ISO/IEC 27031:2025-05 (E)

Cybersecurity - Information and communication technology readiness for business continuity

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Abbreviated terms 3

5 Structure of this document 3
5.1 General 3

6 Integration of IRBC into BCM 3
6.1 General 3
6.2 Enabling governance 4
6.3 Business continuity management objectives 5
6.4 Risk management and applicable controls for IRBC 6
6.5 Incident management and relationship to IRBC 6
6.6 BCM strategies and alignment to IRBC 6

7 Business expectations for IRBC 7
7.1 Risk review 7
7.1.1 General 7
7.1.2 Monitoring, detection and analysis of threats and events 8
7.2 Inputs from business impact analysis 8
7.2.1 General 8
7.2.2 Understanding critical ICT services 8
7.2.3 Assessing ICT readiness against business continuity requirements 9
7.3 Coverage and interfaces 9
7.3.1 General 9
7.3.2 ICT dependencies for the scope 10
7.3.3 Determine any contractual aspects of dependencies 10

8 DefiningprerequisitesforIRBC 10
8.1 Incident based - preparation before incident 10
8.1.1 General 10
8.1.2 ICT Recovery capabilities 11
8.1.3 Establishing an IRBC 11
8.1.4 Setting objectives 11
8.1.5 Determining possible outcomes and benefits of IRBC 12
8.1.6 Equipment redundancy planning 13
8.1.7 Determining the scope of ICT services related to the objectives 13
8.2 Determining target ICT RTO and RPO 14

9 Determining IRBC strategies 15
9.1 General 15
9.2 IRBC strategy options 15
9.2.1 General 15

9.2.2 Skills and knowledge ... 16
9.2.3 Facilities ... 16
9.2.4 Technology ... 17
9.2.5 Data ... 17
9.2.6 Processes ... 18
9.2.7 Suppliers ... 18

10 Determining the ICT continuity plan ... 19
10.1 Prerequisites for the development of plans ... 19
10.1.1 Determining and setting the recovery organization ... 19
10.1.2 Determining time frames for plan development, reporting and testing ... 19

10.1.3 Resources ... 20
10.1.4 Competency of IRBC staff ... 20
10.1.5 Technological solutions ... 21
10.2 Recovery plan activation ... 21
10.2.1 ICT BCP Activation ... 21
10.2.2 Escalation ... 21
10.3 ICT recovery plans ... 22
10.3.1 RPO and RTO plans for ICT ... 22
10.3.2 Facilities ... 22
10.3.3 Technology ... 22
10.3.4 Data ... 22
10.3.5 Response and recovery procedures ... 23
10.3.6 People ... 23
10.4 Temporary work around plans ... 23
10.5 External contacts and procedures ... 23

11 Testing, exercise, and auditing ... 23
11.1 Performance criteria ... 23
11.2 Testing dependencies ... 24
11.2.1 Test and exercise ... 24
11.2.2 Test and exercise program ... 24
11.2.3 Scope of exercises ... 25
11.2.4 Planning an exercise ... 25
11.2.5 Alert based and different recovery stages ... 26
11.2.6 Managing an exercise ... 27
11.3 Learning from tests ... 28
11.4 Auditing the IRBC ... 28
11.5 Control of documented information ... 29

12 Final MBCO ... 29

13 Top management responsibilities regarding evaluating the IRBC ... 29
13.1 General ... 29
13.2 Management responsibilities ... 29

Annex A (informative) Comparing RTO and RPO to business objectives for ICT recovery ... 31

Annex B (informative) Risk reporting for FMEA ... 32

Bibliography ... 33