WHITEPAPER

# HOW TO TURN COMPLIANCE INTO A COMPETITIVE ADVANTAGE



Cloud Checkr

## ABSTRACT

Business managers need to know more about compliance programs to successfully use compliance to their advantage. This paper will provide some insight into common compliance programs and offer helpful information on how to align with compliance goals and use some beneficial tactics to enhance compliance benefits.

## TABLE OF CONTENTS

## OVERVIEW

Companies sometimes see IT security-compliance programs as being like a tax that increases the cost of doing business, rather than as a competitive advantage. This is unfortunate, since compliance programs are created to produce a positive and productive outcome. Most compliance programs have goals like improving security, decreasing risks, improving quality and reputation, and managing the long-term value of an industry.

Businesses should view achievement of each of these goals as a value because it will improve quality as well as trust between the customer and the compliant business. Sometimes this means forcing the business to improve or to adopt standard business-process practices that improve its product or service. When changes are not perceived as benefits, the organization will likely chafe at the requirements.

A company's success with a compliance program depends on its ability to see the value in the program's goals and specific requirements. There are often multiple approaches to meeting compliance requirements that enhance business value.

The logic of a compliance program is that it will improve a business through engagement rather than rejection. That is, businesses that choose a minimalist approach to compliance often do not see much value returned. However, an engaged organization often finds competitive advantage in marketing and enhanced reputation that can improve sales, customer satisfaction, and even employee morale. Additionally, when products are developed to higher standards, these features can be strong differentiators in a competitive market.

> "An organization's ability to learn, and translate that learning into action rapidly, is the ultimate competitive advantage."
>
> **JACK WELCH** | CEO OF GENERAL ELECTRIC

# THE GOAL OF COMPLIANCE

The underlying goal of any compliance program is to improve the target industry or sector by setting standards and enforcing them. Achieving agreement on a standard requires a huge effort, and enforcing the standard is even harder. Problems include setting a mediocre or overly complex standard, and not planning for how to encourage compliant behavior.

The value of any compliance effort will naturally be examined by all participants, who are looking for ways to interpret, improve, and sell the values of the program. This is where most successful businesses engage in order to be one of the early adopters. Achieving early compliance (and sometimes certification) is a distinction with buyers in a competitive field. Also, businesses that are seen as being compliant with the standards in their industry are often seen as industry leaders.

Businesses should think about the future of the programs in their industry. There may be value not only in a better understanding of the compliance effort already underway, but also its next version. Businesses that engage proactively with a compliance program often reap the benefits of involvement in steering committees and work groups tasked with making needed updates to the standards or administration of the program.

# WHAT IS A COMPLIANCE PROGRAM? A SHORT PRIMER

Compliance programs are often driven by a significant trigger, such as credit card fraud, the need to protect personal health information, the need to adopt best practices in information-system security, or individual privacy rights. Many have concluded that without compliance programs, the business world would be a lot more complex and uncertain.

In other words, compliance is needed because of a perceived risk and a recognition that the problem is too complex to assume everyone will do the "right thing." A compliance program starts with a focus on the most severe problem and then expands over time to address larger and larger numbers of participants. Compliance programs regularly reassess and expand their requirements to fit the market and increase their value. Businesses that are aware of the cadence of these changes can be early adopters of changes when it benefits them.

## Definition of Components

Almost all compliance programs have four main components:

**1. Authorities:** There is always an authority behind a compliance program. This could be a government entity or an industry coalition, but it will have some ability to compel the target industry to take it seriously. The authority can also penalize participants, adjudicate disputes, and interpret its own standards to ensure the program is seen as legitimate.

**2. Standards:** The compliance program must have a standard that spells out the rules, objectives, and requirements, and especially in the case of technology, must reflect changes as the industry, technology, or methodology changes.

**3. Assessments:** A compliance program must have a means to assess compliance with standards by entities that adopt the program. Audits and self-assessments are common methods. Following the initial release of standards, assessment guides are published to address how to perform audits, address control requirement interpretation, and issue "certification" of compliance.

**4. Fees:** The authority typically must use fees or fines as a method of enforcement, and sometimes as a means for supporting the compliance program infrastructure.

| Compliance Program | Industry Focus | Authority | Standard | Assessment | Fees | Comments |
|---|---|---|---|---|---|---|
| Information management systems | Any company with information security program | ISO/IEC | ISO/IEC 27001:2013 (latest) | Performed by independent audit firms / trained and certified auditors according to ISO 27002 guideline | › Publications<br>› Third-party audit and certification<br>› No fines or fees paid for non-compliance | Overall well respected – true international standard for management of security program |
| Payment card industry (PCI) | Any merchant or bank that accepts credit cards | PCI Council – made up of all major credit card companies | PCI Data Security Standard (DSS) | Performed by independent audit firms / trained and certified auditors according to PCI DSS guidelines | › Audit<br>› Certification<br>› Fines for merchants between $5,000 and $80,000 a month | Started in 2004 to mixed reviews due to significant fines, and has become a cornerstone security effort for many businesses |
| Statement on Standards for Attestation Engagements (SSAE) 16 &18 | Any type of business engaging with IT/ data-security programs | AICPA | SSAE 16 provides guidance on an auditing method, rather than mandating a specific control set | Performed by independent audit firms / trained and certified auditors | › Audit prior to issuing SOC 2 report<br>› Annual assessment | A popular U.S. standard report, formerly known as SAS70, relied on for security assessment |
| HIPAA – Health Insurance Portability and Accountability Act of 1996 | Any organization or vendor (business associate) that handles health data | U.S. Dept. of Health and Human Resources (HHS) | HIPAA and HITECH security rules | Performed by independent auditor to verify (not certify) compliance | › Audit fees for assessment<br>› Fines up to $1M depending on violation | › Large fines<br>› Expanded to include business associates of health providers |

# MAKING COMPLIANCE WORK FOR YOU

## Top-Line Benefits

Compliance programs have a number of "top-line" benefits that organizations should consider.

1. Better resource management. Meet contracted compliance requirements before signing the contract. This is an obvious but not insignificant benefit for a company. It is not unusual for competitors to stipulate in contracts that they will meet a standard by the time of execution, banking on the procurement cycle and other delays to give them time to meet the requirements. While this is possible, it is also a risk, as organizations typically take 6–9 months to achieve compliance with a significant standard. Companies that do this will likely outperform competitors that are not ready to be assessed for compliance. Avoid the spending required to achieve compliance or certification under contract pressure.

2. Marketing wins. Marketing and sales people should use a successful compliance program (and compliance certification) to help distinguish their company in the eyes of customers and competition, announcing it in newsletters, public relations material, and web pages. Self-congratulation boosts the compliance program's image with customers and gives the company a competitive edge.

   If the compliance program is new, it is not uncommon for the company to be interviewed by the press about the process and the program's goals. Prepare staff to speak about the value of the program and how the company embraces the benefits for consumers or users.

   Additionally, sales staff will readily acknowledge that when a company achieves a strong compliance certification, this often makes the sales process much smoother and sales cycle shorter. Although "supply chain" assessments continue to be common in all industries, many customers rely partly on certified compliance programs in assessing a company. Strong compliance certification saves time and resources.

3. Real security improvement. Take advantage of the security changes required by a security-compliance program. Most compliance programs rely on deploying controls to reduce severe vulnerabilities. Implementing these changes improves the company.

   For instance, a formal continuity program required by a compliance program is a tremendous opportunity to engage with staff, update procedures, and improve risk awareness, procedure effectiveness, and organization security.

   Other compliance requirements, such as incident management, prepare a company for crisis events such as a major security breach or system failure. Companies with a compliance program in place may reduce fines and other repercussions (such as customer backlash and public opinion).

   After an incident or breach, it is not uncommon to hear of compliance infractions or non-compliance with a standard. This is a truly negative repercussion.

4. Improved efficiency and effectiveness of operations. All compliance programs force an organization to document its business and examine and assert that specific efforts are being made to meet the program's goals. This may result in documenting a process that has traditionally been "tribal," or passed down through attrition. When staff members are required to write processes down, this almost always results in some process re-engineering, improved efficiency or effectiveness, and a boost for staff members who feel their documented work efforts are now better understood by management.

   Companies are often surprised at the staff's positive response to a compliance program. This morale boost can help with efforts to improve efficiency and productivity.

## Tactics

To achieve these benefits and others from a compliance program, companies must avoid the common attitude that compliance programs are all a cost and interfere with operations. Here are some suggestions:

1. Scope down to reduce impact. For many organizations, the challenge of the compliance program is the change to operations, and they equate change with the cost of retooling, updating processes, informing management, and the like.

   To lessen the impact of this change, read the compliance program's scope carefully. Most compliance programs have a specific focus, which a company might be able to separate from enterprise systems before the compliance program takes effect.

   For instance, when a compliance program requires that significant new controls be added to the network, there might be justification for changing the program's scope to focus on just a subset of systems in a subnetwork. This would enable the company to become compliant without the higher costs of changes to all operations.

2. Use risk assessment to help manage the compliance project. Most compliance programs assess risk to adjust the priority of control requirements. For instance, a company that does not write software has none of the typical requirements for software development security. Based on the risk assessment, those requirements are removed.

   The compliance risk-assessment process is also a technique for an organization to prioritize compliance program efforts. When starting a compliance effort, review the requirements and do a gap assessment based on the required controls, the actual risks being addressed by those controls, and the program's goals. Requirements that are not applicable can be removed if you can show that you have assessed low risk and company acceptance of that risk. You may also find that controls already in place are sufficient when documented. For the other controls, prioritize tasks to address those based on risk to the company.

This approach will be particularly welcomed by auditors or assessors because it means that the company moving toward reducing high risk. If, during the audit, the company is found deficient, it will more likely be for a low-risk requirement that will be easier to manage and cost less to fix.

3. Use secure and certified vendors to inherit secure processes. Companies exist in an ecosystem of connected relationships to achieve business and sales goals, and it is not surprising that compliance programs address this reality. Because almost all companies use third-party technology vendors (from application services to cloud hosting), the choice of vendors is important for compliance programs.

   To gain maximum value, companies should select vendors that can provide evidence of security controls that are aligned with the company's security requirements. For instance, a FedRAMP verification program using the AWS IaaS platform model can provide an organization with some pre-approved FedRAMP controls. Similarly, your security assessment of a certified vendor may be easier when the vendor can provide you with its certification report. This report may provide you with much more information than you could gather from your own audit of the vendor.

4. Stay informed/get involved. To address concerns or opportunities with a compliance program, companies should consider getting involved with the program authority.

   For instance, companies that are affected by PCI can volunteer to sit on Security Interest Group (SIG) panels, which study technologies and make recommendation to the council to address future requirements. Attending PCI meetings allows a company to talk with others about similar issues.

5. Prioritize the compliance program effort. Analyze for the highest-return compliance programs first. There are often multiple compliance standards for a sector. Clearly, it makes sense to prioritize the options to maximize return on investment.

   One common method is to determine the most common, or de facto standard, and start there. While this method may not select the "best" standard, if most of a company's customers are planning to make it a contract requirement, it is a smart course to pursue.

   Another approach when a company must address multiple compliance programs is to group together those programs that duplicate control requirements. For instance, if a company plans to implement both security- and privacy-compliance programs, it should consider doing the security program first, which will likely address up to 75 percent of the overlapping privacy program requirements.

   Grouping compliance efforts may save time and energy with a compliance assessment as well. Many third-party auditors can audit and assess multiple standards and are well aware of the overlap. Companies can save money by having assessment audits consider the same evidence for overlapping programs.

## CONCLUSION

There are a number of strategic and competitive advantages to addressing a compliance program as an opportunity rather than a burden. Part of the answer is knowledge and attitude. Approaching the compliance program with a good understanding of these benefits will improve company security and possibly sales operations, marketing traction, and the bottom line.

Need CloudCheckr for your organization? Learn more at **www.cloudcheckr.com**.

Cloud Checkr

342 N GOODMAN ST,
ROCHESTER, NY 14607

**1-833-CLDCHCK**

**www.cloudcheckr.com**