Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence,
Civil Protection and Sport DDPS

National Cyber Security Centre NCSCS

Version 1.0

Guidelines for protection needs assessment

of 14 October 2024

1 Introduction

These guidelines are intended for companies and authorities that wish to implement the Federal Administration's security procedure. The blue text is particularly relevant for federal administrative units and other organisations that are subject to the Information Security Act (ISA) or the Information Security Ordinance (ISO).

In accordance with Article 16 paragraph 1 ISA, the authorities concerned must define a security procedure for the use of IT resources that includes an assessment of the protection needs in accordance with Article 16 paragraph 2 letter a ISA. These guidelines describe a procedure for determining the protection needs of (possibly aggregated) IT objects of protection before they are put into operation. This procedure is known as a 'protection needs assessment'.

To do so, the IT infrastructure concerned must first be divided into a number of IT objects of protection. An IT object of protection can and will consist of various IT resources, including hardware and software components, as well as the data stored, processed and transmitted by them, all of which serve a common and defined purpose and therefore logically belong together (e.g. a specialised application for handling a specific business process). IT objects of protection that provide their services to other such objects are considered platforms. Examples include eIAM, virtualised server infrastructures and software as a service (SaaS) offerings.

Normally, an IT object of protection does not simply consist of information, because it would not be useful to carry out a separate protection needs assessment for each type of document.

In principle, the Federal Administration's security procedure requires to assess the protection needs of each IT object of protection. When assessing the need for protection, only the potential implications of a compromise are taken into account. The threat that may lead to this compromise is not considered.[1] The protection needs assessment thus assesses whether there is a risk that needs to be reduced.

The need for protection of information is categorised as increased or not increased for each security objective (confidentiality, integrity, availability, accountability and data protection). In addition to the need for protection, the security levels according to Article 17 ISA are also identified. This is intended to simplify the subsequent selection of controls.

[1] For example, it is irrelevant whether a data loss is due to a missing backup, a hacker attack or a malicious employee (in all cases, the data is lost).

2 Procedure for assessing the need for protection

The procedure described below[2] can be used to identify the need for protection and the security level of an IT object of protection. The procedure comprises two steps: In step 1, the IT object of protection is specified and an information inventory is created; in step 2, the potential implications of a violation of the security objectives (confidentiality, availability, integrity, accountability and data protection[3]) are assessed.

Step 1

The IT object of protection and its technical design must be described in as much detail as possible. It is recommended that the following information be included, although this information can be added at any time, even later:

a) Aim and objectives of the IT objects of protection, specifying the business processes and identifiers[4] concerned;

b) end-users and service providers involved (if known), as well as persons with specific roles (e.g. ITSOO, persons responsible for the object of protection, project managers, etc.);

c) Technical configuration (including development environment and any platform services used) with architectural sketches that are as precise as possible, in particular regarding the network integration;

d) access rights (for persons, groups, roles and processes);

e) any existing territorial conditions (e.g. in which countries information is stored and from where it is accessed).

An information inventory must be created that contains all the information that is either generated, stored, processed and/or transmitted by the IT object of protection or required for its provisioning. The information should be grouped in a meaningful way. The following information must be provided and documented for each such information group:

a) Description of the information group;

b) any existing and/or required classifications in accordance with Articles 18, 19 and 20 ISO[5];

c) indication of whether an information group also contains personal data and, if so, what kind of personal data.

Step 2

The implications of a compromise of the IT object of protection must be clarified for each information group identified in step 1. This requires answering the four questions below:

a) What would happen if the information were disclosed or intercepted by intelligence

---

[2] The procedure is inspired by Mozilla's Rapid Risk Assessment (https://infosec.mozilla.org/guidelines/risk/rapid_risk_assessment).

[3] https://www.bj.admin.ch/bj/de/home/staat/datenschutz/info-bundesbehoerden.html (web page available in German, French and Italian).

[4] e.g. project name, project no / ID, etc.

[5] For information classified as 'internal', 'confidential' or 'secret', the group of authorised persons should also be indicated. This is important for identifying risks and later for selecting appropriate controls.

services or similar organisations[6]? (violation of confidentiality)

b) What would happen if the information were unavailable for an extended period of time? (violation of availability)

c) What would happen if the information were to be modified without authorisation? (violation of integrity)

d) What would happen if it were not entirely clear who modified information after it was originally entered? (violation of accountability)

To assess the protection needs of the information, you need to verify for each information group whether

a) the identified impact could result in compromised information security or financial loss based on the criteria in Article 28 ISO;

b) acts and ordinances (e.g. the Therapeutic Products Act, company secrets, etc.) applicable to these information justify or require increased protection;

c) the data protection officer concludes that there is a high risk of violating the fundamental rights of the data subjects in terms of Article 22 paragraph 1 FADP[7];

d) the impacts are unacceptable for the organisation[8].

3 Results of the protection needs assessment

The procedure outlined in Chapter 2 provides a summary of the information groups and potential impacts that are relevant to the IT object of protection, with the potential implications being identified and evaluated according to the security objectives (i.e. confidentiality, integrity, availability, accountability and data protection).

The security level (of an IT object of protection) in accordance with Article 17 ISA is assessed on the basis of the following criteria:

a) the ‘basic protection’ level applies if the IT object of protection does not need to be classified any higher;

b) the ‘high protection’ level applies if a significant compromise in accordance with Article 28 paragraph 1 ISO is identified or if information classified as ‘confidential’ is processed;

c) the ‘very high protection’ level if a significant compromise in accordance with Article 28 paragraph 2 ISO is identified or if information classified as ‘secret’ is processed.

The IT object of protections are inventoried as assets.

The protection needs analysis must be reviewed by the IT security officer of the organisational unit (ITSOO). The review includes checking whether the potential compromise is plausible and whether the assessment is comprehensible and justified. This may require the involvement of other units. If personal data are affected, the data protection officer should be involved. In the context of projects and business processes, it makes sense for the protection needs assessment to be approved by the clients and those responsible for the business processes.

---

[6] For classified information, you can use the classification catalogue to help you answer the question.

[7] There is a risk assessment tool of the Federal Office of Justice that should be used within the Federal Administration to carry out preliminary risk assessments.

[8] If this is the case, the organisation should carry out a business impact analysis and define relevant criteria for its business processes.

4 Next steps in the security procedure

The protection needs assessment evaluates whether there could be a risk that needs to be reduced. When there is no need for increased protection, there are no extraordinary risks for the organisation. The minimum requirements for IT security are covered by baseline requirements (IT-Grundschutz (Si001)), which must be provided for every IT object of protection.

When an increased need for protection is identified, the potential compromises must be reduced to an acceptable level using appropriate technical and organisational controls. In addition, the directives for an increased need for protection (P042) must be implemented in accordance with an ISDP concept. The interplay of the protection needs analysis, the baseline requirements and the process for increased protection needs is illustrated schematically in Figure 1.

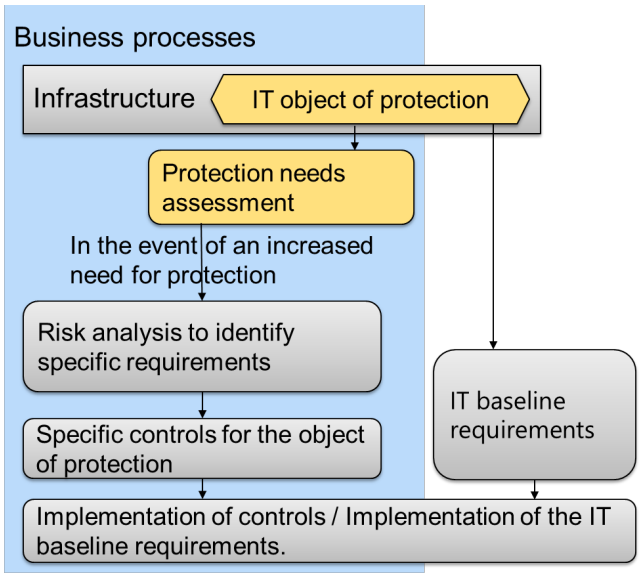

Figure 1: Protection needs assessment as part of the security procedure

If confidential or secret classified information has to be disclosed to external companies, or if external companies are to be involved in the development, administration, operation, maintenance or review of an IT object of protection with a 'high protection' or 'very high protection' security level, an industrial security procedure in accordance with the ISPO must be initiated.

If personal data is processed with the IT object of protection, it may also be necessary to create a record of processing activities in accordance with Article 12 FADP and processing regulations in accordance with Article 6 DPO (for federal bodies) or Article 5 DPO (for private individuals).

A protection needs assessment is a delivery object in projects, and part of the documentation for each IT object of protection. A project can contain several IT objects of protection, so there can be more than one protection needs assessment in each project. The first version of the protection needs assessment must be completed early in the project. However, it should be continued for the documentation and must be kept up to date.