# Audit Readiness Guide

KirkpatrickPrice

# Audits are hard.

We believe if you're going to do it, the audit should be ***worth it.***

We know that when it comes to threats you want to make sure that you're ready. In order to do that, you need a quality cybersecurity and compliance audit report that gives you results you can trust. The problem is audits are hard, and the complicated process feels overwhelming.

**This guide should help make your audit a little less complicated and a little easier to get started.**

## Contents

# #1 Why are audits important?

Auditing is an important function of any information security and compliance program and is a valuable tool for effectively and appropriately managing risk. Conducting an audit answers these important questions:

- **Are we sure we are doing what we say we're doing?**
- **Are there gaps in our policies and procedures?**
- **Are there any areas for improvement?**
- **Are there any unidentified risks threatening our organization?**
- **Are we meeting our compliance goals?**

Since an audit is conducted objectively, it is designed to improve and mature an organization's business practices. The purpose of auditing is to provide insight into an organization's culture, policies, procedures, and to aid board and management oversight by verifying internal controls, such as operating effectiveness, risk mitigation controls, and compliance with any relevant laws or regulations, are in place and operating correctly.

Auditing your organization is critical for monitoring and assuring that all of your business assets have been properly secured and safeguarded from threats. It is also important for verifying that your business processes reflect your documented policies and procedures.

## Let’s take a look at five reasons why conducting an audit is important and how it can keep your organization compliant with the common frameworks and regulations.

1. Provides objective insight
2. Improves efficiency of operations
3. Evaluates risks and protects assets
4. Assesses organizational controls
5. Ensures legal compliance

KirkpatrickPrice

## Reason 1

### Provides Objective Insight

You can’t audit your own work without having a definite conflict of interest.

Your internal auditor, or internal audit team, cannot have any operational responsibility to achieve this objective insight. By seeking an independent and unbiased view, your organization receives a diagnosis of its security health from a trusted partner that provides a new perspective.

## Reason 2

### Improves the Efficiency of Operations

By objectively reviewing your organization’s policies and procedures, you can receive assurance that you are doing what your policies and procedures say you are doing, and that these processes are adequate in mitigating your unique risks.

By continuously monitoring and reviewing your processes, you can identify control recommendations to improve the efficiency and effectiveness of these processes. This, in turn, allows your organization to be dependent on processes, rather than people.

## Reason 3

### Evaluates Risks and Protects Assets

When undergoing an audit, your organization will have to perform and provide a risk assessment. A risk assessment can help to identify any gaps in the environment and allow for a remediation plan to take place. The risk assessment will help you to track and document any changes that have been made to your environment and ensure the mitigation of any found risks.

This process ensures that your assets are being monitored and protected year to year.

## Reason 4

### Assesses Organizational Controls

Auditing your control environment assesses the efficiency and operating effectiveness of those controls.  Are your controls fulfilling their purpose? Are they adequate in mitigating risk? Having an independent, unbiased answer to those questions can give your organization peace of mind that it is doing everything it can to meet its security and compliance goals.

## Reason 5

### Ensures Compliance with Laws and Regulations

By regularly performing an audit, you can ensure compliance with any and all relevant laws and regulations. Gaining client trust and avoiding costly fines associated with non-compliance makes auditing an important and worthwhile activity for your organization.

# #2 Types of Audits

Deciding to undergo an **information security audit** can be daunting for the sole reason that there are so many frameworks and regulations to learn about. **SOC 1, SOC 2, SOC for Cybersecurity, PCI DSS, HIPAA/HITECH, HITRUST CSF, ISO 27001, Privacy, NIST, and FERPA** – what do they all mean? Which framework or regulation does your organization need to comply with? Which one best suits your organization's needs?

In this section, you'll learn about the **10 most common information security frameworks**, who they apply to, and how they can benefit your organization. If you still need help figuring out which framework best applies to your organization, just give us a call!

## When to Choose SOC 1

A SOC 1 audit is an audit that is performed in accordance with the Statement on Standards for Attestation Engagements No. 18 (SSAE 18). SOC 1 reports are designed to report on the controls at a service organization that could impact their clients' financial statements. A SOC 1 audit is not a review of a service organization's financial statements, but rather a review of internal controls over financial reporting.

By being able to produce a SOC 1 report to your clients or prospects, you gain a competitive advantage and client trust by demonstrating that you have the proper internal controls in place.

## When to Choose SOC 2

A SOC 2 attestation affirms the security of an organization's services and gives organizations the ability to provide clients with evidence from an auditor who has seen your internal controls in place and operating. A SOC 2 audit evaluates internal controls, policies, and procedures as they relate to security, availability, processing integrity, confidentiality, and privacy of a system.

Demonstrating SOC 2 compliance can also help an organization maintain loyal clients and attract new ones, operate more efficiently, avoid fines for non-compliance or from breaches, and most importantly: assure clients that their sensitive data is protected.

## When to Choose ISO 27001

ISO 27001 is the only information security standard that is recognized across the globe. Its purpose is to provide requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). An ISMS preserves the confidentiality, integrity, and availability of an organization, and gives confidence to interested parties that risks are adequately managed by applying a risk management process to an organization's security system.

Completing an ISO 27001 audit allows organizations to demonstrate to their business partners that a mature and risk-based information security program is in place.

## When to Choose PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a robust information security standard that encourages and enhances cardholder data security by providing industry-recognized data security measures. In other words, a PCI audit is an information security audit focused on the protection of credit card data.

If you are a merchant, service provider, and/or subservice provider who stores, transmits, or processes cardholder data, you must comply with the PCI DSS. Additionally, if you have a client who is required to comply with the PCI DSS, they are required to validate your compliance with the standard as well.

## When to Choose NIST

Compliance with NIST Special Publication 800-53 is required for anyone working with the federal government, a federal contractor, or a sub-service provider of a federal contractor. Agencies will rely on the NIST security and privacy controls (SP 800-53) to determine which controls they expect to be implemented in any of their business partner's environments. To become certified, organizations must determine the security category of their information system, and then appropriately apply a tailored set of baseline security controls outlined in NIST SP 800-53.

## When to Choose Privacy

Privacy audits affirm your organization's compliance with regulatory requirements like GDPR, CCPA, SOC 2 Privacy, the HIPAA Privacy Rule, and other various laws. As data controllers and data processors that handle personal data, a program must be implemented that ensures the ongoing confidentiality, integrity, availability, and resilience of processing systems. Demonstrating a commitment to privacy allows organizations to improve their data management processes, increase customer trust, and build and maintain relationships with current and potential global business partners.

## When to Choose HIPAA

All covered entities and business associates who process, store, or transmit protected health information (PHI) and electronic protected health information (ePHI) must comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Covered entities and business associates are responsible for securing the PHI or ePHI that they hold.

## When to Choose HITRUST

The HITRUST Common Security Framework, or CSF, is a certifiable framework that provides organizations with a comprehensive, flexible, and efficient approach to regulatory compliance and risk management. It is a framework that was built from what works within other standards and authoritative sources, like ISO 27001/27002, HIPAA, PCI DSS, and NIST 800-53, just to name a few. It was also built on risk management principles and aligns with existing, relative controls and requirements. It's scalable depending on organizational, system, and regulatory factors.

Organizations looking to validate their security controls over protecting sensitive data and meeting various security requirements can benefit from engaging in a HITRUST CSF assessment.

## When to Choose SOC for Cybersecurity

A SOC for Cybersecurity examination is how a CPA firm can report on an organization's cybersecurity risk management program and verify the effectiveness of internal controls, with the intention of giving stakeholders perspective and confidence in an organization's cybersecurity risk management program.

This examination is for any organization who wishes to provide their board of directors, analysts, investors, business partners, industry regulators, or users with confidence in their cybersecurity risk management program.

## When to Choose Cloud Security

As more and more organizations migrate sensitive information and services to cloud environments, it drives customers to consider how the cloud will impact their privacy, security, and compliance efforts. Our cloud security assessment services provide critical insight into your cloud configurations so you can make sure your cloud security is in full support of all of your regulatory compliance efforts.

## Why Not Choose Multiple Frameworks?

What if multiple audit frameworks, say SOC 2 and ISO 27001, apply to your organization? The value of a multi-audit process, which is possible through KirkpatrickPrice's Online Audit Manager tool, is that you can complete both a SOC 2 and ISO 27001 audit in the same project engagement. If you've already completed a SOC 2 audit and are looking to prove to clients that you have a holistic approach to information security instead of just meeting the lower-level requirements, you can exceed expectations by completing both audits.

A multi-audit approach would save time as some of the qualifying questions and scoping information needed to complete SOC 2 and ISO 27001 audits overlap, such as details on security training and management role. That means you can spend less time in the weeds of completing an audit and more time showing your clients, investors, and employees that meeting security goals is a top priority.

# #3 What to Expect

**When you start an audit, questions about terminology, processes, and auditing norms can be overwhelming. Understanding the fundamental elements of the audit process is a great way to make sure you start out fully prepared for success. In this section, we'll answer a few frequently asked questions.**

## What is Reasonable Assurance?

Reasonable assurance is defined as a high, but not absolute, level of assurance that your controls are working as they were designed. When you begin an audit, you can expect a designated Information Security Specialist to focus on a high level of effort and confidence in testing. By collecting a large quantity of accurate data and analyzing a reasonable number of controls, auditors work to reach this level of reasonable assurance.

## What is an independent opinion in auditing?

A qualified CPA firm must establish a barrier of independence in order to accurately audit an organization. How can you be assured you are receiving an audit report from an independent auditor? Be on the lookout for auditors with practices in place and qualifications that ensure full independence such as yearly independence checks, high-level certifications, and extended years of experience.

## What is an assertion?

At the beginning stages of the audit process, an organization will be asked to provide an assertion to their auditor. This assertion lays the foundation for the audit because **it is a written claim by an organization describing their systems and what it is their services are expected to accomplish for the organizations they do business with.** It tells auditors how an organization's system is designed and how it's supposed to operate.

Throughout the audit process, an auditor will review an organization's internal controls, culminating in a final audit report wherein the auditor's opinion is based on whether or not the assertion is fairly presented. **This means that when an organization provides their assertion to their auditor, it needs to be as accurate as possible.** For example, if your organization provides an assertion that states your employees are regularly trained and tested on cybersecurity best practices, an auditor will validate that this is accurate.

## What are control objectives?

Throughout the audit process, you're likely to hear the term "control objective" repeatedly. Why? **Because control objectives are statements that address how risk is going to be effectively managed by an organization,** and your auditor will be validating whether or not your organization meets these control objectives during the audit.

During the scoping phase of the audit, you will narrow down a scope for your audit with your auditor and chose around 10-30 control objectives that will be included in the audit. **Determining the best control objectives for your organization is crucial for ensuring that you get the most out of your audit,** which is why organizations need to partner with senior-level expert Information Security Specialists, like those at **KirkpatrickPrice,** who can assist in writing the control objectives and make sure that they're presented reasonably.

**When going through an audit, control objectives encourage organizations to ensure that their security posture is -- and remains -- strong.** For example, if one of the control objectives your organization includes in your audit was, "Our controls provide reasonable assurance that we restrict unauthorized access to our critical systems," then you would need to implement controls to ensure that this objective was met. To validate this control objective, your auditor might verify that you have controls in place such as locked doors, badges, monitoring systems, and logical access controls because those controls all restrict unauthorized access to critical systems.

## What is scope?

Knowing where your assets reside is critical for any organization. Why? **Because knowing where your assets reside and which controls apply to them is the only way you can manage and secure them from a potential data breach or security incident.**

During the initial phases of an audit, your audit team will walk you through the process of defining the scope of your audit. The scope of your audit sets boundaries for the assessment. It requires organizations to identify the people, locations, policies and procedures, and technologies that interact with, or could otherwise impact, the security of the information being protected.

**The scope of an audit can greatly impact the overall effectiveness of the audit.** If the scope is too broad, an auditor could miss critical items during the assessment. If the scope is too narrow, an auditor might not be able to perform an accurate assessment or give an accurate opinion of an organization's controls because some may have been left out. This is why effective scoping is key.

## Will I Pass or Fail the Audit?

During the audit process, your auditor will perform various tests, interviews, and observations to determine whether or not there is reasonable assurance that your organization has internal controls in place that are operating effectively. Because there is no way to give absolute assurance that these internal controls are operating as intended, **auditors must be able to give reasonable assurance that controls are in place and operating effectively.**

When an auditor determines if there's reasonable assurance, they'll issue either a **qualified or unqualified opinion.** An unqualified opinion means there are no qualifications or significant exceptions being issued and reasonable assurance has been determined. On the other hand, if an auditor issues a qualified opinion, this means that there are exceptions. So, for example, "Except for control X, internal controls are in place, suitably designed, and operating effectively." In cases where a qualified opinion is issued, we will list the specific aspects of your system that were not operating effectively in your audit report and provide recommendations for how to best remediate them.

So, it's not about passing or failing, but rather testing the strength and effectiveness of your internal controls. By engaging in an audit, you are allowing your organization to determine if its internal controls are working for your organization or if they need to be made stronger. **Luckily, when you partner with KirkpatrickPrice, we'll make sure you are confident in the strength of your controls.**

# #4

## How do you know you're ready?

**Preparing for an audit can be one of the most daunting parts of the experience. No matter where you are in your security and compliance journey, you are ready to get started.**

Together, we'll begin with readiness and remediation, then move into the audit, and finally, culminate the experience with a high-quality audit report – all with expert auditor guidance along the way. Readiness is a customized experience; wherever you are, we'll work with you to make sure you are ready to successfully complete your audit.

To best prepare, ensure your policies are in order.  Countless regulatory compliance and client requirements depend on clear and appropriate policies and procedures to demonstrate how organizations are conducting their business. Without defined policies and procedures, you face the threat of heavy fines from regulatory governing bodies, loss of business, or loss of data.

# List of Policies

The point of having extensive policies in place is to provide clarity for your employees, direction for proper security procedures, and proof that you're doing your due diligence to protect your organization against security threats. **We've gathered a list of 15 must-have information security policies** that you can check your own list of policies against to ensure you're on the path towards security:

- [ ] Acceptable Encryption and Key Management Policy
- [ ] Acceptable Use Policy
- [ ] Clean Desk Policy
- [ ] Data Breach Response Policy
- [ ] Disaster Recovery Plan Policy
- [ ] Personnel Security Policy
- [ ] Data Backup Policy
- [ ] User Identification, Authentication, and Authorization Policy
- [ ] Incident Response Policy
- [ ] End User Encryption Key Protection Policy
- [ ] Risk Assessment Standards and Procedures
- [ ] Remote Access Policy
- [ ] Secure Systems Management Policy
- [ ] Monitoring and Logging Policy
- [ ] Change Management Policy

# #5

## Benefits of a Quality Audit

**Too often, organizations must deal with the aftermath of receiving an audit that wasn't thorough enough.**

This could mean public-facing S3 buckets, Active Directory policies that don't reflect written policies, failure of physical safeguards, cardholder data that is inadvertently exposed to the public, or worse. These organizations have to deal with breaches, fines and penalties, and in extreme cases, losing their business altogether.

At KirkpatrickPrice, we want to make sure that your organization never faces these consequences, and we do this by delivering quality audits. But what does that mean?

A quality audit can mean different things depending on the intention of the organization receiving the audit. If a business seeks out an audit firm for the sole purpose of checking a box off a to-do list, they probably aren't looking for what we believe to be a quality audit. We want to partner with organizations who are committed to improving their security posture, finding and mitigating vulnerabilities in their systems, and collaborating with an auditor to ensure that the audit process is effective.

# To us, a quality audit has the following features:

***The audit firm is qualified.*** This means that members of leadership have extensive experience in information security and the firm itself has the appropriate qualifications. For SOC 1 and SOC 2 audits, that would be a CPA firm. For a PCI audit, that would be a QSA. For a HITRUST CSF assessment, that would be a validated HITRUST CSF Assessor.

***The audit will be conducted by senior-level information security specialists who hold industry certifications and are regarded as experts.*** If a junior-level auditor or an auditor with no relevant information security certifications has been assigned to perform your audit, consider how that lack of experience could impact your organization.

***The organization has appropriate communication.*** If you have little to no communication with your audit team during the audit, this should be a red flag. If you are suspicious that any step in your process is being outsourced (penetration testing, report writing, etc.), this should be a red flag. How can an auditor conduct a thorough audit if they aren't speaking with you about your systems? How can they understand your business without analyzing it firsthand?

***There should absolutely be an onsite visit.*** If an audit firm offers to conduct an entire audit remotely, they are going to miss physical security vulnerabilities that could greatly impact your security posture. When our auditors go onsite, they've gained access to "secure" locations, plugged into network jacks "hidden" in public spaces, found "protected" cardholder data printed out and stacked into piles in offices, and even found physical holes in walls of data centers due to construction. What would your auditor miss if they didn't come onsite?

***The audit firm would have a quality assurance program in place to ensure that auditors' work is consistent and thorough.*** If there is no quality assurance program, how can you be sure that the auditor performed their due diligence?

Many people are intimidated by the requirements, price, and efforts of auditing, but we believe the benefits outweigh the cost. Yes, undergoing information security audits is a challenging and time-consuming process for most organizations, but our Information Security Specialists aim to educate clients on the value that attestations and compliance can bring to their business, which range from competitive advantages to reputational improvement. When your organization has completed an information security audit and gained compliance, the challenges you faced will be worth it.

# #6

## Next Steps

KirkpatrickPrice

## Now that you've made it through this guide, let's talk about your next steps. Let's make sure you're ready to successfully complete your audit.

We know that audits are hard; the process is complicated and overwhelming. We believe if you're going to do it, the audit should be worth it. We've been in your shoes and know how hard audits can be, but we've issued over ***20,000 reports*** to ***2,000 clients*** worldwide, giving them the assurance they deserve.

## Here's how it works:

### 1) Get ready for your audit.

Whether you've gone through 1 or 100, audit readiness will set you up for success. This guide is a great first step to prepare and empower you to achieve your challenging compliance goals! If you need more guidance, we can help with that, too!

### 2) We partner you with an expert.

Our cybersecurity and compliance auditors have sat in your seat and know how intimidating audits can be. Your dedicated specialist will walk you through the entire process from audit readiness to final report.

### 3) Show off your audit report.

Even though it was a demanding effort, we will make sure your audit was worth it. By the end of the process, you'll be proud of the work you did and know that it will make the difference in gaining new clients and protecting your clients' data. They will see that your report stands out from the automated audits in the market.

**When you work with KirkpatrickPrice, you can stop feeling you are going to miss something or be surprised when a client or attacker finds something that wasn't in your report. You can stop feeling worried that you're wasting your time using someone who's not advanced enough to thoroughly test your environment. Instead, you'll have a report that gets you ready for your next steps, allows you to say yes to client requests, and brings you the assurance you deserve. Cybersecurity and compliance will no longer be a mystery.**

To get started on your audit, call one of our experts today at ***800-770-2701*** or visit ***www.kirkpatrickprice.com.***

P.S. – Let's stay connected! Follow KirkpatrickPrice on ***LinkedIn*** or subscribe to our ***YouTube*** channel.