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

Part 1:
Principles of incident management

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

Partie 1: Principes de la gestion des incidents



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

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Overview	2
4.1 Basic concepts and principles.....	2
4.2 Objectives of incident management.....	3
4.3 Benefits of a structured approach.....	5
4.4 Adaptability.....	6
5 Phases	6
5.1 Overview.....	6
5.2 Plan and Prepare.....	9
5.3 Detection and Reporting.....	9
5.4 Assessment and Decision.....	10
5.5 Responses.....	11
5.6 Lessons Learnt.....	12
Annex A (informative) Relationship to investigative standards	13
Annex B (informative) Examples of information security incidents and their causes	16
Annex C (informative) Cross reference table of ISO/IEC 27001 to ISO/IEC 27035	19
Bibliography	21