TLD-OPS BCP/DR 行动手册

第 1.0.2 版

2019 年 12 月 3 日

目录

内容

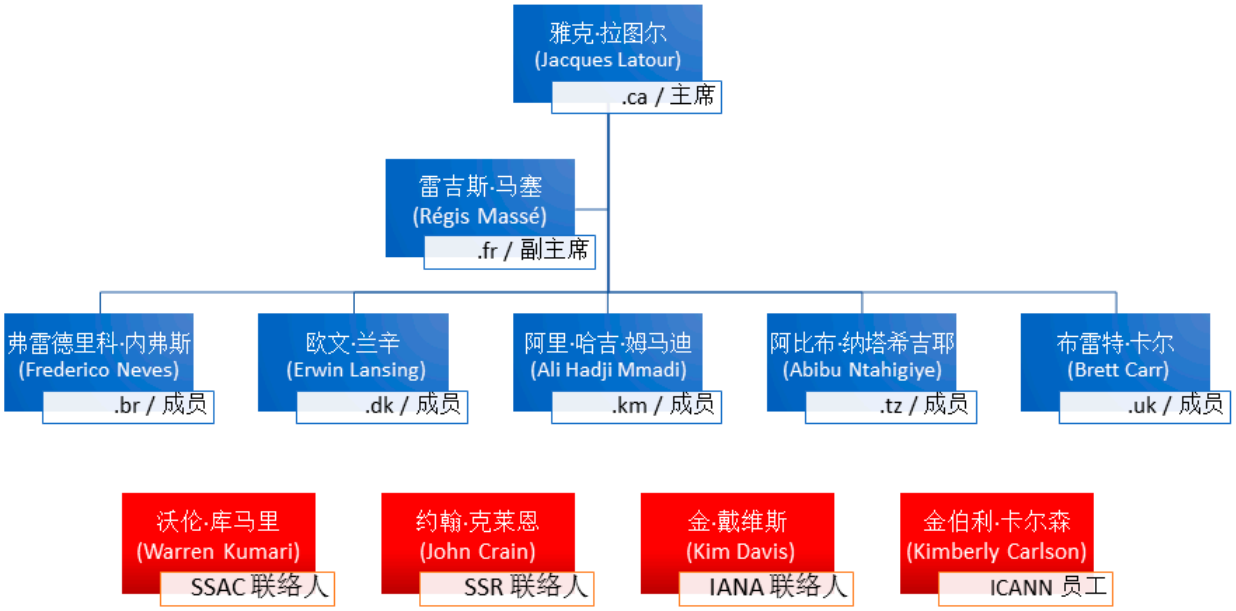
简介

关于 TLD-OPS：ccTLD 安全和稳定

顶级域运营 (TLD-OPS) 是为 ccTLD 设立的事件响应社群，由 ccTLD 管理，汇集了负责各自 ccTLD 的运营安全和稳定的人员。TLD-OPS 社群的目标是帮助全球的 ccTLD 运营商检测并缓和可能影响 ccTLD 服务安全和稳定的事件，例如 DDoS 攻击、恶意软件感染和网络钓鱼攻击。TLD-OPS 旨在进一步扩展成员的现有事件响应结构、流程和工具，而非替代它们。TLD-OPS 面向每一个 ccTLD 开放，无论其是否属于 ccNSO 成员。

有关信息，请参阅：https://ccnso.icann.org/en/resources/tld-ops-secure-communication.htm

特别感谢欧洲互联网域名注册管理机构 (EURid) 安全经理德克 • 朱珀茨 (Dirk Jumpertz) 先生对本文件和项目做出的突出贡献。



TLD-OPS 常任委员会

如何使用本文件

本行动手册旨在为任何希望在较小的注册管理运行机构内实施业务连续性战略的人员提供实践指南。其目标受众主要为高层和/或中层管理人员。本文件假定注册管理运行机构由监管机构（无论是董事会、政府代表机构还是任何其他实体）向其做出承诺、提供赞助并下达使命，通过执行业务连续性计划来提高抵御破坏性事件的能力。

为尽可能确保切实可用，本文件包含了许多实用示例表，可供用户在开发和实施的不同阶段复制和使用。

不仅如此，本文件还列举了一些示例，可为制定业务连续性/灾难恢复计划提供模板或灵感。

最后，读者会发现本文件中偶尔出现“行动框”，其中包含可实施的建议和提示：对某项活动的简要说明以及这项活动的执行者。

什么是业务连续性？

业务连续性是指一个组织在遭受破坏性事件后，能够在可接受的预定义级别继续交付对 ccTLD 注册管理运行机构业务和利益相关方重要的产品或服务。

请注意，业务连续性并不一定只关注技术破坏性事件。任何影响组织运营就绪状态的破坏性事件都可能会触发业务连续性计划。因此，对于一个组织来说，了解哪些事件会妨碍运营就绪状态至关重要。

业务连续性与灾难恢复

业务连续性计划 (BCP) 和灾难恢复计划 (DRP) 密切相关但不可互换。例如，通过 Google 查找模板时会发现两者存在相似之处，即便如此，它们也不可互换。前者包含的是侧重于在危机期间提供常规业务的行动计划；而后者则是一个子集，包含的是在尽可能最短的时间内恢复业务所需的重要系统的程序。

换句话说，业务连续性计划将会引用许多灾难恢复计划。就本文件而言，我们将制定业务连续性计划，其中包含针对特定场景的行动计划。

如何实现这一目标？

通过使用关于业务连续性的 ISO 22301 标准的一些指导，用户可以制定一个有助于创建、管理和改进业务连续性计划的全局框架。

由于域名经理人在 ccTLD 领域的运营使命大致相同，因此他们可以使用一种通用的简单方法，与复杂、耗时且有时抽象的技术相比，该方法注重实用性，更适用于制定正确的业务连续性计划。

与 ISO/IEC 27001:2013 标准的关系

ISO 27001 标准关注信息安全，重点强调开发、实施、监控和改进控制措施，以保持机密性、完整性和可用性（简称 CIA）水平。对于一家 IT 服务公司来说，这与业务连续性存在较多共同之处。

但两者之间有一点不同：ISO/IEC 27001 侧重于在正常运营期间达到所需的机密性、完整性和可用性水平，并通过技术和程序预测必需的缓和措施；而 ISO 22301 则关注影响组织运营能力的破坏性事件，并拟定应对这些事件的计划。

要了解 ISMS（信息安全管理系统）和 BCMS（业务连续性管理系统）之间的区别，请参阅下面列举的一些示例：

- *通常引入具有 RAID 保护和复制功能的冗余存储来提高完整性和可用性 (ISO/IEC 27001)。*
- *组织消防演习，确保在真正发生火灾时能够正确应对，将人员伤亡降到最低 (ISO 22301)。*
- *部署防病毒端点防护系统，以便保护笔记本电脑、台式电脑和移动设备免受网络威胁 (ISO/IEC 27001)。*
- *另一方面，启动演练程序以防遭受勒索软件的攻击，演练程序属于业务连续性计划的一部分 (ISO 22301)。*

（本文件的）范围

本文件是一个指南，旨在帮助小型注册管理运行机构实施基本的业务连续性和灾难恢复措施。

本文件应该有助于回答以下问题：

- 如何确定业务连续性范围？
- 如何确定风险？
- 如何在公司 DNA 中嵌入业务连续性？
- 有效的业务连续性战略需要具备哪些因素？
- 重要材料是指什么？
- 如何起草业务连续性计划或灾难恢复计划？
- 如何实施业务连续性措施？
- 如何加以改进？

规范性参考文献

本文件的依据是：

- ISO 22301:2012 – 社会安全 – 业务连续性管理系统 – 要求。
- ISO 31000:2009 – 风险管理 – 原则和指导方针。
- ISO/IEC 27001:2013 – 信息技术 – 安全技术 – 信息安全管理系统 – 要求。

术语和定义

有关本文件中使用的术语和定义，请参阅 ISO 22301:2012 标准。

请参阅 RFC2119 以了解不同要求级别。

组织的背景

尽管大多数 ccTLD 提供的服务和履行的使命都非常相似，但它们仍存在较大差异，这些差异将会为业务连续性战略指明方向。总的来说，大多数 ccTLD 的运营使命包括：

- 管理其顶级域 (TLD) 的域名服务器基础设施。

- 管理对 ccTLD 至关重要的公共服务。更具体地说，公共服务是指公司网站，以及诸如 WHOIS 或 RDAP 之类的管理查询服务。
- 管理某种注册服务，允许直接或间接注册域名。例如，注册服务可以是像网站一样的人机界面，也可以是像 EPP 一样的专用计算机对计算机界面。
- 最后但也很重要的一项使命是，注册管理机构将管理许多企业业务支持系统，这些系统可能并不对外开放，但对组织的运营至关重要（例如电子邮件、内部网、文件服务器等）。

这一首要步骤的目的在于了解依赖组织的对象、在发生破坏性事件期间需要达到的预期，以及组织要求履行其使命的对象。

了解组织及其背景

制定有效业务连续性战略的第一个简单步骤是全面了解业务及其利益相关方。利益相关方将会设定具体的预期、要求，并制定在业务范围内需要考虑的义务。因此，最佳做法是先列出各个利益相关方，其次对他们进行描述，最后审核他们对运营灵活性和业务连续性的预期。这项活动最好由管理层完成，这样才能获取有效的意见。“与 BC 的相关性”一列指示预期与业务连续性的关系。有些预期可能与业务连续性毫不相关；而其他一些预期则可能非常重要。对于这种情况，可以使用“高”、“中”、“低”和“不适用”来表示相关性。例如，如果认为某个预期与业务连续性高度相关，这基本上意味着利益相关方具有较高的预期。在实际情况中，利益相关方可能期望“它始终运行”，这意味着 DNS 始终处于运行状态；那么其与 BC 的相关性将会很高。

尽管下表中所列的内容并不详尽，但其中有一些**示例**有助于完成这项活动。在实际情况中，建议组织按照如下步骤完成这项活动：首先查看并更新表格，确定利益相关方，列出他们的名称（便于访谈）；其次，考虑使用简短的语句表述预期；最后，评估这些预期与业务连续性的相关性。

利益相关方	**预期**	**与 BC 的相关性**
政府	100% DNS 可用性 注册管理机构准确性和完整性 注册管理机构系统可用性 DNS 专业技术中心 DNS 的研发 域名滥用	高 高 高 不适用 不适用 不适用
ICANN	IANA ccTLD 注册	不适用

董事会	100% DNS 可用性 注册管理机构准确性和完整性 公司系统可用性	高 高 中
公众	DNS 可用性 域名注册可用性	高 高
c-CERT	信息安全 对注册人数据的访问	低 不适用
员工	公司系统可用性	高
执法机构	域名注册完整性	低
注册服务机构	域名注册可用性	中
注册人	域名解决方案可用性 域名注册完整性	低 低
本地 ISP	域名解决方案 DNSSEC 支持	高 不适用
解析器社群	对区域文件的访问	不适用

表 1

此类列表将有助于确定在业务连续性方面具有高优先级的事项。

供应链

在现代企业中，组织依赖于许多合作伙伴、供应商、服务提供商等。这些实体显然对业务连续性战略具有重要影响，因此应该了解组织对供应链的依赖程度。组织需要列出会对其运营使命产生影响的所有供应商，这是一项不可或缺的重要活动。

组织可以通过询问财务部，快速获取所有供应商的名单，创建一个供应商列表，同时还应简要描述这些供应商实际提供的产品和服务。从该列表中，我们可以确定哪些供应商对组织运营弹性具有实际影响。例如，数据中心提供商显然与业务连续性高度相关；而像“宜家”这样的家具供应商与业务连续性的相关性则较低。

根据供应商事件开始产生影响的时间长短，我们可以使用不同的影响标签：

影响	**开始产生影响的时间**
严重	即时
较大影响	一周或 7 天内
中等影响	一个月或 30 天内
较小影响	超过一个月或 30 天

表 2

下表是帮助创建此供应商列表的**示例**：

供应商（名称）	**描述**	**与 BC 的相关性**	**影响**
ISP	互联网服务提供商	高	严重
信用卡处理商	促进商户和持卡人银行之间沟通的实体	中 - 高	较大影响
电话公司	固定电话提供商	中	中等影响
邮政服务	邮政（邮件）提供商	低	低
电力公司	恢复供电		
薪给公司	支付员工工资		
计算机服务公司	为员工购买台式机，为提供服务购买服务器		
网络/ISP 提供商			
移动网络运营商			
保险公司			

表 3

确定业务连续性的范围

运营连续性是 BC 战略的基石

运营连续性包括维持“业务正常运营”需要开展的所有活动。这意味着组织需要从技术、商业和法律角度为注册服务机构、注册人和公众等利益相关方提供支持。此外，这还意味着组织需要运行所有技术服务来注册和管理域名、提供业务支持，最后但也很重要的一点是需要确保 TLD 域名空间可供所有互联网用户使用。

大部分技术影响应通过标准工程实践来处理，因此，业务连续性侧重于评估破坏性事件清单，以及这些事件对运营就绪状态带来的假定和估计结果。业务连续性会通过政策、程序和必要的技术来确定缓和措施。

因此，业务连续性的范围可以概括为

> 通过政策、程序、测试和技术管理**预防**和**纠正**措施，以保证在应对**技术**和**非技术**性质的**破坏性**事件时**运营就绪状态和运营连续性**不受影响。

领导层

制定和维护行之有效的业务连续性战略是一项长期工作，需要获得最高管理层的支持。为此，管理团队（甚至董事会）需要为业务连续性相关活动提供帮助和支持。

管理层不仅需要定期审核业务连续性计划，更新该计划，并保持其相关性，还应主动将业务连续性嵌入所有运营层面（技术、工程、采购、运营等）。

行动：管理团队至少每年实施一次审核并进行监控。

规划

本节回答了如何制定切实可行的业务连续性计划的相关问题，该计划会考虑与注册管理运行机构相关的威胁和漏洞，以及对组织运营弹性产生的影响。

我们需要先创建一个威胁/危害登记表，帮助我们确定需要解决哪些领域的业务连续性问题。请注意，有些威胁很难（但并非不可能）缓和或预防。我们需要调查威胁并评估战略选项。这些措施可能不会成为业务连续性计划的一部分，但从长期来看，它们会成为战略选项[1]。

倘若实际出现这些威胁和危害，在处理它们之前，我们需要先了解这些威胁和危害对运营就绪状态和弹性的影响。我们可以使用简化的风险评估方法来帮助确定应当解决的场景问题。根据该评估结果，许多场景问题将纳入业务连续性策略计划中，还有其他一些场景问题则将纳入业务连续性战略中，该战略可供监管机构参考，为制定进一步战略决策提供指导。

一旦明确哪些威胁/危害需要实施实际的业务连续性计划，就可以根据通用模板创建相应计划。之后，所有部门在需要准备程序时都应将这个模板用作指导。

创建威胁/危害登记表

威胁/危害登记表列出了可能对组织的运营弹性产生巨大影响的灾难来源，这个列表极为重要。以下威胁列表基于《业务连续性管理》（第 4 版，ISBN 978-1-931332-35-4）一书，随着最近各种事件层出不穷，该列表的内容会不断扩充。

在评估这些威胁时，组织应根据可用的统计数据来估测事件发生的可能性。事件发生的几率（可能性）分为以下几类：

1. 极有可能： 一年一次或更频繁地重复发生的事件
2. 可能： 平均每三年发生一次的事件
3. 罕见： 每十年发生一次的事件
4. 不太可能： 每 50 年或更长时间发生一次的事件
5. OoS： 超出范围 – 不纳入业务连续性考虑范围的事件

可能性不基于内部统计数据，而是以区域、国家和地区、业务和环境[2]的相关统计数据为依据。在当前采取安全控制措施的情况下，人们必须对风险的可能性（表 7 和表 8）和影响（表 6）进行评分，强调这一点很重要。威胁基于统计数据；目前未采取具体的控制措施。

[1] 一个典型示例是，政治不稳定这个问题可能极难缓和，但作为 ccTLD，应务必在整体业务连续性战略中考虑到这一点。

[2] 一个与天气有关的事件的典型示例是，龙卷风可能与美国部分地区高度相关，但与美国其他地区完全无关。

威胁类别	威胁	适用	可能性
自然灾害	火灾	☐	_____
	洪涝	☐	_____
	飓风/龙卷风/台风	☐	_____
	恶劣天气	☐	_____
	地震	☐	_____
	山体滑坡/雪崩	☐	_____
	火山喷发	☐	_____
	海啸	☐	_____
	雷击沉降污染	☐	_____
	虫患	☐	_____
	鼠患	☐	_____
	_____	☐	_____
人力资源和医疗	关键人员流失	☐	_____
	流行疾病	☐	_____
	技能/人员短缺	☐	_____
	家庭琐事	☐	_____
	偷窃	☐	_____
	恶意破坏（毁坏）	☐	_____
	勒索	☐	_____
	_____		
网络	DDOS	☐	_____
	黑客入侵	☐	_____
	数据丢失	☐	_____
	勒索软件	☐	_____
	网络战争相关活动	☐	_____
	_____	☐	_____
外部	经济衰退	☐	_____
	公民非暴力反抗活动	☐	_____
	恐怖活动	☐	_____
	战争/侵略	☐	_____
	政治干预/政策变更	☐	_____
	入室盗窃	☐	_____
	技术变革/相关活动	☐	_____
	_____	☐	_____
财务	现金流/流动资产问题	☐	_____
	资本匮乏	☐	_____
	金融渎职行为	☐	_____
	坏账	☐	_____
	利率风险	☐	_____
	汇率风险	☐	_____
		☐	_____

	国债敞口风险	☐	_____
技术和基础设施	网络故障 – 全球	☐	_____
	电力 – 电网故障	☐	_____
	交流电故障	☐	_____
	数据中心故障	☐	_____
	组件故障 [3]	☐	_____
		☐	_____
供应故障	服务级别故障	☐	_____
	质量缺陷	☐	_____
	供应服务中断	☐	_____
	外包失败/供应合同缺货情况	☐	_____
	其他关键资产损失	☐	_____
	供应商套牢	☐	_____
		☐	_____
		☐	_____

表 4

根据以上列表，我们得知一点：注册管理运行机构不应只关注与其所在地区和业务环境相关的威胁；以上列表的内容并不详尽，只用作参考示例。这个列表同样只列举了一部分威胁/危害，后续会不断扩充。

行动：BC 协调员或经理可能希望关注已知的威胁和/或危害， 并根据定期审核的结果不断扩充威胁和/或危害。

风险评估和管理

什么是风险？风险类型

在 ISO 31000 标准中，风险的定义是：“对目标产生的不确定影响”,这是一个非常通用的概括性抽象定义。倘若风险涉及业务连续性、运营弹性和连续性，其定义将变为：“破坏性事件对 ccTLD 注册管理运行机构的运营使命产生的影响”。

如果您倾向于进行正式但简单的风险评估，可以使用下表：

[3] 组件故障是指出现故障的计算机系统、电源、计算机内存、磁盘等的总称；您可以决定将其纳入业务连续性的范围，也可以假定默认情况下在基础设施的设计和架构（即冗余电源、RAID 磁盘系统、服务器中的 ECC 内存等）中此风险能够得以缓和。

风险	描述
财务	事件会给组织造成直接和间接成本损失。根据组织的财务稳定性，某些财务损失是可以接受的。
运营	事件会妨碍组织履行其运营使命（例如域名服务中断）。
声誉	事件可能会造成声誉损害，对运营使命产生直接或间接影响。
法律	事件会引发法律问题，从而导致相关人员受到处罚甚至被刑事定罪。
治理	事件会引发政治分歧和不合规行为，从而导致特许合同终止或政治干预。
人员	事件会对员工（或其家属）造成人身伤害。

表 5

每种风险都分为多个级别，根据级别的不同，我们可以决定在业务连续性计划中是否将其考虑在内。示例：

- 1 百万欧元的财务损失可能导致注册管理运行机构面临破产。
- 导致相关个人面临刑事指控的事件可能是注册管理运行机构无法接受的。
- 对员工造成人身伤害的事件可能无法接受。

该表所列的内容并不详尽，注册管理运行机构可以根据具体风险级别决定要采取的措施。下表说明了每种风险类型对应的五个风险级别。至于这些风险级别是否适用以及实际值是多少，取决于注册管理运行机构。

类型	无或不适用	低	中	高	严重
财务	风险不存在或不适用	< 1,000 美元	< 10,000 美元	< 100,000 美元	> 100,000 美元
运营		影响个人	影响部门	影响注册管理机构	影响公众
声誉		内部	用户组（ICANN、CENTR）	公众	媒体/政治
法律		行政处罚	罚款 < 10,000 美元	罚款 < 100,000 美元	罚款 > 100,000 美元、承担个人责任

					或面临刑事指控
治理 [4]		董事会	地方政府	政治审查	注册管理机构停业
人员		级别未使用	级别未使用	员工家庭	人身伤害

表 6

建议使用不同的颜色对各个风险级别进行标注，以供在日后创建所有适用风险与出现风险的可视化热图时使用。

简单风险评估/业务影响评估

将上述不同风险添加到威胁/危害列表中，有助于组织直观了解这些风险对业务产生的影响。

我们来举例说明这一点。以下场景以对 ccTLD 运营基础设施的 DDOS 攻击为例（包括但不限于 .tld 域名服务器以及注册服务；我们假定注册管理运行机构的基础设施占用空间较小，所有服务都合并在一起，且没有为 DNS 使用任播提供商）。

威胁类别	**威胁**	**适用（是/否）**	**可能性**
网络	DDOS	是	极有可能
风险	**级别**		
财务	中	DDOS 攻击不会造成任何直接成本损失，因为它不会对财产造成任何实际损坏。主要成本损失在于处理事件所需的人力成本。另外，在受到攻击时不能注册域名，当然这属于造成的间接成本损失。	
运营	严重	整个 .TLD 不可用或间歇性可用。这对互联网的运营有着巨大影响。同样，公司网站、公共 WHOIS 和其他注册服务等也会受到影响。	
声誉	高/严重	事件将会受到所有互联网用户的关注。	

[4] 治理风险可能最难处理，同时也是最特殊的风险类型。对于一些注册管理机构来说，这种风险甚至可能不存在。在处理这种风险时，管理层需要先明确定义并说明注册管理机构对外部影响的依赖程度。

法律	高	事件发生后，注册人和注册服务机构可能对各自的收入损失提出投诉。（这取决于注册管理机构的 T&C 及其管辖权。）
治理	高	由于大多数 ccTLD 可以被视为基本服务运营商（引用欧盟 NIS 指令），因此可以肯定的是，政府将会对事件展开相关调查。
人员	无	事件不会直接或间接对任何员工造成人身伤害。
RTO	对于 DNS 为零；服务永远不得停止工作。受 DDOS 影响的所有其他服务应在一个工作日内恢复可用。	
RPO	对于 DNS：可以将服务降级到域名服务器容量的 50%；所有其他服务应当完全可访问，容量降级最多可接受 50%。	

表 7

RTO（恢复时间目标）定义了应恢复服务的速度。这反映了利益相关方的预期和/或组织应履行的法律或合同义务。请注意，可以为一种威胁或危害定义不同的 RTO，具体如何指定，取决于受影响的服务。

RPO（恢复点目标）说明了应将服务恢复到的级别。恢复服务的方式多种多样，例如缩减容量（减少可用的域名服务器、缩减服务器容量等）、延迟服务、将数据恢复到某一点，等等。

RTO 和 RPO 应完全以业务投入为依据，而不应依赖于事件发生时“可能采取的措施”。

这项评估为我们指明了方向，即我们应考虑威胁，并需要进行风险处理。

风险偏好和处理

处理风险的方法大致包括以下 5 种：

1. 接受风险（不采取任何行动）。
2. 规避风险（想出一个替代计划）。
3. 降低风险（更改运营模式）。
4. 控制风险（将影响降到最低）。
5. 转移风险（将风险转给他人，比如购买保险）。

业务连续性计划主要采取第 4 种方法，即通过预定义行动来控制影响，并将运营使命恢复到预定义的级别。

另一方面，业务连续性计划还应考虑业务影响评估的结果，因为该评估结果可能会需要您采取预备步骤（步骤 3，降低风险）和行动来降低风险并实现 RTO 和 RPO。

我们来回顾一下前面的示例，研究如何将风险降低到可接受的级别。

在这种特殊情况下，风险处理排序一目了然，DNS 拥有绝对优先权，排在第一位；诸如公司网站和公共 WHOIS 职能等公共服务排在第二位，排在最后但也很重要的是注册服务。

威胁类别	**威胁**	**适用（是/否）**	**可能性**
网络	DDOS	是	极有可能
风险缓和			
接受风险	不适用		
规避风险	不太可能，因为 DDOS 攻击由未知的对手发起。		
降低风险	现有的基础设施将无法保证组织满足预期的 RTO/RPO 要求。一种可行的解决方案是，为 DNS 使用任播解决方案和/或为其他服务使用清理服务		
控制风险	制定 DDOS 业务连续性计划（参考 ccNSO DDOS 缓和手册），包括其他技术措施（如临时调整某些服务）、沟通计划和支持计划		
转移风险	不适用		

表 8

风险处理计划将包含上表中提到的各项行动。有些行动可以立即实施，而其他一些行动则可能需要额外预算、获得进一步批准和重新规划才能得以实施。

风险处理计划

在进行初始风险评估/业务影响评估时，许多场景可能会导致出现不可接受的风险级别，或者导致组织目前无法保证满足 RTO/RPO 预期和要求。

通过采取降低风险的具体措施，可以处理这些场景。这些措施必须要记录下来，并整合为一个计划，这就是风险处理计划。风险处理计划不属于业务连续性计划的一部分，但两者可以同时存在。风险处理计划包括额外投资、重新调整现有服务和/或基础设施、将某些活动外包等等。

业务连续性计划

我们在起草这个计划之前，需要先了解一些术语的含义。如前所述，如果出现特定破坏性事件，在处理危机时，可将 BCP 作为指导方针和行动计划。

从高层面上来讲，处理危机的方式大同小异，主要包括以下几步：

1. 评估危机形势
2. 遏制危机事件
3. 将危机恢复到 RTO（恢复时间目标）和 RPO（恢复点目标）中的预定义级别
4. 危机解除

请注意，危机结束（以危机解除为标志）并不意味着组织已经恢复到“事件发生前”的状态。“危机解除”是指危机小组认为危机已经得到控制，服务已经恢复，组织可以履行其运营使命。但是，这并不表示所有损坏都已修复。

以下示例可以进一步说明这一点：*周末，一群破坏份子损毁了一家注册管理机构的主要办公室，并抢劫了里面的财物。这家机构的 IT 设备被盗，家具被毁，损失惨重，另外，由于调查正在进行中，因此机构员工基本上无法在办公室工作。在这种情况下，这家机构启用了 BCP，规定当办公室不可用时，所有来电将被转到移动设备进行处理，员工可以在家办公，直到另行发布通知（这表示远程办公切实可行）。与此同时，危机小组与执法机构、保险公司和其他各相关方进行了初步交涉，并确保上述 BCP 能够得以执行。采取这些措施后，服务将会恢复到可接受的级别，机构可以继续履行其运营使命。随后，危机小组分配资源以进一步处理该案件，并将办公室恢复原样。待一切尘埃落定后，危机小组会解散，并恢复到其正常的运营角色。显然，对于小型组织，由于可用资源有限，一人身兼多职的情况在所难免。*

重要材料是处理破坏性事件时必不可少的一系列信息（数字信息和/或物理信息）。这些信息包括以下几类：合同、特定服务的联系人信息（例如网络提供商、清理服务、出租人、权威机构等）、登录帐户和密码、钥匙类实物资产，等等。请务必保护好这些敏感材料，同时也要确保这些材料在危机期间可以获取。

业务连续性计划：一旦确定某种场景存在最高级别的风险，那么便应立刻起草计划。组织可以指定某人制定详细计划，说明在处理灾难事件时要执行的每个步骤。虽然制定详尽的计划并非难事，但是灾难往往会引发一些意外的连带事件，这不利于我们在制定计划时编写需要执行的每个步骤。根据以往经验，在处理危机的过程中，我们应制定一个总体指导方针，重述关键步骤，这样更为有用。之后，可以在培训、测试和模拟活动中使用此类计划。

除此之外，我们还应研究这种场景带来的影响。制定多个 BC 计划毫无意义，因为尽管出现的危机事件可能各不相同，但最终采取的应对措施却大致相同，因此，制定一个计划便已足矣。关于这一点有一个典型的示例，那就是导致办公室不可用的事件。不管这种场景是（火灾、罢工、停电、洪涝、黑色星期五）中的哪一个原因所致，这些原因都不是真正相关的因素，所以它们的处理措施都一样。之后，可以将该处理措施纳入 BC 计划。

下面的模板很精简，重复了上面讨论的处理灾难的所有步骤。这个模板也有助于确定一些准备任务。**请注意，切勿在处理危机期间即兴制定措施，因为这可能带来最糟糕的结果。**总而言之，这个模板只是一个可以帮助危机小组处理危机情况，协助他们做好准备的备忘单。

业务连续性计划（模板）			
参考：	[参考]	威胁类型	受影响的资产
场景：	*说明触发计划实施的条件。可以是某个事件、时间或特定条件等…*		
启动：	*何时启动计划？可以在检测到危机事件后立即启动计划，也可以在事件发生后的几个小时内启动计划。*		
RTO：	*恢复时间目标*		
RPO：	*恢复点目标*		
危机小组：	*危机小组包括哪些成员？实际将由哪些人员处理事件？请注明员工姓名、合作伙伴名称和供应商名称，以防含糊不清。*		
优先行动：	*应优先采取哪些行动？可以将其理解为一个顺序列表。*		
评估：	*处理破坏性事件的第一步是评估事件的严重程度。说明应考虑哪些因素。*		
遏制：	*说明为阻止势态进一步恶化需要采取的行动方案。*		
恢复：	*说明恢复最基本运营就绪状态所需采取的行动方案，同时考虑上述定义的优先行动。*		
危机解除：	*一旦运营恢复正常，危机小组会解散，同时留下进一步的行动指示，以便帮助组织恢复到事件发生前的状态。*		

沟通：	*定义内部和外部沟通，包括消息和通讯组清单以及沟通方式。始终从内部沟通开始。*
重要材料：	*处理危机事件所需的资源列表。这是准备阶段的一项工作。计划不包含实际内容，而仅限于参考材料（各部门领导和/或合作伙伴有责任维护该内容，使其保持最新，并尽可能确保其准确无误和易于携带）*
记录：	*应在危机期间和之后记录哪些内容？这些记录内容有助于收集证据、吸取经验教训和跟进事件进展。*

表 9

附录中列举了 BC 计划的一些示例。

支持

资源

制定业务连续性（管理）系统的初始工作可能非常耗时，但是对于较小的组织来说，上述方法应当有助于使这项工作变得切实可行。

在起草各项清单后，便可以继续制定计划。鉴于威胁和危害情况并非一成不变，因此需要每年对该计划进行一次审核和更新。例如，21 世纪初，网络攻击几乎仅存在于科幻小说中；而如今，它们已变为现实，对人们构成了切实威胁。

在小型组织中，要成功制定业务连续性计划，一方面，需要管理层参与其中，进行管理并提供指导；另一方面，组织应高度重视该项目，并给予支持。

组织无需为此任命专门的业务连续性经理；在某些情况下，将 BC 战略纳入整个组织的职责后，该战略可能会更显成效。

认知度

要成功实施业务连续性战略，整个组织都需要具有这一意识，每个人都应以此为己任。

因此，组织可以定期召开一些会议，提高员工在这方面的认知度。

沟通

正如模板和业务连续性计划示例所示，沟通（内部和外部）在危机管理中发挥着非常重要的作用。

为此，需要完成以下事项：

1. 决定使用哪种沟通方式。例如，电话、短信、消息、Twitter、电子邮件等。
2. 准备沟通模板（在危机管理中，即兴沟通确实会扼杀组织的可信度）。
3. 预定义并准备要沟通的对象，例如，“我们的注册服务机构”不是有效的定义。通过电子邮件沟通时，选择最新的电子邮件地址列表。
4. 设置沟通的优先事项和时间表（例如，每 60 分钟更新一次 Twitter 消息，事件开始和结束时发送一封电子邮件）。
5. 评估是否需要聘请外部危机沟通顾问来帮助制定沟通策略和计划；同时也培养一些人员，以便处理媒体相关事宜。

运营

起草 BCP 后，应将该计划嵌入到日常业务和常规运营中。这意味着业务连续性必须在所有工程、业务流程和工作流程中发挥作用。

同时，这也意味着业务连续性必须在各个领域中发挥作用，例如，采购、法律、工程、运营、沟通。

下面的示例说明了这一点：

- 组织购买了一些服务器和网络设备。发送给供应商的提案征询 (RFP) 提到采用**冗余电源**和双**网卡**实现最大冗余。
- 服务是**外包**的，RFP 明确提到了服务提供商应采取的业务连续性措施。

BC 演练

制定用于应对特定灾难场景的计划是完全没有问题的，但是如果不进行任何测试或演练，制定的计划纯属*“纸上谈兵”*。

因此，对 BC 计划进行测试和演练，是有效业务连续性战略中不可或缺的组成部分。正如消防员进行消防演习一样，危机小组也应花些时间对计划进行实质性测试和演练。

目前有两种进行测试和演练的方法。一种方法称作桌面演练（即 TTX），另一种方法则是实控模拟。

桌面演练 (TTX)

这种“纸上”演练旨在全面回顾所有程序，对训练小组非常有帮助。这种演练需要相对较少的准备工作。

TTX 可以是一种角色扮演练习，所有参与者围坐在桌旁，每个人都扮演其各自的角色。**单独设立的一位“主持人”**将指导小组完成场景的各个步骤，偶尔穿插一些额外增加的意外事件。

TTX 的一个主要缺点是，很难让参与者感受到紧迫感和真实感。

> 行动：有必要让组织的全体员工每年至少通读一次 BC 计划，并对计划的可行性提出批判性意见。BC 计划是动态文件，需要根据不断变化的环境做出调整。

模拟

理想情况下，应通过现实模拟对业务连续性计划进行测试。在进行此类模拟时，可以检查各个小组或合作伙伴对灾难场景的应对情况，进而验证小组工作的有效性以及计划的可行性。

通过对各个计划进行演练，小组将逐步了解并熟知当事件实际发生时，他们所需采取的行动。

模拟现实事件（例如，数据中心断电）显然有时比较困难，但可以通过拟定仿真场景来进行演练。

示例：

- 勒索软件大肆爆发。一位用户致电服务台，表示其笔记本电脑屏幕上出现勒索消息，声称其电脑已被入侵并锁住，需要支付一些比特币才能解锁，用户咨询在这种情况下应当如何做。本练习旨在测试支持团队对此情况的响应能力。
- 由于鼠患，办公室无法进入。办公室显然没有老鼠，本练习旨在测试如何向员工传达此消息。

改进

对于任何有效的业务连续性战略，必须每年至少审核一次业务连续性计划、风险评估、利益相关方清单、威胁和危害清单等，或者每当发生重大变更时进行审核。

重大变更通常是由以下行为引发的：

- 制定新立法
- 外包
- 并购
- 推出新服务
- 利益相关方变更
- 推出新技术
- 威胁形势发生变化
- 发生事件
- ...

附录：任务汇总

本附录汇总了本文件中所述的各项任务。本附录可以用作核对清单，以协助开展实施工作。

1. 制作所有**利益相关方**及其预期的清单，并指明哪些预期与业务连续性相关（表 1）
2. 制作所有**供应商**的清单，说明他们提供的产品和服务，并指明与业务连续性的相关性及产生的影响（表 3）
3. 使用表 4 创建一个**威胁和危害登记表**，指明有哪些适用的威胁和危害及其发生的可能性
4. 使用表 5 指明有哪些**风险**适用于组织；使用表 6 定义每个风险的不同级别
5. 将威胁和危害登记表（表 4）中的适用威胁和危害复制到**业务影响评估**（表 7）中。所有这些表格可以汇总到一个热图中，在该热图中，使用不同的颜色对各个风险级别进行标注，如以下示例所示：

威胁类别	威胁	财务	运营	声誉	法律	治理	人员
网络	DDOS	中	严重	高/ 严重	高	高	无

6. 展开表 7（之前用于进行简单的业务影响评估），然后在其中添加**风险处理**（表 8）。许多威胁若不加以缓和将引发无法承受的风险，因此，可根据风险处理制定风险处理计划，计划中包含降低风险的措施。这并不意味着风险会彻底消除，而是意味着风险将会有所降低。
7. 以表 9 为模板创建**业务连续性计划**，以应对那些被视为对组织有重大影响的切实威胁和危害。

附录：业务连续性计划示例

业务连续性计划（模板）			
参考：	[参考]	威胁类型	受影响的资产
场景：	*说明触发计划实施的条件。可以是某个事件、时间或特定条件等…*		
启动：	*何时启动计划？可以在检测到危机事件后立即启动计划，也可以在事件发生后的几个小时内启动计划。*		
RTO：	*恢复时间目标*		
RPO：	*恢复点目标*		
危机小组：	*危机小组包括哪些成员？实际将由哪些人员处理事件？请注明员工姓名、合作伙伴名称和供应商名称，以防含糊不清。*		
优先行动：	*应优先采取哪些行动？可以将其理解为一个顺序列表。*		
评估：	*处理破坏性事件的第一步是评估事件的严重程度。说明应考虑哪些因素。*		
遏制：	*说明为阻止势态进一步恶化需要采取的行动方案。*		
恢复：	*说明恢复最基本运营就绪状态所需采取的行动方案，同时考虑上述定义的优先行动。*		

危机解除：	*一旦运营恢复正常，危机小组会解散，同时留下进一步的行动指示，以便帮助组织恢复到事件发生前的状态。*
沟通：	*定义内部和外部沟通，包括消息和通讯组清单以及沟通方式。始终从内部沟通开始。*
重要材料：	*处理危机事件所需的资源列表。这是准备阶段的一项工作。计划不包含实际内容，而仅限于参考材料（各部门领导和/或合作伙伴有责任维护该内容，使其保持最新，并尽可能确保其准确无误和易于携带）*
记录：	*应在危机期间和之后记录哪些内容？这些记录内容有助于收集证据、吸取经验教训和跟进事件进展。*

网络：黑客入侵

业务连续性计划			
参考：	BCP-xxx.yy	网络：黑客入侵	全球
场景：	有证据表明，注册管理机构的基础设施遭到黑客入侵和破坏。一名外来人员通过安装软件、创建帐户、使用远程访问工具及其他手段入侵了注册管理机构。数据（包括敏感数据）有可能已泄露。		
启动：	在检测到危机事件时立即启动		
RTO：	24 小时		
RPO：	24 小时的数据丢失。		
危机小组：	法务经理 – +CC 123 55 88 – ivan.horvat@registry.tld 技术经理 – +CC 123 44 55 – juan.perez@registry.tld 业务连续性经理 – +CC 123 33 66 – jane.doe@registry.tld 总经理 – +CC 123 56 44 – yamado.toro@registry.tld		
优先行动：	保护域名服务器和 .tld 区域的可用性和完整性。 如有需要，隔离域名服务器基础设施。 隔离遭入侵的系统。 收集证据。		
评估：	如果发现数据泄露的证据，还启动适用于数据外泄的 BCP。 评估并盘点遭入侵的系统。哪些服务受到影响？DNS、注册平台、内部系统和网站是否受到影响？ 仔细检查域名服务器基础设施。 黑客是否有固定的据点？ 在检测到入侵时黑客是否在线？		

	是否需要向专门从事网络安全的外部公司寻求帮助（是否有证据表明国家行为者参与其中）？
遏制：	确保域名服务器基础设施受到保护，并将域名服务器与受影响的区域隔离开来。 禁用或关闭受影响的系统。 不要试图修复受损系统或对抗入侵者。 集中精力隔离受损系统。 尝试收集证据；切勿篡改证据。
恢复：	应重建和重新部署受影响的系统。 如果最终用户设备遭到破坏，需部署新系统。
危机解除：	在隔离和关闭受损系统，且通过重建和重新部署系统恢复服务后，危机小组将指派一组人员来处理以下活动： 1. 联系执法机构并提出投诉。 2. 确保受损系统得到妥善保管，并将日志文件作为证据保留。 分析核心数据库的完整性（是否有篡改痕迹？）。
沟通：	仅限内部沟通 首先与所有内部人员沟通，传达系统已遭受破坏，当前正在隔离受损系统的消息。强调一点，之后与外部的沟通事宜将由传播经理和法务经理直接负责处理。 外部沟通： 通知各利益相关方（董事会、权威机构） 如果将关闭系统（即网站、WHOIS、EPP），需通知注册服务机构，向其告知将采取的后续措施。 通知执法机构。

重要材料：	基础设施和设置的相关文件。 密码库，用于访问各个系统。 部署和暂存基础设施，用于部署新的基础设施。 通讯组清单（注册服务机构、员工）
记录：	创建事件记录，以记录发现的情况、采取的行动和收集的证据。应在危机处理期间记录，而不是事后记录。

外部：恐怖袭击

业务连续性计划			
参考：	BCP-xxx.yy	外部：恐怖袭击	办公室
场景：	注册管理机构办公室附近发生恐怖袭击。附近是指在同一城市或半径 25 公里以内。本计划全天候适用。		
启动：	立即		
RTO：	未定义		
RPO：	未定义		
危机小组：	办公室负责人 – +CC 123 44 55 – jan.modaal@registry.tld 人力资源经理 – +CC 123 66 23 – maija.meikalainen@registry.tld 业务连续性经理 – +CC 123 33 66 – jane.doe@registry.tld 总经理 – +CC 123 56 44 – yamado.toro@registry.tld		
优先行动：	保护员工人身安全。		
评估：	根据严重程度，重大袭击可能会引发严重后果（封锁公共交通、部署特警队，等等）。首先也是最重要的是，必须要确保员工及其家人的人身安全。由于注册管理机构支持在家办公，已到达办公室的人员不应继续留在办公室，未到达办公室的人员不应再前往办公室。		
遏制：	如果情况允许，将立即关闭办公室，并将员工护送回家。如果袭击地点离办公室太近，建议员工留在原地不动，并遵照执法机构和政府的指示。		

恢复：	办公室负责人将核查是否已向所有员工告知并说明相关事宜。 办公室负责人将告知所有员工在另行通知之前，办公室将关闭并禁止入内。 办公室负责人将向人力资源经理或业务连续性经理报告相关情况。 人力资源经理或业务连续性经理将通知相应部门和经理接管相应活动。
危机解除：	办公室负责人将遵循执法机构和官方的指示，在办公室重新开放时通知员工。
沟通：	仅限内部沟通 办公室负责人首先与受影响的员工通过口头或短信形式进行沟通。 办公室负责人、人力资源经理或业务连续性经理通过电子邮件进行后续沟通。
重要材料：	员工名单，包含电话号码和电子邮件地址。
记录：	员工记录，证明已向所有员工告知并说明相关事宜。

网络：勒索软件

业务连续性计划			
参考：	BCP-xxx.yy	网络：勒索软件	办公室和 最终用户设备
场景：	一次勒索软件感染使有限数量的 MS Windows 笔记本电脑被锁定，无法使用。感染可以局限在一个办公室内，也可以传播到整个组织。		
启动：	在检测到危机事件时立即启动		
RTO：	一个工作日内。		
RPO：	一个工作日的数据丢失。		
危机小组：	技术经理 – +CC 123 44 55 – juan.perez@registry.tld 业务连续性经理 – +CC 123 33 66 – jane.doe@registry.tld 总经理 – +CC 123 56 44 – yamado.toro@registry.tld		
优先行动：	保护 Windows Server 基础设施的可用性和完整性。 隔离受感染的系统。 重新暂存受感染的系统。		
评估：	感染是否在扩散？最初受感染的系统是哪个？ 能否隔离感染？		
遏制：	隔离受感染的计算机（即关闭与数据中心的网络连接）； 远程关闭未受感染的系统；如果无法远程关闭，让用户自行关闭其系统。		

恢复：	必须将受感染的系统视为无法恢复，从而需要重新安装这些系统。一些员工可能会在几天内无法联机工作。
危机解除：	危机小组将指派一组人员来处理以下工作： 1. 识别勒索软件并检查特征码或其他检测方法； 2. 确定初始应变，即首个受感染的系统是如何遭受感染的？ 3. 隔离发生感染的网络环境（有线和无线网络环境）；如果确定有系统未遭受恶意软件感染，则应启动并仔细检查未受感染的系统； 4. 制定计划，以重新安装受感染的笔记本电脑。对于远程办公的情况，这可能会有些困难，因为可能需要派遣一名现场工程师。 5. 根据法律义务/建议，向执法部门和/或其他机构提出正式投诉。
沟通：	仅限内部沟通 通知所有员工勒索软件爆发的消息，并指示他们立即关闭其 (Windows) 笔记本电脑（可通过电子邮件、电话和短信形式通知）。
重要材料：	基础设施和设置的相关文件。 密码库，用于访问各个系统。 通讯组清单（员工）。
记录：	创建事件记录，以记录发现的情况、采取的行动和收集的证据。应在危机处理期间记录，而**不是**事后记录。

附录：工作坊

工作坊时间表

	描述	时间（分钟）	人员
1	介绍手册 - 分发“DR/BCP 计划”文件	45	
2	针对手册展开问答	15	
3	填写表格 - BIA - BCP - 根据您自己的 ccTLD - 分发 DR/BCP 模板	45	
4	讨论表格填写结果	30	
5	组建小组（最多 5 个小组） - 分发卡片、OK 注册管理机构说明和网络黑客入侵 BCP 计划	5	
6	熟悉卡片内容	10	
7	5 轮现实模拟演练 (TTX)	60	
8	演练汇报	30	

（共 240 分钟）

演示和表格填写练习

进行 45 分钟的手册介绍，然后再开展 15 分钟的问答，以突出主要主题。

在 45 分钟的手册介绍环节，我们会要求参与者：

1. 列出所有利益相关方，并写下他们的预期。
2. 查看威胁登记表，明确有哪些适用的威胁？
3. 明确哪些风险对组织有重大影响，并确定各个风险的级别。
4. 选择一个威胁并对其进行业务影响评估 (BIA)。
5. 基于这一威胁，制定业务连续性计划 (BCP)；列出重要材料所包含的项目。

利益相关方列表

这个列表中的利益相关方仅用作示例。请根据相应情况添加尚未列出但您认为相关的利益相关方。
与 BC 的相关性：高、中、低、不适用

利益相关方	**预期**	**与 BC 的相关性**
政府	_____ _____ _____	_____ _____ _____
ICANN	_____ _____ _____	_____ _____ _____
董事会	_____ _____ _____	_____ _____ _____
公众	_____ _____ _____	_____ _____ _____
执法机构	_____ _____ _____	_____ _____ _____
注册服务机构	_____ _____ _____	_____ _____ _____
注册人	_____ _____ _____	_____ _____ _____
	_____ _____ _____	_____ _____ _____
	_____ _____ _____	_____ _____ _____

威胁登记表

根据统计信息，查看哪些威胁适用，并确定各个威胁发生的可能性有多少。

威胁类别	威胁	适用（是/否）	可能性
自然灾害	火灾 洪涝 飓风/龙卷风/台风 恶劣天气 地震 山体滑坡/雪崩 火山喷发 海啸 雷击沉降污染 虫患 鼠患 _____	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____
人力资源和医疗	关键人员流失 流行疾病 技能/人员短缺 家庭琐事 偷窃 恶意破坏（毁坏） 勒索 _____	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____ _____ _____
网络	DDOS 黑客入侵 数据丢失 勒索软件 网络战争相关活动 _____	☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____
外部	经济衰退 公民非暴力反抗活动 恐怖活动 战争/侵略 政治干预/政策变更 入室盗窃 技术变革/相关活动 _____	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____ _____ _____
财务	现金流/流动资产问题 资本匮乏	☐ ☐	_____ _____

	金融渎职行为 坏账 利率风险 汇率风险 国债敞口风险 _____	☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____
技术和基础设施	网络故障 – 全球 电力 – 电网故障 交流电故障 数据中心故障 组件故障 [5] _____	☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____
供应故障	服务级别故障 质量缺陷 供应服务中断 外包失败/供应合同缺货情况 其他关键资产损失 供应商套牢 _____	☐ ☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____ _____

可能性：

1. 极有可能： 一年一次或更频繁地重复发生的事件
2. 可能： 平均每三年发生一次的事件
3. 罕见： 每十年发生一次的事件
4. 不太可能： 每 50 年或更长时间发生一次的事件
5. OoS： 超出范围 – 不纳入业务连续性考虑范围的事件

[5] 组件故障是指出现故障的计算机系统、电源、计算机内存、磁盘等的总称；您可以决定将其纳入业务连续性的范围，也可以假定默认情况下在基础设施的设计和架构（即冗余电源、RAID 磁盘系统、服务器中的 ECC 内存等）中此风险能够得以缓和。

风险表

类型	无或不适用	低	中	高	严重
财务	风险不存在或不适用				
运营					
声誉					
法律					
治理 [6]					
人员					

[6] 治理风险可能最难处理，同时也是最特殊的风险类型。对于一些注册管理机构来说，这种风险甚至可能不存在。在处理这种风险时，管理层需要先明确定义并说明注册管理机构对外部影响的依赖程度。

业务影响评估

以威胁登记表中指定的对业务连续性有明显影响的某个威胁为例，根据风险表评估该威胁对各类风险的影响。可能性是从威胁登记表中复制而来的。

可能性：

1. 极有可能： 一年一次或更频繁地重复发生的事件
2. 可能： 平均每三年发生一次的事件
3. 罕见： 每十年发生一次的事件
4. 不太可能： 每 50 年或更长时间发生一次的事件
5. OoS： 超出范围 – 不纳入业务连续性考虑范围的事件

RTO（恢复时间目标，即业务必须在中断后多长时间内恢复）和 RPO（恢复点目标，即可以接受的数据丢失量）由业务部门定义，它们可能是合同、法律或治理上的要求，不应考虑技术上是否可以实现。

威胁类别	**威胁**	**适用（是/否）**	**可能性**
		是	
风险	**级别**	**动机/描述/说明**	
财务			
运营			
声誉			
法律			

治理		
人员		
RTO		
RPO		
风险缓和	“不适用”或描述缓和风险的计划	
接受风险		
规避风险		
降低风险		
控制风险		
转移风险		

业务连续性计划

业务连续性计划（模板）			
参考：	[参考]	威胁类型	受影响的资产
场景：	*说明触发计划实施的条件。可以是某个事件、时间或特定条件等…*		
启动：	*何时启动计划？可以在检测到危机事件后立即启动计划，也可以在事件发生后的几个小时内启动计划。*		
RTO：	*恢复时间目标*		
RPO：	*恢复点目标*		
危机小组：	*危机小组包括哪些成员？实际将由哪些人员处理事件？请注明员工姓名、合作伙伴名称和供应商名称，以防含糊不清。*		
优先行动：	*应优先采取哪些行动？可以将其理解为一个顺序列表。*		
评估：	*处理破坏性事件的第一步是评估事件的严重程度。说明应考虑哪些因素。*		
遏制：	*说明为阻止势态进一步恶化需要采取的行动方案。*		
恢复：	*说明恢复最基本运营就绪状态所需采取的行动方案，同时考虑上述定义的优先行动。*		
危机解除：	*一旦运营恢复正常，危机小组会解散，同时留下进一步的行动指示，以便帮助组织恢复到事件发生前的状态。*		

沟通：	*定义内部和外部沟通，包括消息和通讯组清单以及沟通方式。始终从内部沟通开始。*
重要材料：	*处理危机事件所需的资源列表。这是准备阶段的一项工作。计划不包含实际内容，而仅限于参考材料（各部门领导和/或合作伙伴有责任维护该内容，使其保持最新，并尽可能确保其准确无误和易于携带）*
记录：	*应在危机期间和之后记录哪些内容？这些记录内容有助于收集证据、吸取经验教训和跟进事件进展。*

业务连续性计划

业务连续性计划（模板）			
参考：	[参考]	威胁类型	受影响的资产
场景：			
启动：			
RTO：			
RPO：			
危机小组：			
优先行动：			
评估：			
遏制：			
恢复：			
危机解除：			

沟通：	
重要材料：	
记录：	

模拟演练 (TTX) 说明

演练完全按照脚本进行，一共有 5 轮，每轮 10 分钟。在每一轮开始时，各小组将获取相应信息，且必须使用恰当的业务连续性计划对给出的信息做出回应。

为确保演练顺利进行，将为每个小组分发一系列卡片。这些卡片中包含一系列实际行动事项，这些行动是针对在每一轮开始时收到的信息而需采取的行动。

参与者每轮最多可以选择 3 项行动（即 3 个卡片），这些行动将留待稍后讨论。卡片分为以下 4 类：“技术”、“法律”、“治理”和“沟通”，分别代表技术部门、法务部门、综合管理部门和传播部。

在每轮演练中，可以增加补充信息；补充信息应由小组给予处理，并可能导致行动方案发生变化。

5 轮结束后，收集卡片，并围绕一系列主题对卡片内容展开讨论，以收集参与者的反馈。

注册管理机构说明

您受雇于“**OK 注册管理机构**”，即 .ok ccTLD 的注册管理运行机构。OK，也称为 Old Kontry，是一个欧洲小国，大约有 5 万居住人口。由于宽松自由的政策，.ok 顶级域非常受欢迎，截至 2019 年 11 月 1 日已注册了 372,304 个域名。.ok 域名由大约 250 个注册服务机构在全球范围内进行出售。

Old Kontry 是单一议会君主立宪制国家。

Old Kontry 并未加入欧盟。

该注册管理机构位于 Old Kontry 首都，隶属“**OK 大学**”，但保持独立运作（在管理、财务和技术上都独立运作）；不过，该注册管理结构受该大学监管。

对于后端服务，该注册管理机构聘用了 MegaRyCorp.Inc.，这是一家专门为注册管理机构提供后端服务的德国注册管理机构服务提供商。DNS 服务由一家美国的任播提供商负责，但该注册管理机构有 3 个在大学网络中运行的旧单播域名服务器。

对于其网络影响力（公司网站、社交媒体等），该注册管理机构在很大程度上依赖于一家当地的创新型数据和技术机构，该机构是一个国际组织的子公司。

除了隐藏的主域名服务器和权威域名服务器之外，该注册管理机构还运行一个 EPP 服务器、一个 WHOIS 服务器和一个注册服务机构外部网（外部网不仅具有与 EPP 相同的功能，而且还具有其他一些功能）。

由于其受欢迎程度和对当地经济的重要性，**OK 政府**在过去几年里通过了符合欧洲《通用数据保护条例》(GDPR) 的立法以加强个人数据保护，另外还通过了旨在保护关键基础设施和基本服务运营商的 NIS 指令。OK 政府还指定电信部作为合规与政策的监管部门。

“**OK 注册管理机构**”是一个小型组织，只有 7 名专职员工。该机构可以依靠大学来获取笔记本电脑/台式机/电子邮件及其他方面的 IT 支持。

该注册管理机构雇用了 3 名工程师（1 名开发人员、1 名系统管理员、1 名网络工程师)，负责以下方面的工作：注册服务机构网站门户、监控、传统域名服务器、防火墙、局域网/无线局域网、注册服务机构支持和技术问题报告。

此外，该机构还有 1 位总经理、1 位销售和市场营销经理、1 位财务经理和 1 位法务经理；技术团队直接向总经理报告工作。业务连续性管理由法务经理负责。

针对网络事件的 BCP 计划：黑客入侵

业务连续性计划			
参考：	BCP-101.01	网络：黑客入侵	全球
场景：	有证据表明，注册管理机构的基础设施遭到黑客入侵和破坏。一名外来人员通过安装软件、创建帐户、使用远程访问工具及其他手段入侵了注册管理机构。数据（包括敏感数据）有可能已泄露。		
启动：	在检测到危机事件时立即启动		
RTO：	24 小时		
RPO：	24 小时的数据丢失。		
危机小组：	法务经理 – +CC 123 55 88 – ivan.horvat@registry.tld 技术经理 – +CC 123 44 55 – juan.perez@registry.tld 业务连续性经理 – +CC 123 33 66 – jane.doe@registry.tld 总经理 – +CC 123 56 44 – yamado.toro@registry.tld		
优先行动：	保护域名服务器和 .ok 区域的可用性和完整性。 如有需要，隔离域名服务器基础设施。 隔离遭入侵的系统。 收集证据。		
评估：	评估并盘点遭入侵的系统。哪些服务受到影响？DNS、注册平台、内部系统和网站是否受到影响？ 仔细检查域名服务器基础设施和服务。 黑客是否有固定的据点？ 在检测到入侵时黑客是否在线？ 是否需要向专门从事网络安全的外部公司寻求帮助（是否有证据表明国家行为者参与其中）？ 是否泄露了数据？如果是，泄露了什么类型的数据？数据泄露会产生什么影响？		

遏制：	确保域名服务器基础设施受到保护，并将域名服务器与受影响的区域隔离开来。 禁用或关闭受影响的系统。 不要试图修复受损系统或对抗入侵者。 集中精力隔离受损系统。 尝试收集证据；切勿篡改证据。
恢复：	应重建和重新部署受影响的系统。 如果最终用户设备遭到破坏，需部署新系统。
危机解除：	在隔离和关闭受损系统，且通过重建和重新部署系统恢复服务后，危机小组将指派一组人员来处理以下活动： 1. 联系执法机构并提出投诉。 2. 确保受损系统得到妥善保管，并将日志文件作为证据保留。 分析核心数据库的完整性（是否有篡改痕迹？）。
沟通：	**内部沟通：** 首先与所有内部人员沟通，传达系统已遭受破坏，当前正在隔离受损系统的消息。强调一点，之后与外部的沟通事宜将由销售和市场营销经理或法务经理直接负责处理。 **外部沟通：** 通知各利益相关方（大学董事会、权威机构） 如果将关闭系统（即网站、WHOIS、EPP），需通知注册服务机构，向其告知将采取的后续措施。 通知执法机构。 定期在社交媒体账号和公共网站上发布工作进展。
重要材料：	基础设施和设置的相关文件。 密码库，用于访问各个系统。 部署和暂存基础设施，用于部署新的基础设施。 通讯组清单（注册服务机构、员工、利益相关方）
记录：	创建事件记录，以记录发现的情况、采取的行动和收集的证据。应在危机处理期间记录，而不是事后记录。

演练场景

第 1 轮：信息 星期五 下午 5:00

- 一名安全研究人员联系注册管理运行机构的总经理，称他在 Pastebin 上发现了关于某个数据库的摘录，摘录内容似乎指向注册服务机构所使用的注册管理机构外部网。
- 该研究人员在 Pastebin 上检查了经过哈希处理的密码，并十分轻松地“破解”了其中一些密码。不出所料，采用的是很常用的密码“password123”。他确认自己在特定时间成功登录了注册服务机构外部网（他会将这些时间告知经理）。
- Pastebin 仍然在线，该研究人员还发现了一些证据，可证实有人在暗网上出售外部网登录凭据。
- 该研究人员认为，已有充足的证据证明有不法分子入侵了注册管理机构，并已开始从中牟利。

这是注册管理机构收到的初步信息。经理将如何应对？他/她会采取什么行动？从此刻开始，必须根据经理选择的行动方案为其提供一些补充信息。请注意时间。参与者每轮只有 15 分钟。

挑选 3 张卡片

第 2 轮：信息 星期五 晚上 8:00

- 距最初发现入侵，时间已经过了 3 个小时
- 有人在 Twitter 上发布了指向另一个 Pastebin 的链接，该推文的标签为 #freeDomains4All #longLive.OK；该标签是从原来的 Pastebin 复制过来的。
- 有人发现并转发了这条推文，而且在推文标签中新增了 #itWorks。

挑选 3 张卡片

第 3 轮：信息 星期五 晚上 10:00

- 又经过了 2 个小时
- 媒体联系注册管理运行机构，询问所发生的情况，并要求注册管理运行机构发表正式声明。
- 注册管理运行机构经理接到国家电视台的来电。
- 工程师们仍在调查此事，但还没有找到泄漏的源头。

挑选 3 张卡片

加分环节：信息（在本轮结束前 3 分钟）

为了使演练变得更加有趣，可以增加补充信息。在现实生活中，事件往往不会按照可预测的模式发展，在发生危机期间当然更是如此。加分环节仅提供补充信息，这些信息需要在本轮演练结束前进行分析和处理。

- 工程师们有一些好消息和一些坏消息。
- 他们发现黑客入侵了系统并追踪到了已遭篡改的内容。

- 他们还发现，注册的域名数量增加了 5 万个，而且还有现有域名遭篡改，其中包括一些非常知名的域名，遭篡改的现有域名数量尚未确定。
- 工程师们建议回滚 DNS，并联系主要的互联网服务提供商，请求他们重新加载解析器。

更新 3 张卡片

第 4 轮：信息 星期六 早上 6:00

- 又经过了 8 个小时
- 国家计算机紧急事件响应小组 (CERT) 联系注册管理运行机构；CERT 获得了一些关于攻击源头的情报
- 注册管理运行机构的社交媒体平台上充斥着相关域名持有者和注册服务机构提出的各种问题
- 注册管理运行机构通用邮箱来信量暴增，共计收到 5,000 多封电子邮件
- 媒体再次联系注册管理运行机构了解最新情况，并询问为何问题在这么久之后仍未得到解决
- 相关监管部门（如电信部）联系注册管理运行机构的总经理，他们希望注册管理运行机构向其汇报事件最新进展和事件影响

挑选 3 张卡片

第 5 轮：结束 星期日 上午 9:00

- 又经过了 21 个小时
- 工程部门将数据库回滚到星期四晚上 11:47 的状态，这是未发现遭篡改域名的最新备份
- 域名服务器已重新加载
- 被黑客利用的漏洞已修复
- 所有注册服务机构凭据均已重置
- 支持人员收到了受影响的域名、注册服务机构和注册人的清单
- 为回复 10,000 多封请求支持票证的电子邮件以及 Twitter 上无数的抱怨推文，造成了大量积压工作
- 一些博文作者和视频博主关注了这个问题，并发表了他们的观点

挑选 3 张卡片

演练结束 - 暂停

参与者需要休息一下 ☺

汇报

每个小组展示他们的卡片。

为了保证演练的有效性和高效性，有必要正确无误地听取汇报并讨论小组采取的行动。因此，必须以书面或录音的方式记录危机小组所做的汇报。汇报应重点关注以下若干主题：

1. 对于这项演练，小组成员普遍做出了什么样的回应？
2. 业务连续性计划的执行情况如何？
3. 小组成员从哪里开始即兴发挥？
4. 小组成员是否认为自己足以胜任这项任务？
5. 小组成员学到了什么？
6. 需要做出哪些改进？

卡片

按名片大小打印卡片，并对每个类别使用不同的颜色标注。

	技术	法律/BC 管理	沟通	治理/管理
1	关闭权威域名服务器	致电执法机构	在社交媒体上发布事件最新资讯	声明灾难情况
2	联系注册管理机构服务运营商，并向其告知此事件	就沟通策略向管理层提供建议	在社交媒体上发布相关消息	召集危机小组
3	联系任播运营商，并向其告知此事件	联系外部事件响应公司以协助处理此事件	答复媒体问询	启动业务连续性计划
4	关闭注册平台	建议尽量减少不必要的沟通	准备关于回滚事件的通讯稿	联系监管机构/董事会
5	开始查找可用的日志文件	建议管理层实现完全透明	撰写新闻稿	通知政府监管机构
6	恢复核心数据库	联系当地电信服务提供商，请求他们重新启动解析器	撰写危机沟通模板	联系国家 CERT 并报告事件
7	重新安装受损系统	将调查结果移交执法机构	发布关于事件影响的新闻声明	召开新闻发布会
8	对遭黑客入侵的系统进行技术评估并收集相关证据	联系注册服务机构，请求他们更改密码	未经法务经理和总经理确认，不得通过公共渠道发布任何信息	向政府监管机构汇报事件最新进展
9	开始回复通过支持电子邮件地址收到的支持票证和其他请求	向欧洲数据保护理事会告知此事件	发布关于内部状态的最新信息	宣布危机结束，解除危机，业务回归正常
10	创建一份遭篡改的域名列表以确定受害者	就此事件向执法机构提出投诉	聘请危机沟通发言人	请求国家 CERT 的援助
11	创建一份新增域名列表	通知保险公司	否认违约	通知 ICANN
12	阻止访问注册系统	通知受影响的注册人	向 TLD-OPS 发送电子邮件以寻求帮助	联系 IANA 全天候紧急热线

13	更改所有密码	通过 TLD-OPS 电子邮件清单通知其他注册管理机构		追究 TLD-OPS 的责任 :-)
14	从 Pastebin 下载密码列表	通过 TLD-OPS 电子邮件清单向其他注册管理机构寻求帮助		
15	安装 SIEM			

这套卡片可在 TLD-OPS 网站上以 Adobe Indesign 格式下载，之后可随时发送到打印店进行打印。

工作坊提示和技巧：

本节包含适用于 DR/BCP 演练的提示和技巧，如果您有任何关于如何改进 TTX 的新想法，请发送电子邮件至 TLD-OPS。

- 识别利益相关方、威胁和风险并不是一个人的工作。应持续传达这一观点。
- 有些威胁“很可怕”，因此着实需要将其记录下来并制定相应计划。
- 让每位参与者练习识别在每个 TLD 中，BCP 经理一职实际上由哪些职能部门/团体/个人担任；此外，还练习识别实际的利益相关方
- 有些人可能不太清楚事件在财务方面所产生的影响，对于这种情况，可请求商务人员的帮助，因为业务连续性演练是一项集体活动
- 指明组织中担任 BCP 经理一职的部门或人员：是法务部、PMO、财务部、CIO、CSO、CEO 还是 COO？
- 或许可在演练开始时向每个小组分发以下 3 张卡片