TIP SHEET

Critical Certifications that Protect Your Company's Data

Data breaches (whether accidental or intentional) can be very costly in terms of damage to an organization's reputation, lawsuits and regulatory fines, as well as customer loss. In pursuing what certifications are important, here are the security frameworks that address the unique requirements of each industry.

SOC 2 + HITRUST CSF

For companies working in financial services, the AICPA offers SOC 2 reporting, which assesses a company's security program against five Trust Services Principles. As an added bonus, SOC 2 reporting is widely recognized across multiple industries.

HITRUST certification is a great option for businesses that handle protected health information. The HITRUST Common Security Framework provides a mechanism for companies to address rigorous HIPAA standards. HITRUST CSF is also mapped to several other security frameworks, like NIST, PCI, CIS and GDPR.

Some security frameworks allow businesses to address multiple security requirements using a single certification. The HITRUST Common Security Framework is a great example of this "assess once, report many" approach to certification. For example, the HITRUST Alliance has partnered with the AICPA, which oversees SOC 2 attestations, to offer a joint reporting process that allows businesses to use the HITRUST CSF and CSF Assurance programs for SOC 2 reporting.

PAYMENT CARD INDUSTRY (PCI DSS 3.2) & PENETRATION TESTING

Companies that accept credit card payments should maintain PCI certification. Overseen by the Payment Card Industry Security Standards Council (PCI SSC), PCI certification requires businesses to meet stringent requirements, including change management processes, continuous monitoring and maintaining seven critical security controls throughout the year.

FEDERAL INFORMATION SECURITY ACT (FISMA) COMPLIANCE

The Federal Information Security Management Act (FISMA) is a United States federal law that made it a requirement for federal agencies and contractors to develop, document, and implement an information security and protection program. Requirements include maintaining an up-to-date system inventory, data categorization, selection and implementation of NIST security controls, development of a System Security Plan, continuous monitoring and conducting annual risk assessments.

ADDITIONAL COMPLIANCE SAFEGUARDS

HIPAA — Health Insurance Portability and Accountability Act

HITECH — Health Information Technology for Economic and Clinical Health

FACT Act — Fair and Accurate Credit Transaction Act

NIST — National Institute of Standards and Technology 800-53 Controls

IRS 1075 Safeguards

Maintaining multiple certifications ensures that the service provider you choose engages in a process of continuous improvement and address any gaps in their security programs. At DATAMATX, we take protecting our clients' data as a top priority. Our successful completion of SOC 2 and HITRUST CSF, along with our compliance with FISMA NIST 800-53, PCI-DSS and SSAE18, allows our clients to have complete trust that their data is appropriately and effectively safeguarded within our facility at all times.

Let's Talk!
Call 800-943-5240
www.datamatx.com

FROM DOCUMENT DESIGN TO SECURE DELIVERY

DATAMATX