



国际标准

ISO/IEC 27031

网络安全--信息和通信技术为业务连续性做好准备

网络安全——信息技术与通信技术的准备，以确保业务连续性

第二版

2025-05-16



受版权保护的文件

© ISO/IEC 2025

保留所有权利。除非另有规定或在实施过程中需要，否则未经事先书面许可，不得以任何形式或手段复制或使本出版物的任何部分，包括电子或机械方式，如复印，或在互联网或内联网上发布。如需获得许可，可向ISO或ISO成员国的成员机构申请。

ISO版权办公室

邮编4012布兰东内特街8号

CH-1214 Vernier, 日内瓦

电话：+41 22 749 01 11

电子邮箱：copyright@iso.org

网 站：www.iso.org

瑞士出版

目录

页

前言	v
介绍	vi
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	3
5 本文件的结构	3
5.1 将军	3
6 将IRBC集成到BCM中	3
6.1 将军	3
6.2 促进施政	4
6.3 业务连续性管理目标	5
6.4 IRBC的风险管理和适用控制措施	6
6.5 突发事件管理及其与IRBC的关系	6
6.6 BCM战略和与IRBC的协调	6
7 IRBC的业务预期	7
7.1 风险审查	7
7.1.1 将军	7
7.1.2 监测、检测和分析威胁和事件	8
7.2 业务影响分析的输入	8
7.2.1 将军	8
7.2.2 了解关键信通技术服务	8
7.2.3 根据业务连续性要求评估信通技术就绪情况	9
7.3 覆盖范围和接口	9
7.3.1 将军	9
7.3.2 信息技术依存范围	10
7.3.3 确定任何合同方面的依赖关系	10
8 定义IRBC的先决条件	10
8.1 基于事件的一事件前准备	10
8.1.1 将军	10
8.1.2 ICT恢复能力	11
8.1.3 建立IRBC	11
8.1.4 设定目标	11
8.1.5 确定IRBC的可能结果和受益	12
8.1.6 设备冗余规划	13
8.1.7 确定与目标有关的信息和通信技术服务的范围	13
8.2 确定目标ICT RTO和RPO	14
9 确定IRBC策略	15
9.1 将军	15
9.2 IRBC战略选项	15
9.2.1 将军	15
9.2.2 技能和知识	16
9.2.3 设施	16
9.2.4 技术	17
9.2.5 数据	17

	9.2.6 过程.....	18
	9.2.7 供应商.....	18
10	确定信通技术连续性计划.....	19
10.1	制定计划的先决条件.....	19
10.1.1	确定和设置恢复组织.....	19
10.1.2	确定计划开发、报告和测试的时间框架.....	19

©ISO/IEC 2025-保留所有权利

10.1.3	资源	20
10.1.4	IRBC工作人员的能力	20
10.1.5	技术解决方案	21
10.2	恢复计划激活	21
10.2.1	ICT BCP激活	21
10.2.2	升级	21
10.3	信息和通信技术恢复计划	22
10.3.1	针对ICT的RPO和RTO计划	22
10.3.2	设施	22
10.3.3	技术	22
10.3.4	数据	22
10.3.5	响应和恢复程序	23
10.3.6	人民	23
10.4	临时变通计划	23
10.5	外部联系和程序	23
11	测试、演习和审计	23
11.1	业绩标准	23
11.2	测试依赖项	24
11.2.1	测试和演习	24
11.2.2	测试和演习计划	24
11.2.3	演习范围	25
11.2.4	计划一次演习	25
11.2.5	基于警报和不同恢复阶段	26
11.2.6	管理锻炼	27
11.3	从测试中学习	28
11.4	对IRBC的审计	28
11.5	文件化信息的控制	29
12	最终MBCO	29
13	最高管理层负责评价IRBC	29
13.1	将军	29
13.2	管理职责	29
附录A (参考)	将RTO和RPO与ICT恢复的业务目标进行比较	31
附录B (参考)	FMEA的风险报告	32
参考文献		33

注：本文件内容受到版权保护，未经恰当的授权禁止复制。本公司客户及相关单位，如需获取文件完整内容，请联系市场部门获取，电话：010-84724911。