Trust but Verify: Enabling Digital Trust Through Compliance

WHAT IS DIGITAL TRUST AND WHY IS IT IMPORTANT

Digital trust is an ever-evolving concept that has rapidly gained widespread traction due to the increased prevalence of cybersecurity incidents and a heightened public awareness of security and privacy issues. Because of the increase in cybersecurity incidents, there is a growing consensus in the market that digital trust is a fundamental prerequisite for stakeholders to do business with almost any organization. Digital trust refers to the confidence consumers have in the security, privacy, reliability, and integrity practices of companies and in the digital products and services they build or operate.

Many research studies from leading organizations have indicated that companies that fail to examine how well they manage digital trust are more likely to be susceptible to increased cybersecurity incidents and privacy breaches as well as potential lost revenue. Read on to learn what types of reports companies should considered to establish and maintain digital trust in the marketplace.

DIGITAL TRUST AND THE ROLE OF COMPLIANCE

Organizations must measure digital trust to understand and demonstrate a commitment to maintain and continually improve their cybersecurity posture. Though there are many ways for an organization to measure digital trust, **ISACA's State of Digital Trust Survey 2022** has shown that an independent third-party assessment is the most impactful and preferred way to demonstrate an organization's commitment towards digital trust and thereby has the potential to increase stakeholder confidence.

Companies are constantly striving to build differentiated products and offer niche services to solve key problems faced by businesses and consumers alike. In addition to the unique details of the features or functionalities provided; customers, investors and prospects care equally about the security of the offering and increasingly focus on the ability to safeguard data collected, stored, and/or processed. One of the most effective options for companies to allay these concerns and affirm that the offering is built, operated, and managed in a secure manner (and reasonably protects customer data) is to obtain a third-party attestation report issued by an independent entity.

Why? Because it is independent, objective, and based on an industry-standard, authoritative framework.

COMPLIANCE REPORTS - A SUITE OF OPTIONS

While there are a plethora of security and compliance frameworks and standards available in the market for companies to consider, the choice ultimately depends on the needs and expectations of the customers and users alike. Typically, the requirements of the industry and geographies in which the company does business are key factors in determining the minimum set of standards it needs to work towards.

SOC 2: Offers flexibility with structure

The AICPA's SOC 2 attestation standard is widely recognized and accepted across North America and a de facto requirement in this region for companies to prove their security credentials. This is a great starting point that offers flexibility yet important structure and allows companies to build a tailored controls framework to meet the various SOC 2 criteria. Additionally, through a SOC 2 Plus report, an entity has the option to demonstrate compliance with other relevant frameworks (e.g. HIPAA, CSA STAR, HITRUST CSF, etc.) and/or include informational control mappings. Overall, SOC 2 helps examine and demonstrate the robustness of the foundational control environment. SOC 2 is continually evolving and requires companies to pay close attention to critical areas such as vendor risk management and incident management, among other areas. The result is a comprehensive report demonstrating the company's commitment to a well-managed internal control environment.

ISO27001: Holistic and highly structured standard

The ISO 27001 Information Security Management System (ISMS) standard has been an immensely popular and widely sought-after global standard for information security. This has been the preferred certification for companies to showcase the implementation of an information security management system to achieve its security objectives. ISO 27001 is an overarching framework that covers a gamut of information security areas including management commitment to governance, planning, risk management, management review, internal audit and a range of technical controls. Companies that have obtained this certification have demonstrated a commitment to implement a solid security and compliance environment including a set of documented policies and technical controls.

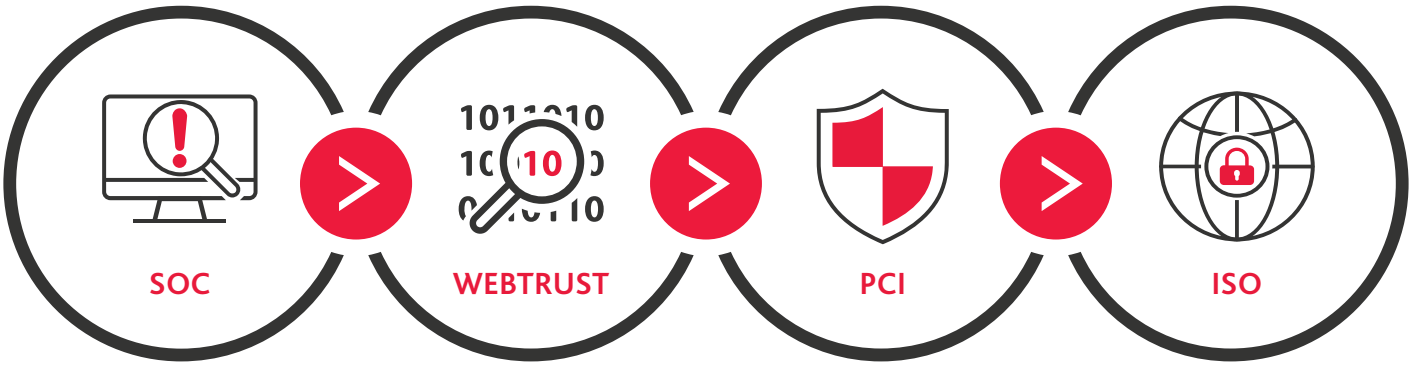
Industry & Geography specific requirements

Large multinational companies that have a significant presence or customer base in different countries are often required to comply with multiple statutory and regulatory requirements depending on industry and region they operate in. For instance, healthcare companies and their business associates that create, store, process or transact with personal health information are required to comply with the HITRUST Common Security Framework to demonstrate they have adequate safeguards in place (as mandated by HIPAA and other security frameworks) to protect the healthcare data. Additionally, companies working with automobile manufacturers in Germany may need to comply with TISAX, which is similar to ISO 27001.

Companies that provide services in the cloud may need to consider region specific regulations. For example, the Cloud Computing Compliance Controls Catalog (C5) created by German Federal Office for Information Security (BSI) is a standard that provides a baseline of security controls for cloud services. This is a mandatory requirement for organizations providing cloud services to government agencies in Germany. The Information System Security Management and Assessment Program (ISMAP) is another example. The Japanese government administers this cloud services assessment program. ISMAP is based on JIS Q (ISO/IEC) 27001 and 27002 on information security and JIS Q (ISO/IEC) 27017 on information security for cloud services.

BDO'S UNIFIED APPROACH TO COMPLIANCE

Recognizing the evolving needs of the market, BDO is uniquely able to provide multiple compliance services in a fully integrated manner with a 'test once and apply many' approach wherever possible. As a result, companies can benefit from a single, highly qualified partner, which may provide meaningful efficiencies, including time and cost savings, and reduced burden on personnel.



CONCLUSION

Long gone are the times when obtaining a security and compliance attestation like a SOC 2 report or ISO 27001 certification was a luxury associated with only large companies or heavily funded start-ups to be used to further their marketing initiatives. In today's world, fraught with new and unknown cybersecurity risks, a security and compliance attestation is a minimum expectation to stay relevant and operate. The ability to demonstrate digital trust consistently and effectively will be the key driver for businesses to thrive.

If you would like to start a conversation about digital trust or explore the types of reports that would benefit your company's needs, BDO is here to help. Our Third-Party Attestation Practice team is dedicated to providing high quality third-party attestation services to meet our clients' unique needs, allowing us to deliver them in the most efficient and cost-effective way possible.

HAVE QUESTIONS OR WANT TO LEARN MORE?

CONTACT US!