

# ISO/IEC 27031:2011-03 (E)

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

---

<b>Contents</b>		<b>Page</b>
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