TECH LOCK®

TECH LOCK Certified

"A multi-regulatory approach that normalizes across all requirements for a holistic assessment".

Prior to beginning a TECH LOCK® Certified assessment, we first review what data elements a company stores, processes, or transmits. Some data elements that we look for include Card holder Data, Protected Health Information, Social Security Numbers, and Federal Tax Information. Upon request, we can also include institution-specific information. For example, certain banks, guarantors, or creditors may want their data included in the scope of a specific type of assessment.

Our TECH LOCK® Certified assessment testing procedures peer deep inside an organization's technical systems and processes. Our assessors are experienced with and certified in many relevant technologies, such as Microsoft and Cisco. We don't just interview staff and then look for documented policies and procedures; we look at the configurations of all relevant information systems and network components to ensure the appropriate policies and procedures are being actively addressed. This goes above and beyond what many single-view audits provide.

For example, the FTC recommends that to comply with the GLBA Safeguards Rule, businesses must use password-activated screen savers to lock employee computers after a period of inactivity. To confirm that this is being followed, our assessors will not just interview the IT Department and review a policy that requires password-protected screen savers; we will also review the actual information systems and network devices to confirm that the policies are used in every day practice.

TECH LOCK Certified Provides Oversight for Organizations with Multi-Regulatory Compliance Needs

Data-centric assessment delivering a full-service package, that evaluates the day to day handling, transmission, and storage of sensitive information.

Expert assessors are deeply-technical and can verify security controls, best practices, and target problems quickly that you may have missed.

Provides validation that your business is diligently protecting customer data and is adhering to the various compliance and regulatory standards that govern your industry.

320 E. Big Beaver Rd., Suite 145 • Troy, MI 48083 info@techlockinc.com 847.245.3727

TECH LOCK®

We map the data elements to relevant data security laws and regulatory standards. Regulatory standards that we look at include PCI DSS, HITRUST, NIST SP800-53, and ISO 27002. Some federal laws that we map data elements include HIPAA, GLBA Safeguards Rule, and FISMA. We also keep track of current and emerging industry and state laws like Massachusetts 201 CMR 17.00, Minnesota Plastic Card Security Act, and Nevada NRS 603A, and California Consumer Privacy Act.

Once we map the data elements to the relevant laws, and regulatory standards, we develop an assessment plan to ensure that our audit covers the handling of information, data flows, and data storage locations. This customized assessment plan delivers several benefits to our clients.

TECH LOCK CERTIFIED BENEFITS

Cost Savings

Since we conduct one audit against all relevant data security laws and regulatory standards, our clients save money because they don't need to pay for multiple audits and certifications. TECH LOCK is one of the only companies in the world that is accredited to conduct PCI DSS and HITRUST assessments at the same time. This means that our client's don't need to first pay a PCI QSA to do a PCI DSS assessment, then a HITRUST CSF Assessor to do a HITRUST Assessment. Annual Review/Update Configuration Standards.

Time Savings

A typical audit may last for several weeks, followed by several more weeks of remediation, and then yet more time for validation of remediation and report writing. Companies that require several such audits every year end up spending a significant amount of time responding to audit requests instead of performing their day-to-day duties. Because TECH LOCK conducts its multi-regulatory audit all at once, our clients experience less overall time under audit and are able to spend more time on contributing to the bottom line.

Increased Trust

Undergoing a multi-regulatory audit means that a holistic view of the security posture is taken. Our audit reports are trusted by our clients and our clients' clients because they do not take a narrow view of specific business processes; they include all relevant business processes by default.

Objective and Standardized

TECH LOCK has developed a standardized set of controls and testing procedures that includes all of the laws and regulatory standards that we audit against. This is opposed to some types of audits (such as a SOC 2 audit) which allows organizations to select which controls would apply, and decide how to in-depth each control should be assessed. This leads to inconsistent audit reports across different organizations. Financial institutions, guarantors, and creditors that utilize many service providers are not well-served by this type of audit. Alternatively, every TECH LOCK® Certified assessment follows the same set of standardized controls and testing procedures, which provides organizations a more consistent view of the security posture of their service providers.

320 E. Big Beaver Rd, Suite 145 • Troy, MI 48083 info@techlockinc.com 847.245.3727