

---

---

**Information technology — Security  
techniques — Information security  
management — Monitoring,  
measurement, analysis and evaluation**

*Technologies de l'information — Techniques de sécurité —  
Management de la sécurité de l'information —  
Surveillance, mesurage, analyse et évaluation*



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2016, 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>iv</b>
<b>Introduction</b> .....	<b>v</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Structure and overview</b> .....	<b>1</b>
<b>5 Rationale</b> .....	<b>2</b>
5.1 The need for measurement.....	2
5.2 Fulfilling the ISO/IEC 27001 requirements.....	3
5.3 Validity of results.....	3
5.4 Benefits.....	3
<b>6 Characteristics</b> .....	<b>4</b>
6.1 General.....	4
6.2 What to monitor.....	4
6.3 What to measure.....	5
6.4 When to monitor, measure, analyse and evaluate.....	6
6.5 Who will monitor, measure, analyse and evaluate.....	6
<b>7 Types of measures</b> .....	<b>7</b>
7.1 General.....	7
7.2 Performance measures.....	7
7.3 Effectiveness measures.....	8
<b>8 Processes</b> .....	<b>9</b>
8.1 General.....	9
8.2 Identify information needs.....	10
8.3 Create and maintain measures.....	11
8.3.1 General.....	11
8.3.2 Identify current security practices that can support information needs.....	11
8.3.3 Develop or update measures.....	12
8.3.4 Document measures and prioritize for implementation.....	13
8.3.5 Keep management informed and engaged.....	13
8.4 Establish procedures.....	14
8.5 Monitor and measure.....	14
8.6 Analyse results.....	15
8.7 Evaluate information security performance and ISMS effectiveness.....	15
8.8 Review and improve monitoring, measurement, analysis and evaluation processes.....	15
8.9 Retain and communicate documented information.....	15
<b>Annex A (informative) An information security measurement model</b> .....	<b>17</b>
<b>Annex B (informative) Measurement construct examples</b> .....	<b>19</b>
<b>Annex C (informative) An example of free-text form measurement construction</b> .....	<b>57</b>
<b>Bibliography</b> .....	<b>58</b>