alliuris

ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS

IT-Security with BSI Basic Protection

Eduardo Isaac Soto Barrera, Lawyer (Mexico) Mag. iur. (Mx), Mag. iur. (D), Hanover

July 2021

For managing directors, a lack of IT security can constitute a significant liability risk: Compromised IT or the loss of data at least lead to business disruptions, but often also to the loss of crucial business information and, in some cases, to the collapse of the company as a result.

In the process, companies make typical mistakes that endanger their security. Missing backups, missing updates for viruses, incorrect documentation of administrator passwords and internal attacks are just a few examples from the field of information security.

For this reason, the Federal Office for Information Security (BSI) has been offering methods and certification according to BSI-Compendium since 2006, based on the norm ISO 27001 and as an implementation of standards 200-1 (procedure) and 200-3 (risk analysis). The BSI Basic Protection Compendium provides a comprehensive catalogue of concrete measures for specific risks on more than 800 pages (without parallel standards).

The ISO 27001 standard on IT security

The *IT-Grundschutz-Compendium* is developed for authorities, service providers, companies, and other institutions. A corresponding certification is carried out by an external auditor certified by the BSI. The programme comprises two areas:

Process modules

The process modules concern the entire IT system or parts of it and include

ORP Organisation and personnel:
Awareness raising and training on infor mation security, compliance management.

CON Conception and procedure:
Encryption concepts, data protection, data protection concepts, deletion and destruction of data, information exchange and data security issues

OPS Operations:
Internal and external operational aspects of the organisation, including third parties, e.g., malware protection and outsourcing for clients, teleworking, cloud usage,

ISMS Information security management system

DER Detection and response:
Security incident response, emergency management

System modules

System modules address individual objects or customisable groups.

APP Applications:
General rules on E-Mail client and Server, office products, Web Server, and Relational database systems

SYS IT systems:
Security issues of end devices such as smartphones and tablets as well as printers, copiers and multifunction devices, also system-specific aspects of servers and desktop systems.

IND Industrial IT:
Process control and automation technology, general ICS component and programmable logic controller (PLC), machines.

NET Networks and communication:
Network management, the correct implementation of firewalls, the use of in-house WLAN, VPN, VoIP, fax machines and fax servers, all in communication and not only on central IT systems.

INF Infrastructure:
Buildings, data centre, server rooms, office and mobile workstations, meeting, event and training rooms, vehicles, general vehicle.

BSI Standards

The following standards are used for effective application of the IT-Grundschutz Compendium:

BSI-200-1: Determines how an ISMS is to be structured. It is addressed to those responsible for information security, security experts, security officers, etc.

BSI-200-2: Builds on the initiation or completion of an ISMS and describes the different types of security: standard, basic and core, including their scopes.

BSI- 200-3: refers to the risk analysis with the creation of a risk overview, risk assessment, risk treatment, etc.

BSI-200-4: Aims at the development of the so-called "Business Continuity Model" (BCM). It is aimed at BCM officers, crisis team members, security managers and others in charge of managing emergencies and crises of technical and non-technical origin.

Risk assessment~~classification~~

For an accurate problem diagnosis, the company must correctly assess its risks. This is done by using a methodology to assess the threats, potential damage, frequency of occurrence and the resulting risks.

Risk classification

The risk classification records the probability of occurrence of risk events

▪ Rare:	every five years
▪ Medium:	every five to once a year
▪ Frequently:	once a year to once a month
▪ Very frequent:	several times a month

Another risk parameter is the potential amount of damage, classified as:

- Negligible
- Moderate
- Considerable
- Existence-threatening

The parameters probability of occurrence and magnitude of damage are combined to classify the risk in the result.

In this context, certain risks are not compatible with certain principles, e.g., availability (fire, natural disasters, destruction of equipment or data carriers, personnel failure, sabotage, loss of data, etc.), integrity (manipulation of information, loss of integrity of information worthy of protection, etc.), confidentiality (spying on information/espionage, wiretapping, misuse of personal data, etc.) or a mixture of one or more of these principles.

Risk treatment

After identifying and classifying a risk, the question of risk treatment arises through

- Prevention (finding the cause),
- Reduction (change of circumstances),
- Relocation (outsourcing, insurance)
- Acceptance (positioning in the market)

The management must document and monitor its decision.

Types of procedure

With the Guideline 200-2, the BSI offers a range of three types of procedure, which are suitable in different respects depending on the size of the company:

Basic assurance

In analogy to the BSI minimum standards, basic assurance analyses all processes relevant to the company across the board, but also all "assets" (everything of value to the company) in case they are damaged or destroyed. This analysis also includes security risks, if they do not pose an existential risk to the company.
This method is an entry point for small companies and can also be carried out by non-specialist personnel.

The fields of action in Basic Assurance are not a closed cycle, but an entry-level approach.

Core Assurance

Core assurance is essentially the equivalent to Basic Assurance but offers the option of an ISO 27001 certification.

Standard assurance

This level also offers a certification and covers the ISMS. Standard assurance is a closed cycle. It should be implemented in all departments of the company, as each has its own characteristics, and the procedures need to be individualised.

In practice, security concepts (core assurance) are created for small areas "with particularly vulnerable assets", while for the other areas only the minimum standards are implemented to ensure "basic assurance". It is important to consider all technical and organisational aspects.

These are of great importance to determine responsibilities and responsible persons - considering the information itself, the specific tasks and affected processes.

BSI-200-4: Protection of business processes

This standard replaces the previous BIS 100-4 and is relatively new (January 2021). It is designed for companies to protect the availability of business processes or specialist tasks to protect the company financially from existential risks.

These processes are important for functioning supply chains and services of third parties, e.g., service providers, suppliers, and vendors.

Risks are increasingly posed by cyber-attacks, especially ransomware attacks, and extreme natural events. Most incidents are not covered by appropriate property and cyber insurance.

General organisational structure (AAO)

The AAO is the permanent organisational form for the tasks of daily business operations. Responsibilities, hierarchical structure and communication and decision-making channels must be defined.

Special organisational structure (BAO)

In the event of serious restrictions, interruptions or breakdowns in business operations, the company can set up a BAO as a temporary form of organisation and thus react appropriately and quickly to extraordinary situations. The BAO comprises three levels with Reactive-BCMS, Build-up-BCMS and Standard-BCMS.

Companies need to protect against massive disruptive events through prevention or appropriate response after a failure.

Disruption is a situation where processes or resources are not available as intended. It is remedied by the AAO.

Emergency is an actual or imminent interruption of business operations that affects at least one time-critical business process and cannot be remedied in normal operations within the maximum tolerable downtime. An emergency is handled by the BAO.

Crisis is a situation in which there are massive consequences for the company and which the BAO can no longer handle on its own.

These three scenarios can occur gradually or suddenly, so that risk management must always have the possibility of an escalation in hand and include it in its strategies and procedures.

+++

ALLIURIS

The ALLIURIS GROUP consists of 20 law firms and 400 business lawyers within Europe, Asia and America. (www.alliuris.law).

Your contact:
Alisha Daley-Stehr,
Alliuris Communication

info@alliuris.org
Fon 0049-511-307 56-0
Fax 0049-511-307 56-10

IMPRINT

EDITORS

ALLIURIS A.S.B.L.
ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS
BRUSSELS

MANAGEMENT
Luisenstr. 5, D-30159 Hannover
Fon +49-511-307 56-50 505056-20 Fax +49-511-307 56-60

BRUSSELS · PARIS · LONDON · AMSTERDAM · AMERSFOORT . LUXEMBURG · LYON · MADRID · BARCELONA · LISBON · MILAN · COPENHAGEN · HANOVER · ZUG · VIENNA · MOSCOW · MINSK · ATHENS · ISTANBUL · BEIJING · SHANGHAI ·GUANGZHOU NEW DELHI · NEW YORK · MEXICO CITY · SAO PAULO · RIO DE JANEIRO · BRASILIA BUENOS AIRES

EDITORIAL DEPARTMENT
Ulrich Herfurth, Rechtsanwalt

All information is correct to the best of our knowledge; liability is limited to intent or gross negligence. Reproduction, even in excerpts, requires the permission of the editors.