

---

---

**Information technology — Security  
techniques — Network security —**

**Part 1:  
Overview and concepts**

*Technologies de l'information — Techniques de sécurité — Sécurité  
de réseau —*

*Partie 1: Vue d'ensemble et concepts*



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2015, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
Ch. de Blandonnet 8 • CP 401  
CH-1214 Vernier, Geneva, Switzerland  
Tel. +41 22 749 01 11  
Fax +41 22 749 09 47  
copyright@iso.org  
www.iso.org

# Contents

	Page
<b>Foreword</b> .....	<b>v</b>
<b>Introduction</b> .....	<b>vi</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>2</b>
<b>4 Symbols and abbreviated terms</b> .....	<b>6</b>
<b>5 Structure</b> .....	<b>8</b>
<b>6 Overview</b> .....	<b>10</b>
6.1 Background.....	10
6.2 Network security planning and management.....	11
<b>7 Identifying risks and preparing to identify security controls</b> .....	<b>13</b>
7.1 Introduction.....	13
7.2 Information on current and/or planned networking.....	13
7.2.1 Security requirements in corporate information security policy.....	13
7.2.2 Information on current/planned networking.....	14
7.3 Information security risks and potential control areas.....	18
<b>8 Supporting controls</b> .....	<b>21</b>
8.1 Introduction.....	21
8.2 Management of network security.....	21
8.2.1 Background.....	21
8.2.2 Network security management activities.....	21
8.2.3 Network security roles and responsibilities.....	23
8.2.4 Network monitoring.....	24
8.2.5 Evaluating network security.....	25
8.3 Technical vulnerability management.....	25
8.4 Identification and authentication.....	25
8.5 Network audit logging and monitoring.....	26
8.6 Intrusion detection and prevention.....	27
8.7 Protection against malicious code.....	28
8.8 Cryptographic based services.....	28
8.9 Business continuity management.....	29
<b>9 Guidelines for the design and implementation of network security</b> .....	<b>30</b>
9.1 Background.....	30
9.2 Network technical security architecture/design.....	30
<b>10 Reference network scenarios – Risks, design, techniques and control issues</b> .....	<b>32</b>
10.1 Introduction.....	32
10.2 Internet access services for employees.....	33
10.3 Enhanced collaboration services.....	33
10.4 Business to business services.....	33
10.5 Business to customer services.....	34
10.6 Outsourced services.....	34
10.7 Network segmentation.....	34
10.8 Mobile communication.....	34
10.9 Networking support for travelling users.....	35
10.10 Networking support for home and small business offices.....	35
<b>11 ‘Technology’ topics — Risks, design techniques and control issues</b> .....	<b>35</b>
<b>12 Develop and test security solution</b> .....	<b>36</b>
<b>13 Operate security solution</b> .....	<b>36</b>