INFOTEHNOLOOGIA
Turbemeetodid
Võrguturve
Osa 2: Võrguturbe kavandamise ja teostamise juhised

Information technology
Security techniques
Network security
Part 2: Guidelines for the design and implementation of network security
(ISO/IEC 27033-2:2012)

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

See Eesti standard EVS-ISO/IEC 27033-2:2013 „Infotehnoloogia. Turbemeetodid. Võrguturve. Osa 2: Võrguturbe kavandamise ja teostamise juhised“ sisaldab rahvusvahelise standardi ISO/IEC 27033-2:2012 „Information technology – Security techniques – Network security – Part 2: Guidelines for the design and implementation of network security“ identset ingliskeelset teksti.

Ettepaneku rahvusvahelise standardi ümbertrüki meetodil ülevõtuks on esitanud EVS/TK 4, standardi avaldamist on korraldanud Eesti Standardikeskus.

Standard EVS-ISO/IEC 27033-2:2013 on jõustunud sellekohase teate avaldamisega EVS Teataja 2013. aasta augustikuu numbris.

Standard on kättesaadav Eesti Standardikeskusest.

NATIONAL FOREWORD

This Estonian Standard EVS-ISO/IEC 27033-2:2013 consists of the identical English text of the International Standard ISO/IEC 27033-2:2012 „Information technology – Security techniques – Network security – Part 2: Guidelines for the design and implementation of network security“.

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.

This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.

The standard is available from the Estonian Centre for Standardisation.

Käsitlusala

See ISO/IEC 27033 osa annab organisatsioonidele juhiseid võrguturbe plaanimiseks, kavandamiseks, teostamiseks ja dokumenteerimiseks.

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

Page

Foreword v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Abbreviations 2

5 Document structure 2

6 Preparing for design of network security 3
6.1 Introduction 3
6.2 Asset identification 3
6.3 Requirements collection 3
6.3.1 Legal and regulatory requirements 3
6.3.2 Business requirements 4
6.3.3 Performance requirements 4
6.4 Review requirements 4
6.5 Review of existing designs and implementations 5

7 Design of network security 5
7.1 Introduction 5
7.2 Design principles 6
7.2.1 Introduction 6
7.2.2 Defence in depth 6
7.2.3 Network Zones 7
7.2.4 Design resilience 7
7.2.5 Scenarios 8
7.2.6 Models and Frameworks 8
7.3 Design Sign off 8

8 Implementation 8
8.1 Introduction 8
8.2 Criteria for Network component selection 9
8.3 Criteria for product or vendor selection 9
8.4 Network management 10
8.5 Logging, monitoring and incident response 11
8.6 Documentation 11
8.7 Test plans and conducting testing 11
8.8 Sign off 12

Annex A (informative) Cross**-references between ISO/IEC 27001:2005/ISO/IEC 27002:2005 network security related controls and ISO/IEC 27033-2:2012 clauses** 13

Annex B (informative) **Example documentation templates** 14
B.1 An example network security architecture document template 14
B.1.1 Introduction 14
B.1.2 Business related requirements 14
B.1.3 Technical architecture 14
B.1.4 Network services 17
B.1.5 Hardware/physical layout 17
B.1.6 Software 18
B.1.7 Performance 19
B.1.8 Known issues 19
B.1.9 References 19

B.1.10 Appendices **20**
B.1.11 Glossary **20**
B.2 An example template for a Functional Security requirements document **20**
B.2.1 Introduction **20**
B.2.2 Firewall configuration **21**
B.2.3 Security risks **21**
B.2.4 Security management **22**
B.2.5 Security administration **22**
B.2.6 Authentication and access control **22**
B.2.7 (Audit) Logging **23**
B.2.8 Information Security incident management **23**
B.2.9 Physical security **23**
B.2.10 Personnel security **23**
B.2.11 Appendices **23**
B.2.12 Glossary **23**

Annex C (informative) **ITU-T X.805 framework and ISO/IEC 27001:2005 control mapping** **24**

Bibliography **28**

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2. The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27033-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This first edition of ISO/IEC 27033-2 cancels and replaces ISO/IEC 18028-2:2006, which has been technically revised.

ISO/IEC 27033 consists of the following parts, under the general title *Information technology — Security techniques — Network security*:

— *Part 1: Overview and concepts*

— *Part 2: Guidelines for the design and implementation of network security*

— *Part 3: Reference networking scenarios – Threats, design techniques and control issues*

The following parts are under preparation:

— *Part 4: Securing communications between networks using security gateways*

— *Part 5: Securing communications across networks using Virtual Private Networks (VPNs)*

Securing IP network access using wireless will form the subject of a future Part 6.

Further parts may follow because of the ever-changing and evolving technology in the network security area.

Information technology — Security techniques

Part 2:
Guidelines for the design and implementation of network security

1 Scope

This part of ISO/IEC 27033 gives guidelines for organizations to plan, design, implement and document network security.

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 27005:2011, *Information technology — Security techniques — Information security risk management*

ISO/IEC 27033-1, *Information technology — Security techniques — Network security — Part 1: Overview and concepts*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 7498 (all parts), ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, and ISO/IEC 27033-1 apply.