



# CyberWatch for COBIT Compliance



## CyberWatch for COBIT Compliance

With today's prevalence of technology in the workplace, we can't stress enough the importance of cybersecurity and keeping an effective cyber framework in place. As such, we often recommend COBIT compliance to anyone looking for best practices regarding IT systems in risk assessments. What's great is that this framework works well across organizations of all different sizes. It also integrates with other popular frameworks and standards such as ITIL and ISO.

### The Five Principles of COBIT:

\*As determined by ISACA

- 1 Meeting stakeholder needs.
- 2 Covering the enterprise end to end
- 3 Applying a single integrated framework
- 4 Enabling a holistic approach
- 5 Separating governance from management



Now that you know the principles, we will discuss what COBIT is and why its framework can be a positive resource to your company.

## CyberWatch

An Information Security Risk Management Platform

## What is COBIT?

COBIT (Control Objectives for Information and Related Technologies) is a globally recognized set of controls for information technology. The framework was created by ISACA (previously known as the Information Systems Audit and Control Association) to help businesses develop and implement strategies around information technology management and governance.

COBIT provides your organization guidance on making decisions regarding the use of information technology to support and maintain your business objectives. They are an independent association with professionals in 187 countries, so anything you're not compliant with should raise some red flags and alert your team to take a closer look. COBIT is not required, so any changes you decide to make are up to you, but it's in your best interest to at least review any suggestions.

## COBIT Users:

Not all COBIT methodology will be relevant to everyone, but at least part of their content usually ends up in our customers' assessments. COBIT is helpful if you want to gain trust from your partners or customers, need guidance on IT processes, or simply need to better understand IT-related goals, objectives, and results. If that sounds beneficial to you, it's worth taking a look at.

Primary users deal with audits and assurance, compliance, IT Operations, Governance, and Security and Risk Management.

## COBIT Compliance:

COBIT offers content that calculates your overall compliance. You can either use their platform, or use another service that has purchased their content and analyzes it for you. As an example, we take all of the content from COBIT and our experts formulate easy-to-answer questions that can be used in a survey format. These questions ask "Has the 3-5 year strategic plan been broken down into 1 year tactical plans that drive towards strategic goals?" and "Has a methodology been adopted for enterprise architecture?"

Upon completion of your survey, or other means of data gathering, you'll easily understand if your organization is COBIT compliant. If not, you can review your data to determine what areas need immediate remediation and what tasks can be scheduled in the future.

## COBIT Primary Functions:

\*As determined by ISACA

- 1 Maintain high-quality information to support business decisions
- 2 Achieve strategic goals through the effective and innovative use of IT
- 3 Achieve operational excellence through reliable, efficient application of technology
- 4 Maintain IT related risk at an acceptable level
- 5 Optimize the cost of IT services and technology
- 6 Support compliance with relevant laws, regulations, contractual agreements, and policies

## Who Uses COBIT:

\*As determined by ISACA

COBIT is used in industries such as financial, healthcare, information technology, manufacturing, government, and more.

The COBIT framework is used globally by anyone responsible for business processes and information technology. Whether you're commercial, not-for-profit, or in the public sector, COBIT will be beneficial to you.

## COBIT Progress

Technology continues to change and advance, so it only makes sense that your frameworks follow suit. Rest Assured, COBIT has done a great job of maintaining relevance, contributing to its global recognition. According to ISACA, COBIT 5 “Consolidates and integrates the COBIT 4.1, Val IT 2.0 and Risk IT frameworks and also draws **significantly** from the Business Model for Information Security (BMIS) and ITAF.”

The most recent model, COBIT 2019, continues this constant change by adding in the latest developments that affect enterprise information and technology.

## How We Help

CyberWatch communicates and guides your client, a third-party, or an internal resource through a standardized assessment process and criteria without requiring any training to capture assessment data. When you create your assessment, simply select any COBIT material, as well as any other standards or best practices from our content library. The assessment created will then calculate your risk and compliance. The platform offers recommendations and remediation tasks upon completion.

CyberWatch is equipped with analysis capability, and identifies threats, vulnerabilities, and security gaps and to develop specific recommendations. All if your data is in a centralized location. From the dashboard, you can see an overview of how risk is reducing or compliance is improving over time.

Try out a demo of CyberWatch and select COBIT on your form. That’s a free 30 days to explore how you can benefit from using the COBIT framework in your organization.

Use CyberWatch to manage all types of risk across your organization through a single, securely accessed, web-based tool that reduces risk and improves operational effectiveness and efficiency.

## CyberWatch Workflow

Create assessment and  
distribute survey(s)



Assessor completes  
survey(s) and provides  
documentation



Compute risk score and  
identify individual risks



Determine if facility is  
within your risk appetite



Provide informed  
recommendations to  
facility to reduce risk