

# ISO/IEC 27033-1:2009-12 (E)

## Information technology - Security techniques - Network security - Part 1: Overview and concepts

---

<b>Contents</b>		<b>Page</b>
<b>1</b>	<b>Scope .....</b>	<b>1</b>
<b>2</b>	<b>Normative references .....</b>	<b>2</b>
<b>3</b>	<b>Terms and definitions .....</b>	<b>2</b>
<b>4</b>	<b>Abbreviated terms .....</b>	<b>6</b>
<b>5</b>	<b>Structure .....</b>	<b>9</b>
<b>6</b>	<b>Overview .....</b>	<b>11</b>
<b>6.1</b>	<b>Background .....</b>	<b>11</b>
<b>6.2</b>	<b>Network Security Planning and Management .....</b>	<b>12</b>
<b>7</b>	<b>Identifying Risks and Preparing to Identify Security Controls .....</b>	<b>14</b>
<b>7.1</b>	<b>Introduction .....</b>	<b>14</b>
<b>7.2</b>	<b>Information on Current and/or Planned Networking .....</b>	<b>15</b>
<b>7.3</b>	<b>Information Security Risks and Potential Control Areas .....</b>	<b>19</b>
<b>8</b>	<b>Supporting Controls .....</b>	<b>22</b>
<b>8.1</b>	<b>Introduction .....</b>	<b>22</b>
<b>8.2</b>	<b>Management of Network Security .....</b>	<b>23</b>
<b>8.3</b>	<b>Technical Vulnerability Management .....</b>	<b>26</b>
<b>8.4</b>	<b>Identification and Authentication .....</b>	<b>27</b>
<b>8.5</b>	<b>Network Audit Logging and Monitoring .....</b>	<b>28</b>
<b>8.6</b>	<b>Intrusion Detection and Prevention .....</b>	<b>29</b>
<b>8.7</b>	<b>Protection against Malicious Code .....</b>	<b>29</b>
<b>8.8</b>	<b>Cryptographic Based Services .....</b>	<b>30</b>
<b>8.9</b>	<b>Business Continuity Management .....</b>	<b>31</b>
<b>9</b>	<b>Guidelines for the Design and Implementation of Network Security .....</b>	<b>32</b>
<b>9.1</b>	<b>Background .....</b>	<b>32</b>
<b>9.2</b>	<b>Network Technical Security Architecture/Design .....</b>	<b>32</b>
<b>10</b>	<b>Reference Network Scenarios - Risks, Design, Techniques and Control Issues .....</b>	<b>34</b>
<b>10.1</b>	<b>Introduction .....</b>	<b>34</b>
<b>10.2</b>	<b>Internet Access Services for Employees .....</b>	<b>34</b>
<b>10.3</b>	<b>Enhanced Collaboration Services .....</b>	<b>35</b>
<b>10.4</b>	<b>Business to Business Services .....</b>	<b>35</b>
<b>10.5</b>	<b>Business to Customer Services .....</b>	<b>35</b>
<b>10.6</b>	<b>Outsourcing Services .....</b>	<b>35</b>
<b>10.7</b>	<b>Network Segmentation .....</b>	<b>36</b>
<b>10.8</b>	<b>Mobile Communications .....</b>	<b>36</b>
<b>10.9</b>	<b>Network Support for Traveling Users .....</b>	<b>36</b>
<b>10.10</b>	<b>Network Support for Home and Small Business Offices .....</b>	<b>36</b>
<b>11</b>	<b>'Technology' Topics - Risks, Design Techniques and Control Issues .....</b>	<b>37</b>
<b>12</b>	<b>Develop and Test Security Solution .....</b>	<b>37</b>
<b>13</b>	<b>Operate Security Solution .....</b>	<b>38</b>
<b>14</b>	<b>Monitor and Review Solution Implementation .....</b>	<b>38</b>
<b>Annex A (informative) 'Technology' Topics - Risks, Design Techniques and Control Issues .....</b>		<b>39</b>

<b>Annex B (informative) Cross-references Between ISO/IEC 27001 and ISO/IEC 27002 Network Security Related Controls, and clauses within this part of ISO/IEC 27033 .....</b>	<b>64</b>
<b>Annex C (informative) Example Template for a SecOPs Document .....</b>	<b>69</b>