

First edition  
2004-10-15

---

---

**Information technology — Security  
techniques — Information security  
incident management**

*Technologies de l'information — Techniques de sécurité — Gestion  
d'incidents de sécurité de l'information*

**PDF disclaimer**

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

© ISO/IEC 2004

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
Case postale 56 • CH-1211 Geneva 20  
Tel. + 41 22 749 01 11  
Fax + 41 22 749 09 47  
E-mail [copyright@iso.org](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

# 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>1</b>
3.1 Business continuity planning .....	1
3.2 Information security event .....	2
3.3 Information security incident .....	2
3.4 ISIRT (Information Security Incident Response Team).....	2
3.5 Other .....	2
<b>4 Background</b> .....	<b>2</b>
4.1 Objectives.....	2
4.2 Processes .....	2
<b>5 Benefits and Key Issues</b> .....	<b>5</b>
5.1 Benefits .....	5
5.2 Key Issues .....	7
<b>6 Examples of Information Security Incidents and their Causes</b> .....	<b>11</b>
6.1 Denial of Service.....	11
6.2 Information Gathering.....	12
6.3 Unauthorized Access.....	13
<b>7 Plan and Prepare</b> .....	<b>13</b>
7.1 Overview .....	13
7.2 Information Security Incident Management Policy .....	14
7.3 Information Security Incident Management Scheme .....	16
7.4 Information Security and Risk Management Policies .....	19
7.5 Establishment of the ISIRT .....	20
7.6 Technical and Other Support.....	21
7.7 Awareness and Training.....	22
<b>8 Use</b> .....	<b>23</b>
8.1 Introduction.....	23
8.2 Overview of Key Processes.....	24
8.3 Detection and Reporting .....	26
8.4 Event/Incident Assessment and Decision.....	27
8.5 Responses.....	30
<b>9 Review</b> .....	<b>36</b>
9.1 Introduction.....	36
9.2 Further Forensic Analysis .....	36
9.3 Lessons Learnt .....	36
9.4 Identification of Security Improvements.....	37
9.5 Identification of Scheme Improvements .....	37
<b>10 Improve</b> .....	<b>37</b>
10.1 Introduction.....	37
10.2 Security Risk Analysis and Management Improvement .....	37
10.3 Make Security Improvements .....	38