FORWARD THINKING IT SOLUTIONS

ACHIEVING PCI COMPLIANCE

Comply with the security requirements of the Payment Card Industry.

ergonomics

ACHIEVING PCI COMPLIANCE

Payment Card Security is Critical for the Economy

A considerable portion of the economy and particularly the retail sector is strongly dependent on the availability of debit and credit card payments. Thus, it is of utmost importance that the local and the international card payment systems remain reliable and secure. Due to the widespread use of payment cards, the related IT systems are attractive targets for cyber criminals. Implementing and maintaining an adequate level of security on the technical and organizational level is a basic requirement for all organizations involved in handling payment card data.

Payment card data is an attractive target for criminals. Attacks via the Internet or data misuse by employees have grown significantly over the past years.

What is the benefit of PCI?

As one of the results, the major card brands – Visa, MasterCard, JCB, Diners Club and Discover – have launched the Payment Card Industry Security Standards Council (PCI SSC) as a standards setting body. This organization issued the IT security standard PCI DSS (Data Security Standard) to improve the card payment security and to better protect consumers, merchants, and the card brands.

PCI DSS is the global security standard for all organizations that handle payment card or card holder data. The PCI DSS requirements apply to all participants in the card payment world, such as merchants, payment service providers (PSP), acquirers, issuers, data storage entities (DSE) and third parties, if they transmit, process or store card holder data.

Why Ergonomics?

Ergonomics is the Swiss IT security specialist for everything PCI DSS. Our certified security consultants offer advisory and audit services to achieve and maintain PCI DSS compliance. We work with partner organizations for the required vulnerability scans and penetration tests. Therefore, Ergonomics – as a certified QSA Company – is your one-stop services provider for all PCI DSS tasks.

PCI Compliance in a Few Steps

The PCI DSS requirements appear to be a rule set that is complex and difficult to grasp. With over 280 individual security measures, approaching compliance requires some preparatory work.

Many of the requirements of PCI DSS are Best Practices of IT security measures, and are also mandated by other security regulations, such as ISO 27XXX, BSI Schutzhandbuch, HIPAA, or SOX. The main difference to other standards is that PCI DSS is particularly focused on protecting the sensitive card holder data.

ACHIEVING PCI COMPLIANCE

The PCI DSS documentation and validation requirements for merchants and service providers are dependent on their transaction volume, but the technical and organizational requirements remain the same. One of the first steps in an assessment is to identify and to verify the relevant documentation and validation category of the customer.

A typical PCI DSS assessment includes the following steps:

- Create awareness and management support. We run workshops to present an overview and the primary requirements of PCI DSS to the senior and mid-level management.
- Reduction of the PCI scope. An initial assessment identifies the system components that may be in the PCI scope and tries to identify measures to reduce the scope, if requested by the customer. Some of the measures may require that operational processes be adjusted.
- For the in-scope system components, the gaps are identified and remedied together with the specialists of the customer. Existing documentation is reviewed and supplemented. Ergonomics' specialists are able to help with implementing the required modifications.
- Quarterly network scans and periodic penetration tests are set-up.
- The customer completes the appropriate self assessment questionnaire (SAQ) or an on-site audit is performed.
- PCI DSS requires an annual recertification. Therefore, processes need to be established to maintain the IT security level. Maintaining the PCI requirements should become business as usual (BAU).

Certified Competence

With over 24 years experience in the areas of IT security and electronic payment systems, Ergonomics is uniquely qualified to assist organizations to reach PCI DSS compliance. We not only identify gaps, but also actively assist our customers with remedying them. For many of the issues, we also present and offer solutions from our suppliers.

For network scans and penetration tests, we work closely with trustworthy partner organizations.

Ergonomics AG is a certified QSA Company (QSAC) and is authorized to perform PCI DSS assessments, based on the guidelines of the PCI Security Standards Council. Our specialists are at your disposal for an initial discussion.

ACHIEVING PCI COMPLIANCE

FORWARD THINKING IT SOLUTIONS

Ergonomics AG, headquartered in Zurich and with an office in Bern was founded in 1991 by the current owners. Right from the beginning, the company's aims were to satisfy and delight customers with the highest demands. Competence, experience, innovation and responsible actions are the fundamental values on which the company is built – and success has proven us right.

Ergonomics, a leading consulting company in areas of integrated security, can support you in recognizing and resolving enterprise wide IT risks, dangers, and weak spots. Over the years, Ergonomics security consultants have gained immense knowhow – valuable in tackling the most challenging organizational and technical IT security issues.

Please find additional information at:
www.ergonomics.ch

Ergonomics AG » Nordstrasse 15 » CH-8006 Zurich
Ergonomics AG » Zeughausgasse 18 » CH-3011 Bern
+41 58 311 10 00 » info@ergonomics.ch » www.ergonomics.ch

ergonomics