INFRASTRUCTURE COMPLIANCE AUDITS

« PROTECTING YOUR COMPANY »

OPPORTUNITY:

Audits are expensive to a business, demanding both valuable time and hard-earned treasure. Audits are also outside of your company's core competencies and distract from revenue generating activities.

Modern cloud-computing platforms provide customers with more protection than ever before. Set up properly with the right provider, customers "inherit" compliance audit results for that infrastructure, meeting their requirements and eliminating that expensive and time consuming requirement.

WHAT AUDITS ARE REQUIRED?

This is an open-ended question, but the base audits every debt recovery operation should engage to certify their application and database infrastructure are as follows: PCI DSS, SSAE18 (SOC), and Penetration Testing for any internet-connected applications. Beyond that, it usually depends on client requirements and can get into FedRAMP or even IRS 1075.

AUDITING COMMITMENTS

Whether a company attempts to manage audits with their own staff or hires an outside IT firm, there is a great deal of time, energy, and dollars committed to the auditing process. This should look familiar:

1. Map infrastructure
2. Identify existing security protocols
3. Submit audit materials, receive results
4. Address identified deficiencies
5. Resubmit audit with performed fixes in place
6. Pass audit fully or qualified with notations of deficiencies by priority

ROLE OF CLOUD COMPUTING

Economy of scale directly applies in this setting, and customers benefit from not only the web-based software provider's compliance auditing, but the data center's as well.

A data center today is a highly-secure, continually monitored fortress of digital protectionism. Data security and integrity has become the business of the data center and there is no industry better at it. Setting the standard in the industry is Amazon through their AWS cloud computing infrastructure with government-grade security, encryptions, and compliance.

Parking your server at a data center with strong security and compliance does not mean you are in compliance. You are responsible for ensuring that the software and security meet the same auditing requirements.

DO YOUR DUE DILIGENCE

There are three levels of data security and compliance to consider: At the top is the Data Center, next is the Software Provider's platform, and then there is the server leased to your business.

Most web-based software providers, or software vendors that supply off-premises servers you need a secure connection to, are NOT providing the compliance audits for your company's database or application server instances.

CHOOSE WISELY

Every decision in life and business comes down to being fully informed. Collect the right information and strive to understand the material to make educated decisions.

To fully leverage the advantages of a web-based software platform to your company, make sure the software vendor will provide the audits of your server instances so you can concentrate on what you do best—not IT work.

(360) 604-3531

www.InterProse.com

INTERPROSE
RELENTLESS INNOVATION®

203 SE Park Plaza Dr.
Tower II, Suite 190
Vancouver, WA 98684

INFRASTRUCTURE COMPLIANCE AUDITS

« KNOW YOUR ACRONYMS »

Security and Compliance is Filled with Acronyms

There is a reason why IT firms charge so much money to keep your infrastructure up to date with regulatory requirements and safe from bad actors or poor practices. They are paid to stay current on an ocean of regulations.

If you are unfamiliar with any of these terms, it's time to start studying and asking questions. Data security is a complex business, whether you are doing it yourself or paying an IT consultant.

If you are benefiting from the strategies your software provider includes as part of your SaaS subscription, ask for documentation to be sure your company's individual server instances undergo the necessary audits.

GLOSSARY OF ACRONYMS

AES: Advanced Encryption Standard—government encryption standard to secure sensitive electronic information.

AOC: Attestation of Compliance—a declaration of a merchant's adherence to the PCI DSS.

ASV: Approved Scanning Vendor—a company approved by the PCI SSC to conduct vulnerability scanning tests.

BCP: Business Continuity Plan—identifies an organization's exposure to internal and external threats.

CDE: Cardholder Data Environment—any individual, software, system, or process that stores, processes, transmits, or handles cardholder data.

CHD: Cardholder Data—sensitive data found on payment cards, such as account holder name or primary account number (PAN) data.

CVSS: Common Vulnerability Scoring System—standardized method for rating and describing IT vulnerabilities.

DMZ: Demilitarized Zone—neutral zone between a private and public network, providing an additional buffering layer of security, typically where web servers are hosted.

FIM: File Integrity Monitoring—a method to watch for changes in software, systems, and applications in order to detect potential malicious activity.

IDS/IPS: Intrusion Detection System/Intrusion Prevention System—a system used to monitor network traffic and report potential malicious activity.

IRP: Incident Response Plan—policies and procedures to effectively limit the effects of a security breach.

OWASP: Open Web Application Security Project—a non-profit organization focused on software security improvement. Often heard in the context of "OWASP Top 10", a list of top threatening vulnerabilities.

WAF: Web Application Firewalls—specific to HTTP applications to protect servers, sets rules to protect against cross-site scripting (XSS) and SQL injection attacks.

MFA: Multi-Factor Authentication—security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or transaction.

(360) 604-3531

www.InterProse.com

INTERPROSE
RELENTLESS INNOVATION®

203 SE Park Plaza Dr.
Tower II, Suite 190
Vancouver, WA 98684

INFRASTRUCTURE COMPLIANCE AUDITS

« YOUR AUDIT CHECKLIST »

How to Make Your Auditor Happy if You Are Responsible for Your Servers

If an infrastructure audit is done properly, it is a labor intensive process filled with humorless interactions. Auditors are happiest if you are prepared, educated, and able to provide the materials they need to ensure the audit isn't slowed down or complicated.

The security auditor is there to inspect and analyze your systems, methods, tools, and processes. While a SaaS provider can take responsibility for your infrastructure security and compliance requirements if they choose, your processes, location, and methodologies are still your responsibility—**it's just a much shorter (and cheaper!) audit if you don't have to worry about the hardware your software runs on.**

TIPS FOR MAKING YOUR INFRASTRUCTURE AUDITOR HAPPY

1. **Update Your Network Diagram Regularly**—make sure the infrastructure diagram you present to the auditor is an accurate, up-to-date representation of how your software interacts with its application and database servers, complete with reference to compliance statues.
2. **Never Assume You are Compliant**—requirements evolve as the threats change, and typically they just get more onerous. Don't make the mistake of assuming that just because you were compliant last year, you are good to go this year.
3. **Learn About Your Risks and Demonstrate Understanding**—protecting data and mitigating risk to your infrastructure is a big deal, which is why PCI DSS requirements include stipulations that all entities with vulnerable infrastructure perform annual risk assessments. You have to be educated to properly identify and manage security risks. A good policy that goes hand-in-glove with this effort is to perform your own internal audit in preparation for the third-party examination.
4. **Develop a Relationship with Your Auditor**—These professionals work at this year round and they can give you a heads up to any issues that come up after your last audit and prior to your next. Just having some visibility to arcane changes to the regulatory environment a couple of months in advance to an annual audit can make the process much smoother.
5. **Document Everything, and Keep it Current**—if you are documenting your security policies, software and hardware versions, firewall configurations, flow diagrams, personnel roles, etc. yourself already, you know what a challenge it is to keep this material updated and in the correct format. If you are not doing this currently, get started—your auditor is going to ask for your documentation within the first 5 minutes.
6. **Establish a Responsible Party**—every ship needs a captain, so make sure your compliance auditor knows who their main point of contact within your company is and how to interact with them most efficiently.

The alternative is selecting a SaaS provider that supplies all of this information as part of your subscription!

(360) 604-3531

www.InterProse.com

INTERPROSE
RELENTLESS INNOVATION®

203 SE Park Plaza Dr.
Tower II, Suite 190
Vancouver, WA 98684