ISKE – Three-level baseline IT security system

Mihhail Karagjaur Oliver Erlich Taaniel Kraavi

Vjacheslav Rukavishnikov

Abstract

The Estonian Three-level IT Baseline Security System ISKE is a security standard with the goal of ensuring sufficient security levels for data processed in IT systems, based on a required security level. We will first give a high-level summary of what ISKE is and then explore how it came to be as well as explore more deeply the concepts that make up the standard. We will also discuss and simplify the requirements it sets out and explore its practical use in Estonia.

Keywords: ISKE, Information systems security, IT-Grundschutz

1 Introduction

ISKE is a three-level baseline security system[1] for IT systems. Its purpose of application is achieving and maintaining the security of information systems and assets in a required and strictly defined minimal extent. A three-level baseline system means three different sets of security measures depending on the particular security requirements.

ISKE mainly caters to the Estonian government's and other official bodies' IT systems' security needs in safeguarding their data, but it is also meant to be usable by businesses and other organisations wishing to secure their IT assets following clearly defined practices and requirements. The Estonian Government's Regulation established in 2004 that ISKE's implementation is compulsory for the Estonian public sector handling databases or other forms of registers and stores.

ISKE is based on the German IT Baseline Protection manual (IT-Grundschutz) and had its first version of ISKE's specification was published in October 2003. The latest official major version at the time of writing is version 8.00, with the final draft confirmed on 30.01.2017.

[1]It should be noted that in the given context, "system" represents an abstract framework akin to a standard, and not a physical system.

2 Historical background

The reasons that prompted for a need for an ISKE-like standard were the shortcomings of typical methods of dealing with threats, as there was a need to treat separately the concepts of availability, confidentiality and integrity, but also due to the high expenses in conducting detailed risk-analyses on information systems.

In a sense, in creating ISKE, it was attempted to tackle the problem of not being able to achieve perfect security, which is fundamentally flawed in a production environment, but also satisfy the requirement of needing some general standard of information security.

ISKE's first draft was conceived in 1999 and then refined, with the final draft of the first version published in Ocrober 2003. The first draft and both further and current developments take their roots in the German BSI's, the Federal Office for Information Security, information security standard, called the IT Baseline Protection Manual, or IT-Grundschutz in German.

While the base concepts were ported over from the IT-Grundschutz compendium[2], the Estonian Information System Authority states that adaptions were made in order to suit the Estonian situation.

The first legislation regarding ISKE was accepted on August 29, 2004, which set out the requirements of implementing ISKE to sections of the public sector. The legislation expired on December 31, 2007, with a new one replacing it.[3]

The current legislation regarding the status of ISKE in Estonian information systems was accepted on December 20, 2007, and took effect on the first of January, 2008. It has has been refined twice with the current revision having taken effect on 18.09.2020.[4]

3 ISKE guides and materials

ISKE is comprised of set of different materials. On top of the implementation manual, which is the core of ISKE, it also includes the following:

- Safeguards catalogues
  - Standard modules specifications (catalogue B)
  - Security measures for security levels L, M (catalogue M)
  - Security measures for security level H (catalogue H)
- Hazards catalogue
- Auditing manual

These materials serve to complement the implementation manual, which makes reference to the additional materials for references to more specific requirements or approaches.

[2]2019 version available here.
[3]https://www.riigiteataja.ee/akt/791875
[4]https://www.riigiteataja.ee/akt/115092020015

The auditing manual represents ISKE guidelines in auditing information systems, but is not part of the standard/specification itself and is therefore only a recommended resource..

4 Security classes

ISKE's requirements on systems are set out based on a combination of security objectives and their levels which make up a security class. Each objective is represented by identifier letter and the level is mapped on a 0 - 3 scale, with 3 being the strictest. The objectives are as follows:

- K: availability
- T: integrity
- S: confidentiality

The levels themselves are defined in the ISKE implementation manual.

The data security class is therefore a combination of the three security subclasses, with $4^3 = 64$ possible security classes. An example of such a class would be `K2T3S1`, which represents data with:

- availability in the range $99\% \leq k < 99.9\%$ per year, and consecutive downtime being no more than 4 hours;
- the information's edits and validity must be evident, its correctness verifiable in real time and the information up to date at all times;
- provided to any individual requesting it but only on the basis of legitimate interest.

Furthermore, the letter R represents the consequence element, which also takes a level on the four-level scale, with `R3` standing for mission critical damages, and `R0` being security incidents with no considerable damages.

It is important to note that the ISKE implementation manual requires the required security level for data to be assigned by the owner of the data, and not a security specialist or other third party. This is because other parties may not known the full contents or context of the data in order to appropriately assign a security level. However, security specialists may act as advisors in the matter.

Lastly, security classes must be confirmed by management after they have been assigned by the owner, otherwise they cannot be considered valid.

5 Security levels

In addition to security classes, ISKE also employs the concept of security levels, which depend on the former. There are three baseline security levels:

- L: low security level
- M: medium security level
- H: high security level

TABLE 1: Security classes and their corresponding security levels

		K0	K1	K2	K3
T0-T1	S0-S1	L		M	H
	S2	M			H
	S3	H			
T2	S0-S2	M			H
	S3	H			
T3	S0-S3	H			

The security levels are additive, which means that if M level security measures are to be implemented, then L level measures must be implemented as well. For H level measures, L, M and H must be implemented.

6 Implementation manual

The ISKE implementation manual[5] contains three main sections:

1. Short overview
2. Assigning the required security level of information assets
3. Assigning the required security level and set of security measures

and two minor sections, with definitions and references.

The short overview provides some insight into the workings and structure of ISKE, as well as a higher level overview on how to practically implement it. The most notable subsection is "`1.5.1 11 steps of implementing ISKE`" which can be used as a roadmap.

The second section relates to analysing information systems. It covers the explanation of security classes and their assignment, and specifies criteria and properties of information assets. More importantly, it states that data security is reached only when information availability, integrity and confidentiality have been met.

The third section covers the explanation of security levels and their assignment, as well as criteria relating to those security measures. It also talks about how to assign security levels for information assets without a security class. This would be data such

[5] v.8.00 English version available here.

as additional organisational resources, and, if they belong to standard modules group B1 (general components), should be assigned the highest security level assigned to information with a security class.

7 ISKE in practice

It should be noted that ISKE's practical implementation in a system is not a one-time effort. It should be taken as a model for continuously updating and improving the security of information systems, as the IT infrastructure, threats, safeguarding methods and standards change and evolve with time.

The current law in regards to ISKE in Estonia requires all government agencies or other public sector bodies to follow the the requirements set by the ISKE implementation manual.

It is important to note that the law does not force a specific security class to any information system, as determining the security class is, as ISKE specifies, the role of the owner of the data. However, the law relays ISKE's requirement of confirming the security class, and also describes the auditing requirements of the information systems.

There is little information regarding ISKE's use outside of the public sector, even though the standard is publicly available and allowed to be used by the private sector. However, there exist private companies that provide ISKE auditing services.

The existence of such third party auditors is important, as it is only natural that in auditing systems, be they part of the government or not, the auditor is impartial and not subject to any conflict of interests. This is also a requirement stated in the law.