURITY ASSESSMENT

✉ 954-669-1960

✓ sales@cybrhawk.com

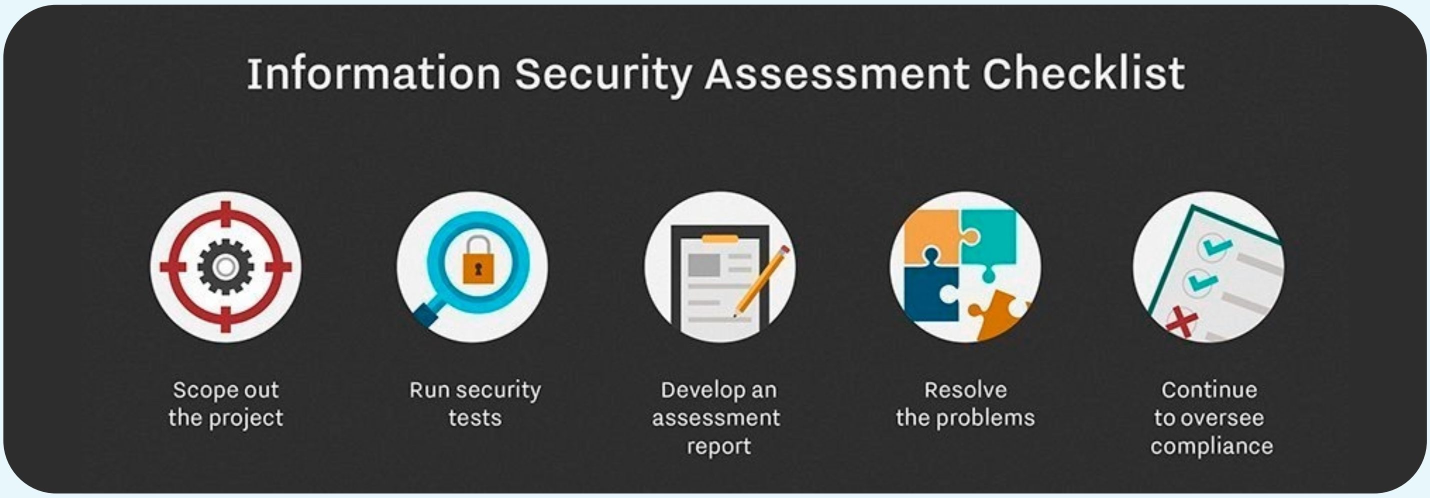
www.cybrhawk.com

Why **safety reviews** are a must for **every businesses**

You are in the cloud. In 2020, 78% of small businesses will have cloud computing completely embraced. Although most major cloud providers are following standard security protocols, you still need to be cautious. Gartner research estimates that the client, not the vendor, will be responsible for at least 95%of cloud protection vulnerabilities over the next four years. Adopting data visibility and monitoring tools like dashboards to track cloud utilization, however, would reduce security error occurrences by one quarter.

To comply with the specifications. HIPAA, FISMA, GDPR, PCI DSS — you may feel endless about the regulations you need to keep with. Many of these require regular assessments of security. Daily internal security reviews will help ensure that you pass the compliance certificate third-party audits that are required.

To remain up to new threats. Changes in technology are occurring rapidly now. According to Gartner's report, "A Comparison of Vulnerability and Security Configuration Assessment Solutions" (full content available to Gartner clients), different approaches to security assessments are necessary because of IoT (internet of things), virtualization, Bring Your Own Device (BYOD), big data, and mobile devices.


Information Security Assessment Checklist
Scope out the project
Run security tests
Develop an assessment report
Resolve the problems
Continue to oversee compliance

To detect infringements of security. Also, a security breach is not revealed to businesses until the hacker demands ransom and sensitive information begins to circulate in the public domain. Assessments of protection help you identify breaches faster. The sooner a data breach is detected and included, the lower the costs will be.

How to thoroughly and effectively **carry out** a security assessment

Most businesses do not carry out safety evaluations either because they feel it is expensive or because they are unfamiliar with the method of carrying out an evaluation. Organizations may perform safety audits internally using in-house tools to minimize costs. Even then, it is still a good practice to bring in a third party specialist to evaluate your security posture on a less frequent basis. This will not only enable you to capture the gaps that you have missed, it will also help you to remain compliant with regulations such as HIPAA and PCI DSS that require assessments from third parties.

The first step in building a culture of security and constant vigilance is to perform regular security assessments.

The below five basic steps are how to plan and carry out an internal security audits:

- Update the safety policies in place: The organization may or may not already have a safety policy in place. If you don' have one, making it is now the best time. If you have one, now is the time to review it to ensure that any recent market developments are still valid.

- Understand vulnerabilities and risks: Prepare a list of all potential threats to your company based on past experiences, your colleagues' experiences, news reports, etc. Identify weaknesses in your process that might exploit these risks.

- Prepare the reviews: List the existing control systems in place and outline additional actions that may help mitigate the risks found. Such controls may include improvements in policies or practices, procurement of software, learning material and specifications, or new applications and/or hardware implementation.

- Scanning for protection: To detect threats and hazards, use security software to conduct a full review of systems, networks and computers at least once a month. Some security software offers scanning capabilities in real time and automatically. If you don't have security software in place, it should be a priority to incorporate such a program.

- Check for security weakness: It's often hard to spot holes or flaws in a program you've built or used for a long time. A vulnerability evaluation is a collection of processes that help you identify vulnerabilities and score them based on the nature of the problem they could potentially cause.