Regulatory requirements from the latest IT Security Act

How companies can actively prevent IT security issues

Holger Schellhaas, Ulrich Kolberg, Norbert Fuchs

The German IT Security Act ("Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" or „IT-Sicherheitsgesetz") came into force on July 25th, 2015. This law provides specific regulations for minimum standards for IT security as well as duties to report security incidents for operators of so-called "critical infrastructures". These are institutions with particular importance for the proper working of the public, e.g. from the energy, healthcare, water supply, telecommunication, finance or insurance sectors.

These companies are required to report cyber-attacks on their systems instantly to the Federal Agency for Information Security (BSI, Bundesamt für Sicherheit in der Informationstechnik) and to comply with minimum standards for IT security as defined by the BSI. In total about 2000 companies are required to report cyber-attacks. The BSI analyses the received information, consolidates them to an overview of the situation and alerts other companies if required. Noncompliance can be fined up to 100.000 Euro.

Nothing new for financial institutions, already being obliged by the Federal Financial Supervisory Authority (BaFin, Bundesanstalt für Finanzdienstleistungsaufsicht) to implement a working IT security management ensuring the security of their IT processes and systems. Insurances within the EU are forced to meet **Solvency II** since 2013, implementing minimum requirements for risk management especially for operational risks. The regulation **MaRisk** (Minimum Requirements for Risk Management, Mindestanforderungen für das Risikomanagement) of the BaFin includes specific protection categories for IT security and refers to the established standards, namely the **ISO 27001** and the **IT Baseline Security** (IT-Grundschutz) of the BSI.

What does this mean for companies?

Why shall a company aim to improve its IT security system or even strive for a certification? In many cases this is not due to own motivation but to expectations of business partners or regulatory authorities, to binding definitions in tenders or to requirements for evaluating credit rating or insurance risks. Most companies which are bound by the new IT Security Act are evaluating their IT systems and are improving it if required. These companies are acting proactively and are preventing critical situations to the best of their knowledge and belief by managing their IT risks adequately. This approach is also deemed reasonable by the legislator; he recommends specifically to follow the international standard ISO 27001 in the 2013 version. This ISO norm claims to cover all aspects of IT security and to reach the stipulated minimum standard by taking the proposed actions.

Our experiences with customers confirm that intelligent implementation of established standards directly leads to minimization of risks in business processes. For example, together with the TCI-partner SSP Europe we are conducting an IT compliance transformation project at a mid-size insurance company, a subsidiary of the Italian Generali group. We are supporting a well-known savings banking group to implement compliance goals according to MaRisk and at the same time to meet the IT quality goals and IT requirements of the clients. Target is to actively support the executives achieving the certification readiness according to ISO 27001 based on the BSI IT Baseline Security. Both projects have not only been initiated by the executive boards but also actively supported, which has proven to be a major success factor.

The frequently uttered opinion that compliance with regulations or ISO standards would not yield security but would just mean to fulfil rules set by organisations, banks or the regulator has not been confirmed. Quite the contrary is true: The step-by-step establishment of comprehensible rules and of a security mind set of the employees is today one of the most important actions and the most powerful protection against the varied threats.

Additionally, this boosts the company image: E.g., the NÜRNBERGER life insurance does good and talks about it – they have again earned the IT security certificate according to ISO 27001 based on the BSI IT Baseline Security. With this both goals of NÜRNBERGER are supported: Scope and level of IT security measures are guided by business requirements, and they also adhere to relevant laws, regulations and guidelines.

Our approach for implementation

Image, business success and stability of the company are vitally dependent on qualified management systems and processes for IT security. What is the most specific and easiest approach for coping with these challenges? To shape the awareness for IT security, to transform IT operations from “Hey Joe”-action into managed procedures and to raise the IT infrastructure to the appropriate level – all this cautiously, step-by-step and with sound judgement, to integrate all actions in the day-to-day business and the awareness of all participants.

Standards are outstanding guidelines for this: ISO 27011 tells what to do, BSI Baseline IT Security tells how to do it and specifies this in more detail. In both cases we are designing and implementing a management system step-by-step, together with our clients, by following well-tested modules which have proven their effectiveness and efficiency for many years:

1. **Setup of the IT security management system**

   Together with the heads of the organisation, the risk management and the IT the scope is focused on the critical core processes.

2. **Participation of top management**

   The evaluation of critical core processes is the entry point to the active participation of the top management. Subsequently, company-wide guidelines and Standard Operating Procedures (SOPs) for the management of IT security are developed and approved.

3. **Evaluation of essential building blocks with the Health Check IT Security**

   The Health Check IT Security is a fast and cost effective alternative to complex analyses. It is a qualified tool to assess maturity levels or readiness for alignment to standards, and to design the appropriate measures.

4. **Actions to reach the stipulated minimum standard**

   Results of Heath Checks often show that the technical realization is not as poor as expected in the beginning. But documents and evidences for business risk provisioning are lacking, operational manuals are inconsistent, installations are not standardised, operational procedures are unclear. ISO and BSI standards can help to clean up: Suitable rules are implemented, documentation is optimised, and everything irrelevant or non-value-adding is eliminated.

5. **Raising awareness of managers and employees**

   To raise awareness of managers and employees in the IT and business departments we are developing awareness programs, trainings and campaigns, and are conducting them ourselves upon client request.

Summary

TCI supports financial institutions, telecommunications companies and energy providers since many years and knows their specific requirements. As no company equals another, the implementation of the regulations of the IT Security Act requires an overall and strategic view and approach for IT compliance. The new IT Security Act shows that transparency provides an important contribution to performance improvements.

In our projects around IT security topics we have proven that not only the ISO 27001 standard but also the more sophisticated procedures according to BSI IT Baseline Security are suitable methods to gradually reach an appropriate level of security. This is also true for small companies. Organisational efforts are minimised to impact the daily routines as little as possible. This is transformation at its best: Compliance pays off!