ICS 03.100.01
A 90

中华人民共和国国家标准

GB/T 35625—2017/ISO/TS 22317:2015

公共安全　业务连续性管理体系 业务影响分析指南(BIA)

Societal security—Business continuity management systems—Guidelines for business impact analysis (BIA)

(ISO/TS 22317:2015,IDT)

2017-12-29 发布　　2018-06-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准使用翻译法等同采用 ISO/TS 22317:2015《公共安全　业务连续性管理体系　业务影响分析指南》(英文版),做了下列编辑性修改:

——增加了缩略语(见 3.2);

——按照出现的顺序调整了国际标准附录的顺序。

本标准由全国公共安全基础标准化技术委员会(SAC/TC 351)提出并归口。

本标准起草单位:中国标准化研究院、中国信息安全认证中心、国网山东省电力公司、江苏省质量和标准化研究院、厦门国际银行股份有限公司、北京科技大学、广发银行、中国质量认证中心、英标认证技术培训(北京)有限公司、国际灾难恢复协会中国分会。

本标准主要起草人:秦挺鑫、尤其、孙世军、刘珏、张松滨、高玉坤、张桂明、潘英、赵连河、于天、邢立强、魏军、韩洪、杨正科、王序、刘佳。

引　言

本标准为业务影响分析(BIA)的建立、实施、持续改进提供了详细的指导,并与 ISO 22301 保持一致。

本标准可应用于任何过程的 BIA。

图 1 说明了 BIA 和业务连续性(BC)的关系。组织宜在业务连续性策略确定前完成 BIA。

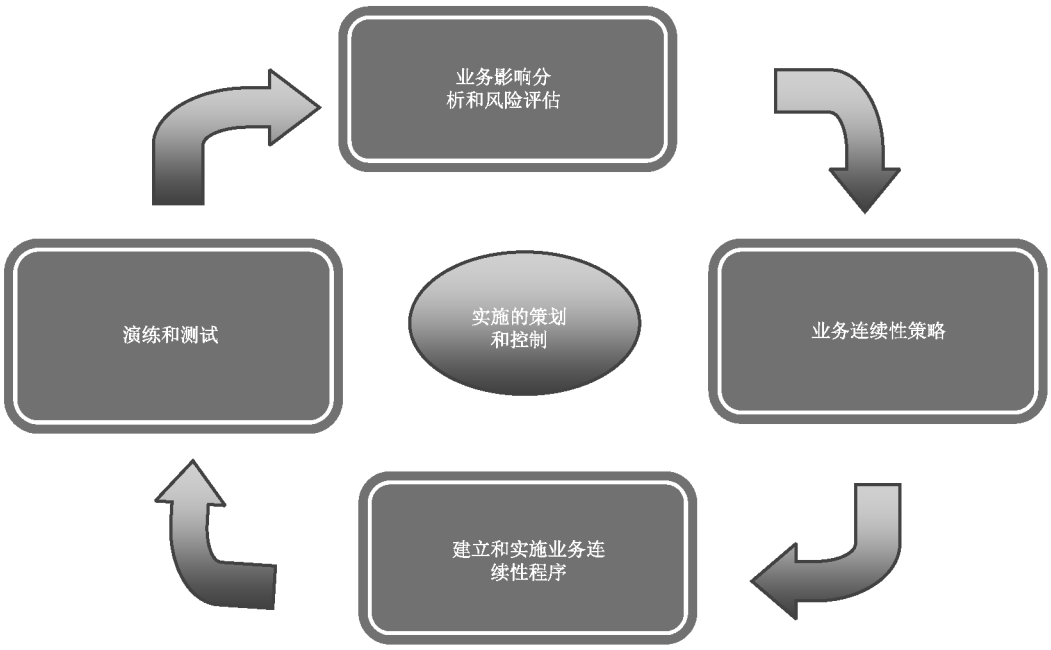

图 1　业务连续性管理(BCM)要素(来源:ISO 22313)

BIA 是分析破坏性事件对组织影响后果的过程。其结果是论述业务连续性的需求。

BIA 过程包含多个单独的 BIA,每一个 BIA 专注于业务连续性方案中的某一个小部分。BIA 过程首先对产品和服务进行优先级区分,并能够在涵盖业务连续性方案整个范围的同时,持续对过程和活动的优先次序进行区分。由组织确定一段时间之后,重复各项单个 BIA,以保证 BC 的要求始终保持最新。

注:在本标准中,业务连续性要求和连续性恢复优先级、目的和目标的意思是一致的(ISO 22301:2012,8.2.2)。

本标准的目的:

——为组织理解、开发、实施、检查、保持、提升有效的 BIA 过程提供依据;

——为 BIA 的策划、实施、改进提供指导;

——协助组织良好开展 BIA;

——确保 BIA 过程能够和 BC 方案之间进行良好的协调。

BIA 过程的产出包括以下内容:

——对组织的业务连续性方案范围进行认可或修正;

——确定法律、法规和合同的要求,以及它们对业务连续性要求的影响;

——评估随着时间的推移对组织的影响,可作为业务连续性要求的论证(时间和能力);

——识别和了解突发事件发生后对产品/服务的交付要求，然后对恢复活动和资源确定优先级和时间；

——识别和确定产品/服务、过程、活动和资源之间的关系；

——确定需要优先安排的活动所需要的资源（如场地、人员、设备、信息、通讯和技术设备；物资和资金）；

——了解其他活动、供应链、合作伙伴以及其他利益相关方之间的依赖关系；

——确定如何更新所需的信息。

注：本技术标准的目的，提供的产品、作品和服务生产所需的供应链，在本文件的余下部分被称之为“供应”。

图 2 是 BIA 的生命周期、前提条件以及策略识别的关系。图中引用的条款是本标准的章条。

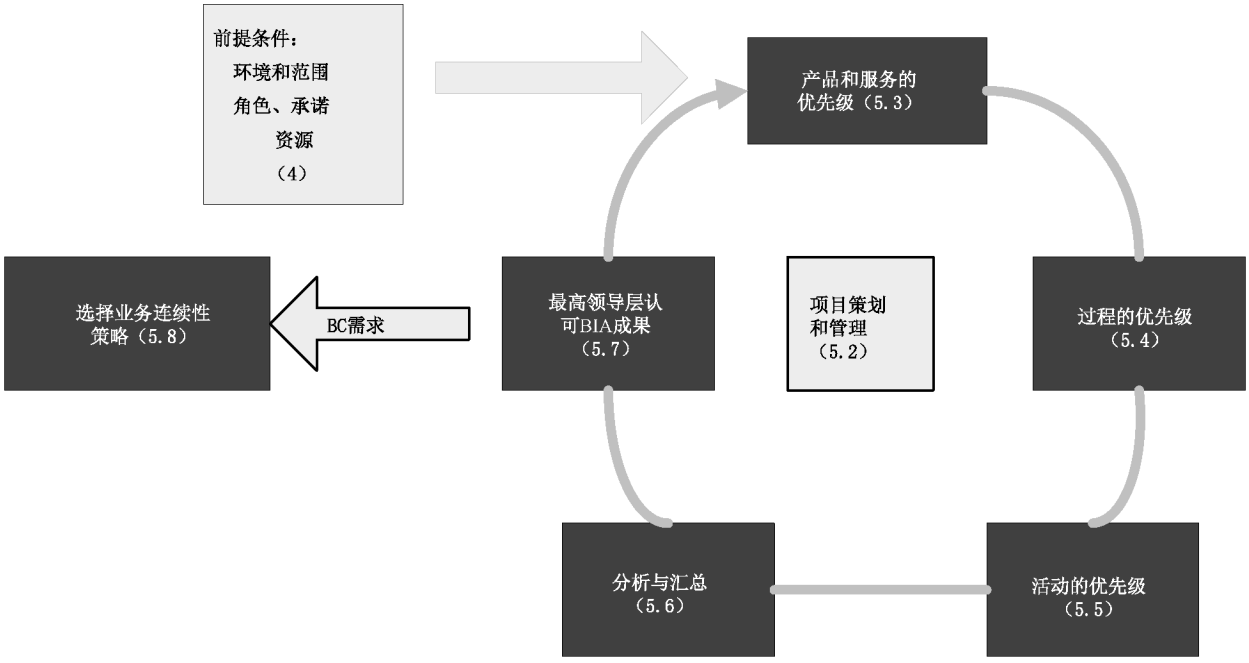

图 2　BIA 过程

公共安全　业务连续性管理体系
业务影响分析指南(BIA)

1　范围

本标准为组织建立、实施业务影响分析(BIA)提供良好的操作建议,它并没有规定统一的 BIA 程序。

本标准适用于各种类型、规模与性质的组织。组织可根据其需求、目标、资源与限制性条件作出调整。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修订版)适用于本文件。

ISO 22300　公共安全　术语(Societal security—Terminology)。

3　术语和定义以及缩略语

3.1　术语和定义

ISO 22300 界定的术语和定义适用于本文件。

3.2　缩略语

BC——业务连续性

BCM——业务连续性管理

BIA——业务影响分析

4　前提条件

4.1　总则

引言中已注明,本标准与 ISO 22301 一致,可用来开发、实施、评审、保持和持续改进 BIA 过程,该过程满足其他标准或法规要求。无论是 BCM 体系或业务连续性方案的一部分,组织宜在 BIA 过程开始之前考虑一系列的前提条件。本章总结了这些前提条件,其中一些来自 ISO 22301。

组织在开始 BIA 过程之前,宜在 BCM 方案内采取一系列措施,包括:

——定义环境和范围(4.2);

——定义并沟通角色和职责(4.3);

——获得领导层承诺(4.4);

——分配足够的资源(4.5)。

注:更多的信息,参见附录 A 本标准与 ISO 22301 的对应关系。