
**Information technology — Guidelines for
the management of IT Security —**

Part 3:
Techniques for the management of IT Security

*Technologies de l'information — Lignes directrices pour la gestion de
sécurité IT —*

Partie 3: Techniques pour la gestion de sécurité IT

Contents

1 Scope	1
2 References	1
3 Definitions	1
4 Structure	1
5 Aim	1
6 Techniques for the Management of IT Security	2
7 IT Security Objectives, Strategy and Policies	3
7.1 IT Security Objectives and Strategy	4
7.2 Corporate IT Security Policy	5
8 Corporate Risk Analysis Strategy Options	7
8.1 Baseline Approach	7
8.2 Informal Approach	8
8.3 Detailed Risk Analysis	8
8.4 Combined Approach	9
9 Combined Approach	10
9.1 High Level Risk Analysis	10
9.2 Baseline Approach	10
9.3 Detailed Risk Analysis	11
9.3.1 Establishment of Review Boundary	12
9.3.2 Identification of Assets	13
9.3.3 Valuation of Assets and Establishment of Dependencies Between Assets	13
9.3.4 Threat Assessment	14
9.3.5 Vulnerability Assessment	15
9.3.6 Identification of Existing/Planned Safeguards	16
9.3.7 Assessment of Risks	17
9.4 Selection of Safeguards	17
9.4.1 Identification of Safeguards	17
9.4.2 IT Security Architecture	19
9.4.3 Identification/Review of Constraints	20
9.5 Risk Acceptance	21
9.6 IT System Security Policy	21
9.7 IT Security Plan	22
10 Implementation of the IT Security Plan	23
10.1 Implementation of Safeguards	23
10.2 Security Awareness	24
10.2.1 Needs Analysis	25
10.2.2 Programme Delivery	25
10.2.3 Monitoring of Security Awareness Programmes	25
10.3 Security Training	26
10.4 Approval of IT Systems	27
11 Follow-up	28
11.1 Maintenance	28
11.2 Security Compliance Checking	28

© ISO/IEC 1998

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 the publisher.

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland