REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

Implementation manual for the THREE-LEVEL BASELINE SECURITY SYSTEM ISKE

Version 8.00
January 2017

Contents

1 Short overview

ISKE is based on the description of information assets which require protection by means of standard modules and includes means for assigning a security class to each standard module and assigning the required security level to a module based on its security class. Pursuant to the required security level of a standard module, the security measures are assigned from catalogues based on the module's security specification, and the module's security is checked using the threats catalogue.

The ISKE catalogues are located in the ISKE portal at https://iske.ria.ee; the same portal also includes the amendment history of catalogue versions.

1.1 Scope of application

ISKE is intended for achieving and maintaining the security of information systems and information assets related to these systems used for data stores.

ISKE can also be implemented in other state and local government agencies, commercial enterprises, and non-profit organisations.

ISKE is not intended for protecting information systems handling state secrets.

1.2 The nature of baseline security

Implementation of ISKE means that all the specified obligatory measures must be implemented for a specific type of information asset and specific required security level to achieve the required security level. A security measure does not have to be implemented if implementing the specific security measure does not reduce risks and/or implementing the security measure is costly compared to minimising the risks stemming from implementation of the security measure. In addition, every new security measure does not have to be implemented if the risks are covered with the implementation of other measures.

In state agencies, not implementing a specific security measure must be accepted by the information security manager or person responsible for information security. The head of the agency must be notified of risks stemming from not implementing the security measures.

In addition, each security level has recommended measures where implementation is recommended, but not obligatory:

- 'Z' means recommended measures which may prove to be necessary mainly in cases of higher need for security.
- 'W' marks measures which are meant to help in understanding and implementing other security measures.

NB! Discarding even one obligatory measure may mean that the required security level is not achieved.

Irrespective of implementing ISKE, the persons responsible for information security in the agency must carefully monitor information related to new threats and, if necessary, implement other measures in addition to the baseline measures to control these threats. In addition, threats not included in this manual, its future versions or most other security standards remain and must be considered daily.

1.3 Multilevel baseline security

Usually, agencies use systems and services differing from one another based on the level of security requirements. It is practical to implement to these systems respective security measures with varying strength.

ISKE offers three security levels: low (L), medium (M), and high (H).

The measures have a layered structure, so that the medium level is achieved by adding certain measures to the lowest level and the high level is achieved by adding certain measures to the medium level.

1.4 The structure of the implementation manual

The main components of the ISKE implementation manual are guidelines for specifying information assets and security analyses, and the following baseline instruments:

1) 4-level scale for assigning security classes (see section 2.3),
2) table for assigning the required security level (L/M/H) based on security class, see section 3.1,
3) catalogue B of security specifications of information assets standard modules, see the latest valid version at https://iske.ria.ee,
4) threats catalogue G, see the latest valid version at https://iske.ria.ee,
5) catalogue M of security levels L and M security measures, see the latest valid version at https://iske.ria.ee,
6) catalogue H of security level H security measures, see the latest valid version at https://iske.ria.ee

The foreign (base) materials referred to in section 5 includes other resources: methodical manuals, thorough guidelines for implementing security measures, documenting forms, etc.

1.5 Implementation of ISKE

Implementation of ISKE is a continuous process changing the IT environment, security threats and measures, as well as ISKE itself.

Added modules, threats and security measures should be checked regularly and in case of changes to the IT environment or systems of an agency, and necessary security measures should be implemented, if needed. The same should be done after updating the implementation manual of ISKE and publishing a new full version in the ISKE portal.

The ISKE requirements must be considered before commencing development of new information systems or amending existing ones, as it may be very difficult to bring the information systems into accordance with valid rules retroactively.

A person responsible for the implementation of ISKE – ISKE coordinator, person responsible for information security/information security manager, etc. – must be determined to improve the implementation of ISKE in an agency. Implementing ISKE cannot be a 'project' of the IT department, but rather a programme or set of activities involving the entire agency, which is why the person responsible for the implementation of ISKE must be connected well to the management and different departments of the agency. The requirements of the system of security measures for information systems regulation must also be considered; see https://www.riigiteataja.ee/akt/119032012004 (in Estonian).

1.5.1 11 steps of implementing ISKE

The person responsible for the implementation of ISKE must organise the following:

1. Carry out an inventory and specification of information assets in cooperation with the person responsible for IT in the agency and the management of the agency in accordance with guidelines provided in section 2.1.
2. Map data stores in cooperation with the representatives of the principal activity. Each owner of a data store (i.e. main user) assigns a security class for the data store in cooperation with the person responsible for implementing ISKE pursuant to the guidelines provided in section 2.3, and marks the security classes in the specifications of information assets. In addition, the security class of a data store must be forwarded to RIHA via https://www.riha.ee.
3. Assign the security class to other information assets with the specialist of information security pursuant to the guidelines provided in section 2.4, and marks the security classes in the specifications of information assets.
4. Assign the required security level to all information assets with a security class, using the table provided in section 3.1, and marks the security levels in the specifications of information assets.
5. If the highest required security level is M or H, the representative of the management must decide with the person responsible for the implementation of ISKE whether one security level should be implemented in the entire agency, or whether the agency should be divided into zones with different security levels. In the latter case, they must plan the zones and changes necessary for creating such zones. If, during the assignment of the security level, there was no need for security higher than security level L, level L is implemented in the entire agency.
6. Examine catalogue B in the ISKE portal, compare it to the specifications of information assets, and note the marks of standard modules in the specifications pursuant to the guidelines provided in section 2.1. If unspecified assets appear during review of the standard modules catalogue, they must specify these in the course of this work. Standard modules that do not correspond to any assets in the agency are not considered, as the requirement does not involve the assets of the organisation included in module group B1.
7. Pursuant to the highest assigned security level, the person must prepare a list of security governance measures found in the ISKE portal based on catalogue B in the security measures catalogue 'M: security measures for security level L, M' and, in the case of security level H, in catalogue 'H: security measures for security level H'.
8. Involving a representative of the management and employee responsible for IT in the agency, the person must devise a plan for implementing measures of security governance module B 1.0 from the ISKE portal, and after that, the person must assign priorities for implementing the security of other information assets and plan for implementing security, considering the cost of implementing measures and estimated

duration. An overview of which security measures have already been implemented and which have not is necessary for devising the plan.

9. Organise carrying out the plan, preparing lists of security measures based on security specifications of standard modules and catalogues of security measures, stemming from security governance measures and involving relevant employees and regularly informing the management.
10. After each implementation of security measures of an information asset, the person must check the actual security situation from the ISKE portal based on threats catalogue G by considering actual threats in the specific information system. If any threats appear that the security specification of the standard module does not consider, the person must check the adequacy of the implemented security measures in actual conditions and implement additional security measures, if necessary.
11. Maintain the configuration and changes, i.e. all changes related to information assets, standard modules, security classes and measures must be entered into the tool used in the agency to ensure relevant overview of activities related to the information assets of the agency.

NB! If material changes related to data stores (a new data store is created, data content of a data store changes, etc.) and/or information assets related to these are made in the agency, the entire implementation process is started from the beginning or as from the stage impacted by the change.

1.5.2 Implementing ISKE in the use of cloud services and outsourcing services

When using cloud services and outsourcing IT services, the fact that the infrastructure and processes of a service provider cannot usually be directly audited must be considered. Due to this, the implementation of ISKE may partially be based on the terms and conditions of the agreement between the agency and service provider, general conditions of providing the service, and security certificates of the service provider, by including the aforementioned in a relevant risk assessment.

In addition, possible risks, such as long-term network failure of the third party, bankruptcy of the service provider, etc. must be considered. A more detailed list can be found in module B1.11, Outsourcing. In the case of service providers outside the European Union, legal and security aspects must also be considered. Insofar as the agency using the managed software or service is always responsible for data security, the responsibility of parties must be clearly defined in the service agreement when choosing a service provider.

The most important terms and conditions that should be regulated in the agreement between the agency and provider of cloud service, if possible, have been listed in the document ‘Riigipilve kontseptsiooni rakendamise õigusanalüüs’ (p 57, clause 4.7, ‘Lepingutingimused avaliku pilveteenuse osutajaga’, available at: https://www.mkm.ee/sites/default/files/report-state-cloud-concept.ria_2016-05-11.final_.sorainen.pdf (in Estonian)).

1.6 Updating baseline security

ISKE catalogues are published in the ISKE portal (https://iske.ria.ee).

The official full version of ISKE catalogues approved by the Minister of Economic Affairs and Communications is published regularly and is marked as (X.00), full version.

In-between full versions, RIA issues additional interim versions (marked as X.01, X.02, etc.). Interim versions include important changes and additions due to increased need for security and are also included in the next official version. Interim versions also allow the implementer to start implementing security measures on an ongoing basis.

Each following version may include new standard modules with corresponding security measures and/or new security measures for current standard modules.

If an ISKE implementation manual and/or new version is published, the information specialist must examine the updates in the list of modules and security specifications of modules, and organise the security of information assets conforming to the new modules and possible security measures updates of assets conforming to current modules **within one year after the new guide was officially confirmed** by the Minister of Economic Affairs and Communications. The updates/changes must be added to the list of audited objects one year after the publishing of a new official implementation manual.

2. Assigning the required security level of information assets

2.1 Analysis of information systems

This is preparatory work which creates input for security analysis of information systems and its documentation. The work is carried out in three stages. All prepared specifications must include the security class, and cells for security level and standard module marks, which are filled in later.

The level of detail of inventory and specification depends on the needs of the agency and architecture of the system. One of the principles is that the level of detail must allow the implementation of ISKE without causing unnecessary extra time and work for the implementer. There are several options for assigning the level of detail:

- Specification must be carried out with a level of detail sufficient for implementing ISKE – assigning modules, planning the works for ISKE implementation, involving persons carrying out such works, etc.

  For example, if an agency uses Windows Server 2008, it must be marked in the specification to implement module B 3.108, plan its measures, assign persons carrying it out and monitor its implementation.

- Specification must be carried out with a level of detail sufficient for managing the IT environment and/or managing systems configuration.

  For example, agencies must in any case have an overview of the IT environment (devices, licenses, systems, etc.). Such overview which has been updated, if necessary, may be sufficient for implementing ISKE.

In any case, information system components under the control of the agency and outsourced services, including cloud services, must be distinguished.

2.1.1 Inventory of information systems

The conformity of information systems inventory must be checked at least once a year. It is recommended to immediately mark all changes in information systems which are important with relation to implementing ISKE in the inventory management tool.

2.1.2 Specification and categorisation of information assets

For each component, minimal information should be available, and this information may be recorded in a separate table, catalogue, or tool/management facility. The level of detail chosen for each component depends on the needs of the agency but must be sufficient to allow the implementation of ISKE and auditing based on it.

Example of a level of detail of information:

- Unique name (e.g. full name or ID number of the device);
- Type (e.g. database server, workstation, communication system of application x, etc.) and function;
- The platform used (i.e. hardware and operation system);
- Work method (e.g. operating, supporting or autonomous);
- Application and database used;
- Location (e.g. building and room number);
- Administrator responsible and users (unit/title/role, etc.);
- Status (being used, in testing, planned)
- Communication interferences used (Internet, Bluetooth, WLAN adapter);
- Type of network connection and network address.

In addition to devices, the commonly used parts of infrastructure must also be specified (e.g. archive and storage rooms, meeting rooms, server rooms, racks, switchboards, power lines, etc.)

Network topology, connections between the components of the information system, etc. should be presented/managed as schemes.

Information assets are divided into operating, supporting, and autonomous assets.

Operating information assets – assets directly required to ensure the work of a data store (e.g. application, database, server, etc.);

Supporting information assets – assets required to ensure the work of data stores and/or operating assets related to these, which in themselves are not directly required to process data or make data available from a data store.

Autonomous information assets – assets whose primary function is not related to data or data stores (e.g. workspaces, buildings).

Dividing into different types of assets in different ways may vary between agencies and therefore there are no right solutions. It is more important to assess the support level of assets. The guidelines necessary for this are provided in section 2.4 of this manual.

2.1.3 Grouping of information assets

It is recommended to group similar information assets, as it simplifies ISKE management and the process of implementing security measures.

The following characteristics may be considered in grouping similar information assets:

- Information assets are of the same type;
- Information assets have been configured and are configured the same way;
- Information assets have been connected to the network the same way (IT systems into the same communicator);
- Information assets have the same administrative and infrastructure-related requirements;
- Information assets have the same security requirements;

It should be considered in the grouping of information assets that the security measures implementation process would still allow maintaining records of the implementation of security measures.

One example of grouping information assets is workstations of an agency. One group may include agency workspaces with operation system Windows 7 that are being centrally and similarly managed.

2.2 Security indicators

2.2.1 Information security and security goals

ISKE uses a security model which is based on ensuring three partial goals (availability, integrity, and confidentiality).

Data availability is the timely and easy accessibility of usable data at the previously agreed upon necessary and required working time (i.e. at the necessary and required moment and within the necessary and required time period) by the persons or technical means authorised for this. Availability is the primary requirement for all data and other information assets of each information system; if availability is lost, the entire information system becomes useless.

Data integrity means the assurance of data correctness, completeness and being up to date and authenticity of origin, and absence of unauthorised changes.

Data confidentiality means the accessibility of data only by authorised consumers (persons or technical means) and inaccessibility by anyone else.

No information system is completely secure, available, integral, and confidential. The information security aspects that should be considered in the case of specific data depend on that information system and its purpose, i.e. value of handled data. In most cases, all three security components must be considered, but they carry different weight. The required security level of an organisation depends on the tasks, legal acts, and rules of the organisation, internal organisation of the activities of the agency, and guaranteed or required security level of information systems, service providers and partners or contractual partners.

Data security means that the three goals**: information availability (K), information integrity (T), information confidentiality (S)** have been met.

2.3 Assigning data security classes

The owner of the data must assign the required security level of data. The information security specialist cannot assign the required security level of data, as they may not know the background of the data security needs and requirements provided to data by the principal activity. The IT or information security specialist may act as an advisor. The security classes must be **confirmed by the management of the agency** after the security classes and security subclasses have been assigned by the owner.

ISKE uses a four-level scale for assigning security levels and stems from the three security goals provided in section 2.2.1.

The following **security subclasses** are assigned by implementing the four-level scale to the three security goals, and the markings of such security subclasses comprise the marking of a security goal and security level value.

Availability:

K0 – Availability – less than 90% per year and maximum acceptable single interruption duration during the service is more than 24 hours (i.e. single interruption duration may exceed 24 hours)*;

K1 – Availability – more than or equal to 90% and less than 99% per year and maximum acceptable single interruption duration during the service is up to 24 hours (i.e. single interruption duration may be between less than or equal to 24 hours and more than 4 hours)*;

K2 – Availability – more than or equal to 99% and less than 99.9% per year and maximum acceptable single interruption duration during the service is up to 4 hours (i.e. single interruption duration may be between less than or equal to 4 hours and more than 1 hour)*;

K3 – Availability – more than or equal to 99.9% per year and maximum acceptable single interruption duration during the service is up to 1 hour (i.e. single interruption duration may be less than or equal to 1 hour)*;

Integrity:

T0 – information source, detectability of amendments or termination is not important; controlling the correctness, integrity, and being up to date is not necessary;

T1 – information source, the fact of its amendments or termination must be detectable; controlling the correctness, integrity, and being up to date in special cases and according to need;

T2 – information source, the fact of its amendments or termination must be detectable; periodic control of the correctness, integrity and being up to date is required;

T3 – information source, the fact of its amendments or termination must have evidential value; real-time control of the correctness, integrity, and being up to date is required.

Confidentiality:

S0 – public information: access to the information is not limited (i.e. all interested persons have read access, permission to change is determined based on the integrity requirement);

S1 – information intended for internal use purposes: access to the information must be granted if the person requesting access has legitimate interest;

S2 – classified information: information can only be used by certain user groups; access to the information must be granted if the person requesting access has legitimate interest;

S3 – highly classified information: information can only be used by certain users; access to the information must be granted if the person requesting access has legitimate interest.

* The maximum number of accepted interruptions, the maximum total number of accepted interruptions, and other more detailed security level measures are described and agreed on in service level agreements (SLAs). Service provision conditions (e.g. time for replying to queries, time for regular maintenance, required time for eliminating errors, contact information for reporting errors, backup conditions, etc.) must be established with more detail in the service level agreement.

Data security class is the specific combination of the three security subclasses. The total number of their combinations is 4 × 4 × 4 and therefore, there are 64 different security classes.

The data security class marking must be formed based on the markings of subclasses in their order K-T-S.

One specific data security class is, for example, **K2T3S1**. This marking must form the basis for assigning the obligatory baseline security measures of data and other information assets. Security measures corresponding to the security class of an information asset must be implemented to ensure the goals of data security. Security measures are chosen from the catalogue of baseline measures relevant for that security class, based on the specifications of baseline security of that information asset.

In assigning the data security class, the chief processor of the data store must perform the security analysis of the data handled in information systems, assigning the security subclasses based on the abovementioned criteria. Different data of the same data store may have a different security class. The security analysis must focus especially on data handled either by using cloud services or e.g. as a full service of a service provider.

The data security class is not sufficient to replace service level agreements or other agreements of services provided using a data store.

The following requirements must be considered upon assigning **security subclasses**:

- **Requirements arising from legal acts and agreements**

  Requirements arising from legal acts e.g. to information confidentiality. If information has been acknowledged as information subject to publication in legislation (e.g. pursuant to the Public Information Act), confidentiality security subclass S0 should be assigned. If information has been acknowledged as information with a certain level of

limited access under the laws, confidentiality security subclass S1, S2 or S3 should be assigned pursuant to the requirements. At least security subclass S2 should be assigned in processing sensitive personal data.
Agreements should be followed if they provide obligations to data availability, integrity and/or confidentiality. If, for example, a state agency uses the services provided by another state agency and they have entered into an agreement which provides specific requirements to data availability, integrity, and confidentiality, these requirements and obligations must be considered in assigning security subclasses.

- **Requirements arising from the processes of the principal activity (or business activity)**
  The principal activity may provide specific requirements to the provided IT services and these also establish requirements to data availability, integrity, and confidentiality. If the service bureaus of an agency must provide a service to citizens e.g. Mon–Fri at 9.00 a.m. – 6.00 p.m., the IT systems must work, and data availability must be ensured during these hours.

- **Assessing the importance of consequences**

  Importance of consequences means assessing the damage caused by a security incident. The damages may be assessed on a four-level scale:

  R0 – security incidents (i.e. not conforming to the requirements of data availability, integrity, and/or confidentiality) do not result in considerable damages;

  R1 – insignificant damages occur, a security incident (i.e. not conforming to the requirements of data availability, integrity, and/or confidentiality) is likely to result in significant obstacles to performing the function of the agency, or significant financial losses;

  R2 – significant damages occur, a security incident (i.e. not conforming to the requirements of data availability, integrity, and/or confidentiality) is likely to result in considerable obstacles to performing the function of the agency or danger to human health or danger of environmental pollution, or significant financial losses;

  R3 – highly significant (mission critical) damages occur, a security incident (i.e. not conforming to the requirements of data availability, integrity, and/or confidentiality) is likely to result in not performing the function of the agency or significant disturbances in state organisation or danger to human health or danger of environmental pollution, or highly significant financial losses.

If the aforementioned requirements assign different levels, the highest level must be based on in assigning the security subclass.

For example, if no requirements are provided for the integrity security subclass by laws/agreements, principal activity requirements assign level ‘2’, and importance of consequences assigns level ‘3’, then security subclass T3 is assigned based on the aforementioned.

Information systems specifications prepared as a result of the analysis of information systems (section 2.1) and containing the data security classes are used for systematic performance and

documenting of the security analysis. All specified information systems are reviewed in the course of the security analysis. The chief processor of the data store must perform the security analysis of the data.

2.4 Assigning the security class of other information assets

If data security classes have been assigned, the security classes of other information assets are assigned, starting from information systems handling data with the highest security classes.

After that, all information assets related to the system (including supporting and autonomous assets) are reviewed and their importance is assessed considering the data stores of the highest security class by using the scale in the table below.

Role of an asset	**Criterion**
Important	Without this asset, the data store cannot function, and this asset is directly required for the functioning of the data store and/or the data store can function a relatively short period with other means.
Unimportant	The data store can function, and/or works/services/functions can be performed in another way.

If an asset proves important for a data store with a high security class, it must be assigned an equivalent security class; in other cases, the class may be one level lower. The security subclass may only be lowered if it does not endanger the security of the entire system and does not contradict the assigned security class.

The specialist responsible for information technology along with the information security specialist must assign security classes of information assets.

When performing the work, connections between systems must be carefully considered, taking care that insufficient security of other systems related to important information systems does not endanger the security of important systems. If the agency structure, rooms, technical infrastructure, and conditions allow zoning with regard to various ISKE classes to reduce costs, it may be used. Dangers and risks which may result from lowering the security level of an asset, and whether the agency is prepared to accept those risks must be considered upon assigning the support level of information assets.

Examples of assigning the security class of an asset

If the security level of a data store is H and the H security level is based on availability, then in most cases it is reasonable to also assign high availability requirements to all assets ensuring the availability of the data store, i.e. application, database, operation system, server, network devices, firewall, server room, cables, and workstations which require high availability in the meaning of data handling. It is reasonable to lower the security level for the following supporting assets: office rooms, meeting halls and workstations where users do not have to access the data store on handling level H. It should also be observed that if the confidentiality of the data store should be ensured on level S2, the security class of the workstation where the data is processed must be equivalent. In addition, if the system's architecture allows, separate security classes may be assigned to the data store services.

However, if security level H is based on data confidentiality, it is not always necessary to assign security level H, for example, to cabling, if the data is encrypted in the cable.

For information systems independent of other information systems, the data security class is primarily considered. If it is relatively low, the importance of the entire system is assessed; the table provided above may be used for this. If the system as a whole proves more important than the currently handled data (e.g. considering the cost), it must be assigned a corresponding higher security class. The security class assigned to an information system must also be assigned to the information assets directly related to it.

When assessing information assets which are not currently in use (power and communication lines which have not been put into use yet, software being tested, etc.), their future purpose must be considered.

3. Assigning the required security level and set of security measures

3.1 Assigning the security level based on security class

Based on the security class, all previously specified (section 2.1.2) information assets which were assigned a security class based on the security analysis must be assigned a required security level.

There are a total of 64 security classes, i.e. various combinations of the three security subclasses.

The following table assigns three baseline security levels to these 64 combinations:

- **low security level (L),**
- **medium security level (M),**
- **high security level (H).**

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

Based on the security subclasses of each information asset's security class, the required baseline security level must be located from the table, and this must be marked in the information assets specification (section 2.1.2).

After that, standard modules catalogue M is used to locate the standard module marking corresponding to that information asset, and this must be marked in the information assets specification (section 2.1.2).

If the security levels of all specified assets have been assigned, the following activities are based on the number of security levels obtained:

- if all assets have the same security level, security measures may be assigned based on standard modules security specifications and security measures catalogue;
- if there are two or three security levels, the option of optimal zoning of the agency should be analysed.

Optimal organisation of zoning may require changes in system functions and locations, room functions, etc. The changes must be designed, confirmed, and planned. In the interest of optimal zoning, the previously assigned security level of some information assets may be raised, while for some, the level may be lowered as a result of transfer of functions.

3.2 Assigning the security level of information assets without a security class

Section 3.1 provides guidelines for assigning the required security level of information assets with a security class, i.e. specified information assets. However, only data, tangible information assets, and software were subject to specification. The work organisation processes and other organisational resources also need protection, and information security management itself is dependent on the required security level.

All such unspecified assets have been described as relevant standard modules in catalogue B, which mainly belong in standard modules group B1.

The highest security level assigned in section 3.1 must be assigned to standard modules group B1.

If it becomes evident during the review of standard modules that there are some unspecified information assets, their connections to already categorised information assets should be examined, and the security level should be assigned based on this.

3.3. Assigning security measures

If the required security level of all information assets has been assigned, the standard modules corresponding to each information asset should be located from catalogue B. The standard modules specifications also include a list of security measures subject to implementation.

In doing that, the layers of baseline security should be considered. This means that security measures of levels L and M must be implemented in implementing level M, and security measures of levels L, M and H must be implemented in implementing level H.

The measures of the highest level are divided into:

- obligatory (measures of sub-catalogue HG of catalogue H) and

- conditional (measures of sub-catalogues HK, HT, HS of catalogue H).

The implementation of conditional measures depends on the module group's security subclass(es) of the highest level:

- for K3, all HK measures listed in the following table must be implemented
- for T3, all HT measures listed in the following table must be implemented
- for S3, all HS measures listed in the following table must be implemented

Assignment of security measures must be started with module group B1 and module B1.0, which assigns the information security management measures.

After that, security measures must be assigned to the information assets of the highest security level, and their layered implementation must be achieved.

The following handling of assets is not as important and may depend on specific circumstances.

Once all security measures have been established, the actual threat situation must be checked compared to the threats column of module specification and data in ISKE threats catalogue G to establish possible threats not included in the catalogue. If such new threats are established, it must be examined whether the baseline measures assigned are sufficient for managing them or whether additional measures should be implemented.

4 Definitions and abbreviations used

This glossary provides definitions and terms not included in the http://akit.cyber.ee dictionary or the ISO/IEC 27000 standard *Information technology — Security techniques — Information security management systems — Overview and vocabulary*.

Information i.e. **info** is any knowledge related to objects – e.g. facts, events, processes, or ideas – which holds a meaning in specific context.

Data is the redefining presentation of information available for forwarding, interpreting, or processing. Information itself does not have a form; it is created through presentation, i.e. data. Data means the presentation of information in a previously agreed upon form and on a carrier, such as a paper document, digital recording on a magnetic disc, microfilm, photo, etc.

Data store is a set of organised data processed in the information system of a state, local government or another person in public law, or private person performing public duties, and such data is established and used to perform duties provided in laws, legislation issued on the basis of these, or international agreements.

Security analysis of data – the assessment of the criticality of data, carried out for the assignment of security class and determination of damages arising from the lack of data security.

Audit is the systematic inspection of the suitability of and adherence to a provided security policy. An audit must be independent and neutral.

BSI (Bundesamt für **Sicherheit** in der **Informationstechnik**, Federal Office for Information Security of Germany**)** – an agency which develops and manages the baseline security handbook *IT-Grundschutzhandbuch* forming the basis for ISKE, see https://www.bsi.bund.de.

Digital signature is authentication information added to a message or file, which is characterised by the following features:

- digital signature allows unambiguous identification of its creator;
- digital signature allows checking whether the digitally signed file is identical to the actually signed file.

Baseline measures – typical catalogued security measures equipped with selection methods; the selection among them depends on the security class and the composition of the information system processing the data.

Layered nature of baseline security – the ISKE methodology provides three layers: high (H), medium (M) or low (L).

- 'Z' means recommended measures which may prove to be necessary mainly in cases of higher need for security.
- 'W' marks measures intended to help in understanding and implementing other security measures.

Baseline security – set of measures, the implementation of which is necessary for obtaining and retaining data security.

Information system – technical system processing, storing or transmitting data, along with the means, resources, and processes needed for its normal operation.

Information security manager – competent person from the IT department of a company or agency who is responsible for all matters of IT security participates in the IT security process and work of the IT security management team, contributes to the development of the IT security concept and other documents (e.g. preparedness for emergency), and plans and monitors their implementation.

ISKE – three-level IT baseline security system of information systems.

Coordinator of ISKE – person whose duty is to entirely coordinate and manage the introduction of ISKE in an agency.

Procedure for implementing ISKE – procedures and methods provided in sections 1–3 of the ISKE implementation manual for implementing ISKE.

IT baseline security analysis – IT baseline security analysis includes modelling along with establishing the required security measures and a basic security check where the implementation of security measures currently used in a company or agency are compared to the requirements.

IT baseline security – the term 'IT baseline security' means the methodology of developing the management system for information security as well as securing IT assets with basic security measures. This term is also used for a situation where standard security measures are required for IT systems with normal security requirements.

IT-Grundschutzhandbuch – baseline security handbook published by BSI; forms the basis for ISKE (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html).

Operating information assets – assets directly required to ensure the work of a data store (e.g. application, database, server, etc.).

Catalogue of measures – for each module, IT baseline security catalogues recommend a suitable measure which have been arranged as catalogues and divided into infrastructure, organisation, staff, hardware/software, communication, and preparedness for an emergency.

Modelling – pursuant to IT baseline security, modelling is interpreted as mapping of the IT assets of a company or agency based on the modules included in the IT baseline security catalogues. Pursuant to chapter 2.2 of the IT baseline security catalogue, each module contains a reference regarding when it should be implemented and what should be considered.

Module – the term is used for structuring the recommendations included in the IT baseline security catalogue. Modules are units of one layer (e.g. IT systems, networks). On the one hand, these describe technical components (e.g. cabling); on the other hand, organisational measures (e.g. concept of preparedness for an emergency) and special forms of implementation (e.g. home office). Each module describes a specific IT component and lists threats, as well as provides recommendations for implementation of organisational and technical security measures.

Cloud service – a web-based shared IT management or implementation service. In the case of a cloud service, various information systems share the same resources or various agencies use the same web-based information system. More detailed definition of shared cloud service has been provided in the NIST manual 800-145 http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

RIA – Information System Authority.

RIHA – Administration System for the State Information System, see https://www.riha.ee

Supporting information assets – assets required for ensuring the work of data stores and/or operating assets related to these, which in themselves are not directly required for processing data or making data available from a data store (e.g. backup server, network devices, firewall, etc.)

Security level – information security indicator assigned based on a security class pursuant to the guidelines provided in the ISKE implementation manual. ISKE includes three security levels L – low, M – medium, and H – high.

Security incident – event and/or events resulting in loss of data availability, integrity and/or confidentiality and/or other information assets and/or in material danger of loss of data availability, integrity and/or confidentiality.

Security class – security level based on the criticality of data, expressed on a four-level scale and with three components, i.e. as a combination of three security subclasses. The data security class marking must be formed based on the markings of security subclasses in their order K-T-S, e.g. K2T3S1.

Security subclass – level required to obtain the purpose of information security based on the criticality of data, expressed on a four-level scale. The three purposes of information security give rise to three security subclasses. The security subclass marking comprises the security goal marking (e.g. K, T, S) and security level value (e.g. 0, 1, 2, 3), e.g. K2.

Security measure – organisational acts and means, technical processes and implementation of technical means for obtaining and retaining the safety of data and data in information systems. Security measure (measure in short) means all activities with the purpose of decreasing and preventing security risks. This can be done with security measures related to the organisation, as well as persons, technical means, or infrastructures. Synonyms 'safeguard' or 'control measure' are also sometimes used. The term 'control' is often used with 'safeguard'.

5 References to additional information

ISKE is based on the IT baseline security handbook (*IT Grundschutzhandbuch*) published by the Federal Office for Information Security of Germany (Bundesamt für Sicherheit in der Informationstechnik, BSI). The BSI system has been documented very comprehensively and with a great level of detail, and it is updated regularly once a year. We recommend finding additional information from the BSI handbook for the description of modules, threats, and security measures with no clarifying entries or if such entries prove to be insufficient.

The following materials are available on the BSI webpage:

- ***IT Baseline Protection Manual* in English** (2013 version): https://download.gsb.bund.de/BSI/ITGSKEN/IT-GSK-13-EL-en-all_v940.pdf
- ***IT-Grundschutzhandbuch* in German** (2016 version): https://download.gsb.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2016_EL15_DE.pdf

The following standards may also provide some useful guidelines in organising security management:

- EVS-ISO/IEC 27002. Information technology. Security techniques. Code of practice for information security controls
- EVS-ISO/IEC 27001. Information technology. Security techniques. Information security management systems. Requirements.