

Zero Trust – Compliance

By Chris McDuffie



Our series on Zero Trust Security first discussed the basic security principles every organization should implement. In this second article, we will examine how a Zero Trust security model helps ensure compliance.

Basic Steps for Ensuring Compliance

Implementing a Zero Trust Security model can be daunting, particularly if you also are concerned about compliance. To improve security and compliance, here are four basic steps toward [Zero Trust](#).

Step 1: Do Your Research

The first step is to identify what frameworks and regulations apply to your organization. This could include wide-sweeping legislation such as [GDPR](#), which applies to all organizations that have European customers, or more targeted legislation such as [PCI DSS](#), which applies to organizations that process payments or hold payment card data.

Industry regulatory bodies govern compliance requirements. For example, healthcare organizations need to ensure they are [HIPAA](#)-compliant, while organizations involved in power generation are regulated by [NERC CIP](#).

Various states have also enacted their own regulatory frameworks, such as the [CCPA](#) (California Consumer Privacy Act). By educating yourself about security regulations that apply to your organization, you can ensure that your new Zero Trust Security framework is built with compliance in mind.

Step 2: Create Policies that Promote Security & Compliance

Once you become familiar with all regulations that apply to your organization, you can begin crafting policies to ensure compliance and security. Make sure that your policies identify strategic goals for remote applications, desktops, and any Software-as-a-Service (SaaS) applications your organization uses.

Policies must be clearly codified and communicated with all employees and outside contractors. Even the best, most comprehensive policy is useless if your workers and other users do not understand how they need to conduct themselves.

For your organization to remain compliant, consider establishing and monitoring key risk indicators for compliance objectives. These metrics provide data required to accurately assess policy effectiveness and keep your program on track. This data should be documented in a risk program or risk register, both for security and compliance purposes.

Step 3: Get a Pre-Audit Assessment Done by a Qualified Third Party

Once your policies and procedures are codified and implemented, consider a pre-audit assessment from a qualified third party. Use the audit to identify deficiencies for remediation.

If you choose to conduct an internal audit, make sure your audit includes proper scoping to identify the people, processes, and technology included in the assessment

framework. Your team should also be familiar with the necessary controls and be able to objectively self-assess your environment.

Make sure you are thorough when assessing your control areas. Some areas that are commonly overlooked include:

- Change control
- Access management
- Boundary security
- Vulnerability management
- Configuration management

Step 4: Achieving the Correct Security Certifications

The fourth step involves the process of acquiring the correct security certifications such as PCI-DSS, HIPAA, NERC CIP, or other validations. Many broad verticals such as government, manufacturing, and service sectors set their own requirements around privacy and security, either based on state statutes (like CCPA) or other privacy acts such as GDPR.

Remember, any situation that requires privacy will also typically require underlying security controls.

The process for certification will vary depending on the organization issuing it. If unsure of what steps to take, contact the certifying body directly for more information.

Two security certifications that have been receiving a lot of attention are [SOC 2](#) and the [CMMC](#) (Cybersecurity Maturity Model Certification). SOC 2 applies to service organizations that require an attestation of the management principles the provider is following, including both information security and confidentiality. CMMC applies to organizations that do business with the Department of Defense as either parts suppliers or service suppliers in the Defense Supply Chain.

Regardless of which vertical your organization occupies, where you are based, or where your customers are based, any information your organization stores, processes, or transmits will determine which compliance and certification requirements you require. If you are unsure where to begin, you should seek assistance from a trusted third party with experience in the security and compliance spheres.

Make Zero Trust Security Easier with Structured and Citrix

To help you ensure your policies are adequate and your organization remains compliant, Structured offers governance, risk, and compliance guidance and assessments. We have extensive experience with the [Zero Trust security model](#) and only partner with trusted organizations such as Citrix, which meet our product quality and customer service standards.

Protecting users, apps, and data with end-to-end contextual access, a key component of establishing trust, is made easier with Citrix and its approach to [secure workspace access](#). The company's [virtual apps and desktops](#) provide all users with the same protected experience regardless of what device or operating system they are using.

Citrix Case Study: Financial Institution

Many organizations have chosen to partner with Citrix in their quest to achieve [Zero Trust](#). One client, a financial institution, was concerned about ensuring security while quickly transitioning to a remote workforce:

"As we deployed a huge mobile workforce during the onset of COVID-19, various compliance and regulatory agencies were very concerned that we had the security and capacity to support almost 1500 remote workers. Citrix allowed us to quickly deploy our mobile workforce and maintain security over our critical data. By keeping all of our remote workers' data in the protected Citrix environment, we were able to quickly alleviate all our compliance and regulatory agencies' concerns related to expanding our mobile workforce."

By partnering with Citrix, the financial institution reduced its inventory and its scope, therefore reducing the controls applied to their environment.


Achieving a Zero Trust architecture while ensuring compliance is complicated for even the largest organizations. It can be particularly challenging for mid-size companies and SMBs with few experts on staff. To maintain compliance and safeguard your applications, users, and data, Structured offers a variety of professional and managed services that can be tailored to meet your organization's unique needs.

For more information on Zero Trust Security or to schedule an audit, [please contact us today](#).

Get started with Zero Trust Security

Visit structured.com to start the conversation

 structured.com

 1 (800) 881-0962

 [STRUCTUREDINC](#)

 [STRUCTURED-COMMUNICATION-SYSTEMS](#)