INFOTEHNOLOOGIA
Turbemeetodid
Võrguturve
Osa 1: Ülevaade ja mõisted

Information technology
Security techniques
Network security
Part 1: Overview and concepts
(ISO/IEC 27033-1:2009)

EESTI STANDARDIKESKUS EVS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA	NATIONAL FOREWORD
See Eesti standard EVS-ISO/IEC 27033-1:2011 „Infotehnoloogia. Turbemeetodid. Võrguturve. Osa 1: Ülevaade ja mõisted“ sisaldab rahvusvahelise standardi ISO/IEC 27033-1:2009 „Information technology – Security techniques – Network security – Part 1: Overview and concepts“ identset ingliskeelset teksti.	This Estonian Standard EVS-ISO/IEC 27033-1:2011 consists of the identical English text of the International Standard ISO/IEC 27033-1:2009 “Information technology – Security techniques – Network security – Part 1: Overview and concepts “.
Ettepaneku rahvusvahelise standardi ümbertrüki meetodil ülevõtuks on esitanud EVS/TK 4, standardi avaldamist on korraldanud Eesti Standardikeskus.	Proposal to adopt the International Standard by reprint method has been presented by EVS/TK 4, the Estonian standard has been published by the Estonian Centre for Standardisation.
Standard EVS-ISO/IEC 27033-1:2011 on jõustunud sellekohase teate avaldamisega EVS Teataja 2012. aasta jaanuarikuu numbris.	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardsation.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Käsitlusala

ISO/IEC 27033 see osa annab ülevaate võrguturbest ja seotud määratlustest. Standard määratleb ja kirjeldab mõisteid, mis on seotud võrguturbega ja annab võrguturbe halduse juhiseid. (Lisaks sidelülide kaudu edastatava teabe turbele puudutab võrguturve seadmete turvet, nende seadmetega seotud haldustegevuste turvet, rakendusi ja teenuseid ning lõppkasutajaid.)

Standard puudutab kõiki, kes on seotud mingi võrgu omamise, käituse või kasutamisega. Lisaks juhtidele ja ülematele, kellel on erikohustused infoturbe ja/või võrguturbe ja võrgu käituse alal või kes vastutavad organisatsiooni üldise turbekava ja turvapoliitika väljatöötamise eest, kuuluvad nende hulka kõrgemad juhid ja muud kasutajate mittetehnilised juhid. See puudutab ka kõiki võrguturbe arhitektuuri aspektide plaanimises, kavandamises ja teostamises osalejaid.

Lisaks annab ISO/IEC 27033 see osa

— juhiseid selle kohta, kuidas tuvastada ja analüüsida võrgu turvariske ning määrata selle analüüsi põhjal võrgu turvanõuded;

— ülevaate meetmetest, mis toetavad võrgu tehnilise turbe arhitektuure ja nendega seotud tehnilisi meetmeid ning ka neid mittetehnilisi ja tehnilisi meetmeid, mis on rakendatavad mitte ainult võrkudele;

— sissejuhatava kirjelduse kvaliteetsete võrgu tehnilise turbe arhitektuuride saavutamise ning tüüpiliste võrgustsenaariumite ja võrgu tehnoloogiliste aladega seotud riski-, kavandamis- ja reguleerimisaspektide kohta (üksikasjalikumalt käsitlevad neid ISO/IEC 27033 järgmised osad);

— lühida küsimuste käsitluse, mis on seotud võrguturbe meetmete teostamise ja käitusega ning nende teostuse pideva seire ja läbivaatusega.

Kokkuvõttes annab standard ülevaate standardisarjast ISO/IEC 27033 ning sissejuhatuse teistesse osadesse.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.040

Contents

Introduction

In today’s world, the majority of both commercial and government organizations have their information systems connected by networks (see Figure 1), with the network connections being one or more of the following:

- within the organization,
- between different organizations,
- between the organization and the general public.

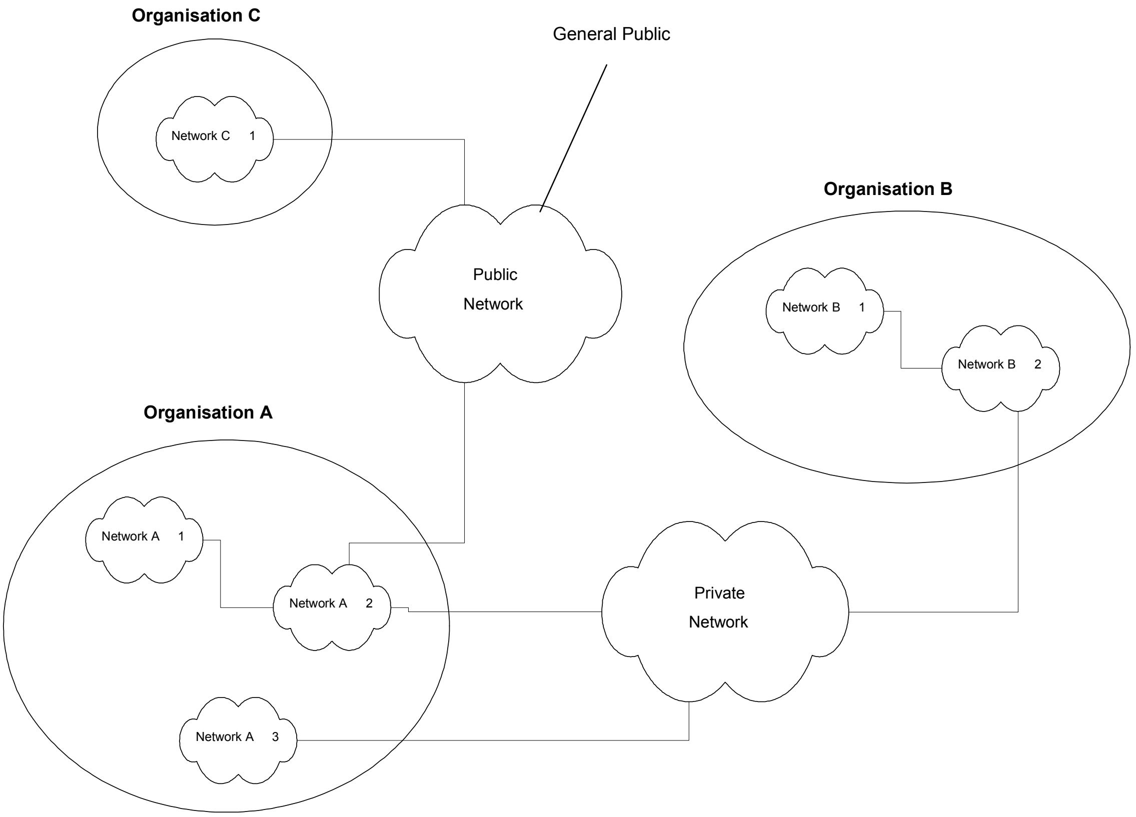

Figure 1 — Broad types of network connection

Further, with the rapid developments in publicly available network technology (in particular with the Internet) offering significant business opportunities, organizations are increasingly conducting electronic business on a global scale and providing online public services. The opportunities include the provision of lower cost data communications, using the Internet simply as a global connection medium, through to more sophisticated services provided by Internet service providers (ISPs). This can mean the use of relatively low cost local attachment points at each end of a circuit to full scale online electronic trading and service delivery systems, using web-based applications and services. Additionally, the new technology (including the integration of data, voice and video) increases the opportunities for remote working (also known as “teleworking” or “telecommuting”) that enable personnel to operate away from their home work base for significant periods of time. They are able to keep in contact through the use of remote facilities to access organization and community networks and related business support information and services.

However, whilst this environment does facilitate significant business benefits, there are new security risks to be managed. With organizations relying heavily on the use of information and associated networks to conduct their business, the loss of confidentiality, integrity, and availability of information and services could have significant adverse impacts on business operations. Thus, there is a major requirement to properly protect networks and their related information systems and information. In other words: *implementing and maintaining adequate network security is absolutely critical to the success of any organization’s business operations.*

In this context, the telecommunications and information technology industries are seeking cost-effective comprehensive security solutions, aimed at protecting networks against malicious attacks and inadvertent incorrect actions, and meeting the business requirements for confidentiality, integrity, and availability of information and services. Securing a network is also essential for maintaining the accuracy of billing or usage information as appropriate. Security capabilities in products are crucial to overall network security (including applications and services). However, as more products are combined to provide total solutions, the interoperability, or the lack thereof, will define the success of the solution. Security must not only be a thread of concern for each product or service, but must be developed in a manner that promotes the interweaving of security capabilities in the overall security solution.

The purpose of ISO/IEC 27033 is to provide detailed guidance on the security aspects of the management, operation and use of information system networks, and their inter-connections. Those individuals within an organization that are responsible for information security in general, and network security in particular, should be able to adapt the material in this International Standard to meet their specific requirements. Its main objectives are as follows.

— ISO/IEC 27033-1, *Overview and concepts,* to define and describe the concepts associated with, and provide management guidance on, network security. This includes the provision of an overview of network security and related definitions, and guidance on how to identify and analyze network security risks and then define network security requirements. It also introduces how to achieve good quality technical security architectures, and the risk, design and control aspects associated with typical network scenarios and network “technology” areas (which are dealt with in detail in subsequent parts of ISO/IEC 27033).

— ISO/IEC 27033-2, *Guidelines for the design and implementation of network security,* to define how organizations should achieve quality network technical security architectures, designs and implementations that will ensure network security appropriate to their business environments, using a consistent approach to the planning, design and implementation of network security, as relevant, aided by the use of models/frameworks (in this context, a model/framework is used to outline a representation or description showing the structure and high level workings of a type of technical security architecture/design), and is relevant to all personnel who are involved in the planning, design and implementation of the architectural aspects of network security (for example network architects and designers, network managers, and network security officers).

— ISO/IEC 27033-3, *Risks, design techniques and control issues for reference network scenarios*, to define the specific risks, design techniques and control issues associated with typical network scenarios. It is relevant to all personnel who are involved in the planning, design and implementation of the architectural aspects of network security (for example network architects and designers, network managers, and network security officers).

It is proposed that future parts of ISO/IEC 27033 will address the following topics.

— ISO/IEC 27033-4, *Risks, design techniques and control issues for securing communications between networks using security gateways*, to define the specific risks, design techniques and control issues for securing information flows between networks using security gateways. It will be relevant to all personnel who are involved in the detailed planning, design and implementation of security gateways (for example network architects and designers, network managers, and network security officers).

- SO/IEC 27033-5, *Risks, design techniques and control issues for securing virtual private networks,* to define the specific risks, design techniques and control issues for securing connections that are established using virtual private networks (VPNs). It will be relevant to all personnel who are involved in the detailed planning, design and implementation of VPN security (for example network architects and designers, network managers, and network security officers).

- ISO/IEC 27033-6, *IP convergence*, to define the specific risks, design techniques and control issues for securing IP convergence networks, i.e. those with the convergence of data, voice and video. It will be relevant to all personnel who are involved in the detailed planning, design and implementation of security for IP convergence networks (for example network architects and designers, network managers, and network security officers).

- ISO/IEC 27033-7, *Wireless*, to define the specific risks, design techniques and control issues for securing wireless and radio networks. It will be relevant to all personnel who are involved in the detailed planning, design and implementation of security for wireless and radio networks (for example network architects and designers, network managers, and network security officers).

It is emphasized that ISOI/IEC 27033 provides further detailed implementation guidance on the network security controls that are described at a basic standardized level in ISO/IEC 27002.

If there are other parts in the future, these will be relevant to all personnel who are involved in the detailed planning, design and implementation of the network aspects covered by those parts (for example network architects and designers, network managers, and network security officers).

It should be noted that this International Standard is not a reference or normative document for regulatory and legislative security requirements. Although it emphasizes the importance of these influences, it cannot state them specifically, since they are dependent on the country, the type of business, etc.

Unless otherwise stated, throughout this part of ISO/IEC 27033 the guidance referenced is applicable to current and/or planned networks, but will only be referenced as “networks” or “the network”.

Information technology — Security techniques — Network security —

Part 1: Overview and concepts

1 Scope

This part of ISO/IEC 27033 provides an overview of network security and related definitions. It defines and describes the concepts associated with, and provides management guidance on, network security. (Network security applies to the security of devices, security of management activities related to the devices, applications/services, and end-users, in addition to security of the information being transferred across the communication links.)

It is relevant to anyone involved in owning, operating or using a network. This includes senior managers and other non-technical managers or users, in addition to managers and administrators who have specific responsibilities for information security and/or network security, network operation, or who are responsible for an organization's overall security program and security policy development. It is also relevant to anyone involved in the planning, design and implementation of the architectural aspects of network security.

This part of ISO/IEC 27033 also

- provides guidance on how to identify and analyse network security risks and the definition of network security requirements based on that analysis,
- provides an overview of the controls that support network technical security architectures and related technical controls, as well as those non-technical controls and technical controls that are applicable not just to networks,
- introduces how to achieve good quality network technical security architectures, and the risk, design and control aspects associated with typical network scenarios and network "technology" areas (which are dealt with in detail in subsequent parts of ISO/IEC 27033), and
- briefly addresses the issues associated with implementing and operating network security controls, and the on-going monitoring and reviewing of their implementation.

Overall, it provides an overview of the ISO/IEC 27033 series and a "road map" to all other parts.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 7498 (all parts), *Information technology — Open Systems Interconnection — Basic Reference Model*

ISO/IEC 27000:2009, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*

ISO/IEC 27005:2008, *Information technology — Security techniques — Information security risk management*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 7498, ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 and the following apply.

NOTE The following terms and definitions will also apply to future parts of ISO/IEC 27033.

3.1
alert
"instant" indication that an information system and network may be under attack, or in danger because of accident, failure or human error

3.2
architecture
fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution

[ISO/IEC 15288:2008, definition 4.5]

3.3
attacker
person deliberately exploiting vulnerabilities in technical and non-technical security controls in order to steal or compromise information systems and networks, or to compromise availability to legitimate users of information system and network resources

3.4
audit logging
recording of data on information security events for the purpose of review and analysis, and ongoing monitoring

3.5
audit tools
automated tools to aid the analysis of the contents of audit logs