CyberWatch for IT Risk Management

IT Risk Management

IT risk management can be difficult for many organizations that don't understand the full breadth and vulnerability of cyber data and devices. As such, IT risk management is a topic that is never really completed and should always be part of conversation at your place of business.

At its most basic level, IT risk management is applying risk management methods to any area of information technology; you identify threats and vulnerabilities to your resources, and decide what actions to take and when. While this sounds simple enough, it's a crucial subset of your company's overall risk management and requires constant monitoring and improvement. Luckily, standards such as COBIT, ISO, NIST, and CIS Cloud Security help guide your way.

It is even becoming more commonplace for third parties to ask for proof of compliance with these standards before agreeing to do business with another organization. As part of their due diligence, companies will ask for records of compliance as well as an assessment. Due to the highly specialized content that companies must be familiar with, many are often forced to bring in specialists or consultants to complete these risk assessments.

However, hiring professionals or consultants can be costly, and with such a large task, most companies will need multiple individuals. We've designed our software so that you don't need to hire any additional staff to complete your risk assessments and using the software to complete an assessment doesn't require any training. Ultimately, your goal is to reduce risk and prove you are maintaining your systems to be in line with all required standards.

These standards outline very specific security criteria that a business must meet to be deemed compliant. As an example, NIST 800-53 dictates that information systems have session locks able to conceal displayed information for when users stop work and move away from the area temporarily. CyberWatch turns these standards into an easy to answer survey format that can be distributed to existing staff members.

Risk Callout

In January of 2019, power company Duke Energy Corp. was fined an alarming **$10 million** for over 100 different violations from 2015 to 2018.

The violations were quoted as collectively posing a serious risk to the security and reliability of the power system. “many of the violations involved long durations, multiple instances of noncompliance, and repeated failures to implement physical and cybersecurity precautions.”

Why Manage IT Risk

The importance of IT risk is due to the legality of following set standards, as well as the risk carried by not following them. If a data breach were to occur, any third parties you are in business are going to need proof that you were compliant, as well as your legal team, in order to avoid hefty legal fees

As with all aspects of risk management, IT risk management is an indefinite process. New threats and vulnerabilities emerge in the business environment almost as quickly as solutions can be prepared. This is even more-so true in IT, as technology advances at an ever-increasing rate.

Old threats and solutions need to be reevaluated regularly to ensure the processes in place are still effective and are being followed. The identification, assessment, and management of IT risks ensures your business continues to operate smoothly and you avoid any fines for negligence or noncompliance.

It may often be the case that after identifying a threat to one of your assets, your company decides not to take countermeasures to lower risk. This often occurs with resources that aren’t vital to the company. This is standard, and an essential component of management as you decide how to best allocate your resources. IT risk management is essential because it forces you to take a closer look at all of your company’s assets and determine their value and importance in your priorities.

You’ll find there is an increasing number of regulations and a demand for operational transparency. Not only when required, but for the safety of other businesses, they might request proof of your compliance with certain laws, policies, regulations, or best practices.

An organization in the U.S. may only have to be compliant with NIST, but for doing business globally, they’ll then have to check compliance against ISO to show they meet international standards.

After a study discussed by Safran, we know a staggering **92%** of CEOs that were surveyed agree that having information about risk is important or critical to long-term success. In addition to the aforementioned reasons, it really comes down to being able to plan for business continuity and understanding your goals for your organization.

IT Risk Management Methodology

Different methodologies and frameworks were created to guide the IT management process, and each have their own steps and processes. Often, you'll find that these frameworks align with content.

ISO and COBIT, for example, are very similar and so companies prepping assessments will typically choose just one or the other for content. ISO covers information security management (policy/procedures), whereas NIST 800-53 covers actual controls/safeguards but you will find that both will have you verify that your organization employs a secure log-on procedure. Some crossover is never a bad thing as it allows you to ensure that you're not bypassing any important areas of risk management.

Ultimately, the standards you select for your assessment are going to bring to light some degree of risk. The following standards and best practices are popular for use in understanding IT risk and are worth looking into:

- COBIT
- ISO 27001
- CIS Cloud Security
- CSA Critical Controls
- NIST 800 Series & CSF

Many tools offer limited visibility and leave organizations vulnerable to threats both internally and within third party networks. Utilizing data-driven security ratings can help you continuously monitor and measure your cybersecurity. Sign up for a trial of CyberWatch and select the suggested standards for IT risk management.

Using CyberWatch, we can help you to meet all required standards and regulations for your industry and location, as well as supplemental standards that ensure your business is safe and secure. Fully utilize the power of technology and automation; we know your time is better spent elsewhere.

Key Features

Customized Assessments and Reports

Simply select which regulations and standards you want to measure risk with and the questions will be added to your survey. You can edit the questions and how they are answered to better fit your needs. Reports can be customized to mimic your current report layout and with white labeling.

IT Risk Reporting

With the click of a button, create an auto-generated report showing the status of any risk assessments you've completed. Easily gain insight into problem areas with suggested remediation and any supplemental photos.

Assessment Ease of Use

The software sends introductory emails to anyone that will be completing an assessment and explains how to complete their task. Assessment management is automated with reminder emails that are sent to users that have not completed their assignments and the software will email an admin if there is continued lack of progress.

Dashboard Overview

Quickly look at your dashboard to see an overview of your risk score across all locations, letting you know where to focus your attention and resources.

How We Help

You must delve into some specialized content, but it comes down to knowing what is required and making sure you meet those expectations. This is simplified with the use of software. Managing third parties is a multifaceted task and becomes more difficult with every third party you choose to do business with, but CyberWatch offers a proactive approach to understanding your security gaps.

Our platform helps you prepare for audits, identify vulnerabilities and manage your mitigation plan. You can even complete your assessments in about 70% less time, all while keeping your data organized in a central location and creating automated reports with the click of a button.

CyberWatch uses a survey-based process and risk is then calculated based on responses and gaps found in the survey. The software also recommends action plans, assign tasks, and tracks and manages remediation based on the results of the survey.

With our software, there is no need to train staff on specific content or hire specialists. CyberWatch comes preloaded with over 35 content libraries that our experts have formulated into easy-to-answer questions. Simply select your standards and send out the surveys. This process is entirely customized, allowing you swap in any relevant questions from our content libraries or create your own. The system sends automated reminders for completing assessments and compiles data in the dashboard for a quick overview of areas assessed and overall risk.

CyberWatch saves time by sending smart email to users, introducing them to the assessment process, automatically pushing them through the assessment, offering recommendations, and assigning tasks to implement those recommendations.

* Model Inputs	Without CyberWatch	With CyberWatch
Hours needed to communicate (email) and interview client, perform survey or request documents to review	1	0
Hours required to gather assessment data**	3	1
Hours required to analyze data gathered	4	2
Hours required to perform remediation	3	1
Hours required to write report	20	4
Total Hours	31	8
Total Reduction of Time	74% (23 hours per assessment)	

*The time saved can be multiplied by the amount of people that are involved in each step of the assessment process. We have only included a single person for each step in the model inputs above.

**SecureWatch can provide data not available in current assessment program

RiskWatch offers free trials and a consulting service to assist in performing a proof of concept using any of its assessment platforms. Manage all types of risk from across your business through a single, securely accessed, web-based tool that reduces risk and improves operational effectiveness and efficiency.

Try it Now

RiskWatch