

BS ISO/IEC 27031:2011



BSI Standards Publication

Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity

bsi.

...making excellence a habit.™

This is a preview. [Click here to purchase the full publication.](#)

National foreword

This British Standard is the UK implementation of ISO/IEC 27031:2011. It supersedes BS 25777:2008 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT - Security techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© BSI 2011

ISBN 978 0 580 59426 7

ICS 03.100.01; 35.020; 35.040

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 March 2011.

Amendments issued since publication

Date	Text affected
------	---------------

**Information technology — Security
techniques — Guidelines for information
and communication technology
readiness for business continuity**

*Technologies de l'information — Techniques de sécurité — Lignes
directrices pour mise en état des technologies de la communication et
de l'information pour continuité des affaires*

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.



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2011

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
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword	v
Introduction.....	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Abbreviations.....	3
5 Overview.....	3
5.1 The role of IRBC in Business Continuity Management	3
5.2 The Principles of IRBC	5
5.3 The Elements of IRBC	6
5.4 Outcomes and benefits of IRBC	7
5.5 Establishing IRBC	7
5.6 Using Plan Do Check Act to establish IRBC.....	8
5.7 Management Responsibility	8
5.7.1 Management leadership and commitment.....	8
5.7.2 IRBC policy	8
6 IRBC Planning.....	9
6.1 General	9
6.2 Resources	9
6.2.1 General	9
6.2.2 Competency of IRBC staff	9
6.3 Defining requirements	10
6.3.1 General	10
6.3.2 Understanding critical ICT services	10
6.3.3 Identifying gaps between ICT Readiness capabilities and business continuity requirements.....	10
6.4 Determining IRBC Strategy Options.....	11
6.4.1 General	11
6.4.2 IRBC Strategy Options.....	11
6.5 Sign Off.....	14
6.6 Enhancing IRBC Capability	14
6.6.1 Enhancing Resilience	14
6.7 ICT Readiness Performance Criteria	15
6.7.1 Identification of performance criteria	15
7 Implementation and Operation	15
7.1 General	15
7.2 Implementing the Elements of the IRBC Strategies	15
7.2.1 Awareness, Skills and Knowledge	15
7.2.2 Facilities	16
7.2.3 Technology	16
7.2.4 Data	16
7.2.5 Processes.....	17
7.2.6 Suppliers	17
7.3 Incident Response.....	17
7.4 IRBC Plan Documents.....	17
7.4.1 General	17
7.4.2 Content of Plan Documents	18
7.4.3 The ICT Response and Recovery Plan Documentation	19

7.5	Awareness, competency and training program	20
7.6	Document Control.....	21
7.6.1	Control of IRBC records.....	21
7.6.2	Control of IRBC documentation	21
8	Monitor and Review	21
8.1	Maintaining IRBC	21
8.1.1	General.....	21
8.1.2	Monitoring, detection and analysis of threats	22
8.1.3	Test and exercise.....	22
8.2	IRBC Internal Audit.....	26
8.3	Management Review	26
8.3.1	General.....	26
8.3.2	Review Input.....	27
8.3.3	Review Output.....	27
8.4	Measurement of ICT Readiness Performance Criteria.....	28
8.4.1	Monitoring and measurement of ICT Readiness	28
8.4.2	Quantitative and Qualitative Performance Criteria	28
9	IRBC improvement.....	28
9.1	Continual improvement.....	28
9.2	Corrective action.....	28
9.3	Preventive action	29
Annex A	(informative) IRBC and milestones during a disruption	30
Annex B	(informative) High availability embedded system	32
Annex C	(informative) Assessing Failure Scenarios	33
Annex D	(informative) Developing Performance Criteria	35
Bibliography		36