ICS 13.200
CCS A 90

中华人民共和国国家标准

GB/T 44483—2024

安全与韧性　术语

Security and resilience—Vocabulary

（ISO 22300：2021，MOD）

2024-09-29 发布　　2025-04-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前言 …… Ⅲ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
3.1　安全与韧性相关术语 …… 1
3.2　反伪造税票相关术语 …… 33
3.3　供应链相关术语 …… 37
3.4　闭路电视相关术语 …… 38
参考文献 …… 40
索引 …… 41

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件修改采用ISO 22300：2021《安全与韧性　术语》。

本文件与ISO 22300：2021相比做了下述结构调整：

——删除了3.1.31、3.1.32、3.1.72，后续条目号依次前移。

本文件与ISO 22300：2021的技术差异及其原因如下：

——更改了术语“突发事件”的定义（见3.1.84，ISO 22300：2021的3.1.87），以符合我国现行法律法规；

——删除了“公民社会”（见ISO 22300：2021的3.1.31）、“公民社会组织”（见ISO 22300：2021的3.1.32）、“去中心化的权利”（见ISO 22300：2021的3.1.72）的术语和定义，以符合我国国情。

本文件做了下列编辑性改动：

——更改了3.1.14、3.1.71、3.1.131等部分术语定义中的注。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件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。

本文件起草单位：中国标准化研究院、城市安全发展科技研究院（深圳）、北京市科学技术研究院、应急管理部大数据中心、国网四川省电力公司、北京邮电大学、清华大学、中国矿业大学（北京）、北京工商大学、对外经济贸易大学、应急管理部国家自然灾害防治研究院、重庆大学、深圳市城市公共安全技术研究院有限公司、中铁隧道局集团建设有限公司、中铁七局集团有限公司、湖南防灾科技有限公司。

本文件主要起草人：张超、秦挺鑫、王皖、邓创、杨继星、张少标、胡燕祝、王晶晶、杨锐、杨跃翔、董方、孟祥程、周倩、徐凤娇、王英剑、郭德华、王亚飞、何明珂、李丽、谭波、聂百胜、黄帅、刘国生、吴阳、李波、凌君、周琳、柳先锋、毛必君、李建国。

安全与韧性　术语

1　范围

本文件界定了安全与韧性标准的术语，包括安全与韧性、反伪造税票、供应链和闭路电视等相关术语。

本文件适用于安全与韧性相关标准的制修订工作。

2　规范性引用文件

本文件没有规范性引用文件。

3　术语和定义

3.1　安全与韧性相关术语

3.1.1

访问　access

权利所有人(3.1.211)使用某种服务或产品或从中获得效益(3.1.17)的能力。

注：限制可能由与源的距离(例如供水网络无法到达某个社区)或无法负担(例如对于某个家庭或人群而言服务成本太高)等原因造成。

3.1.2

活动　activity

一组具有确定输出的一个或多个任务的集合。

3.1.3

胶粘剂　adhesive；glue

将两种材料粘结在一起的混合物。

注：通过热量、压力或化学反应使其产生作用。

3.1.4

受影响区域 affected area

受冲扰事件(3.1.73)(事故、灾害)影响的空间范围。

注：该术语通常与立即疏散(3.1.89)相联系。

3.1.5

行动后报告 after-action report

演练最终报告 final exercise report

记录、描述和分析实际冲扰(3.1.72)或演练(3.1.94)情况，借鉴观察员(3.1.160)的汇报和报告，总结经验教训的文件(3.1.74)。

注：行动后报告记录了行动后评审(3.1.208)的结果。

3.1.6

警报　alert

突发事件(3.1.84)发展过程中，引起第一响应人和处于风险的人(3.1.173)的注意。

注：警报是公共预警(3.1.194)的一部分。

3.1.7

解除警报　all clear

危险已经结束的消息或信号。

3.1.8

全部危险　all-hazard

对组织(3.1.162)、社区(3.1.37)、社会及其依存环境造成潜在影响(3.1.115)的自然事件(3.1.93)、人为事件(有意和无意)和技术事件。

3.1.9

备用工作区　alternate worksite

当主要工作区不能使用时,可供使用的工作场所。

3.1.10

分析领域　analysis area

已选择要进行同行评审(3.1.171)的主题。

示例:风险管理(3.1.221)、风险评估、金融能力、城市发展、气候变化适应和生态系统保护、机构能力、社区(3.1.37)和社会能力、经济和业务连续性(3.1.19)、基础设施(3.1.125)、公共卫生、恢复和重建的综合治理。

3.1.11

分析系统　analysis system

由相互连接、共同工作的部分组成的,能够形成和提供分析领域(3.1.10)的集合。

3.1.12

危险区域　area at risk

可能被冲扰事件(3.1.73)(事件、事故、灾害)影响的位置。

注:该术语与预防性疏散更相关。

3.1.13

资产　asset

对组织(3.1.162)具有价值的事物。

注:资产包括但不限于人员、物理实体、信息(3.1.124)、无形的和环境资源(3.1.204)。

3.1.14

审核　audit

为获得审验证据并对其进行客观的评价,以确定满足审核准则的程度所进行的系统的、独立的并形成文档的过程(3.1.187)。

注 1:审核可能是内部审核(3.1.131)(第一方)或外部审核(第二方或第三方),也可能是联合审核(两方或多方参与)。

注 2:内部审核由组织(3.1.162)自身,或外部团体代其开展。

注 3:“审验证明”和“审核准则”由 ISO 19011 定义。

注 4:审核的基本要素包括:由不承担审核职责的人员(3.1.176),按规定程序(3.1.186)对对象(3.1.158)做出的合格(3.1.42)评定结果。

注 5:内部审核能够用于管理(3.1.141)评审(3.1.208)和其他内部目标,并且可能形成组织符合性声明的基础。能够通过对审核活动(3.1.2)的自由性声明来表明其独立性。外部审核包括第二方和第三方审核。第二方审核可能由与组织有相关利益的组织,例如消费者或其他利益相关人员来实施。第三方审核可能由外部或独立审核组织,如提供合格评定的认证/注册的组织或政府机构实施。

注 6:该术语是 ISO 管理体系标准的高级结构的核心术语之一。原始定义已通过补充的注 4 和注 5 进行了修改。

3.1.15

审核员　auditor

实施审核(3.1.14)的人员。

[来源:ISO 19011:2018, 3.15]

3.1.16

基本社会服务　basic social services

在教育、健康等社会领域提供的满足基本需求的一系列服务。

3.1.17

效益　benefit

由于引入同行评审(3.1.171)产生的变化所导致的可衡量改进。

注:效益可能是有形的或无形的,可量化的或非可量化的,经济性的或非经济性的。

3.1.18

生物多样性　biodiversity/biological diversity

包括陆地、海洋和其他水生生态系统(3.1.81)在内的所有来源的生物体之间的变异性,以及该生物体所组成的生态复杂性。

注:这包括物种内部、物种之间以及生态系统之间的多样性。因此,生物多样性不仅是所有生态系统、物种和遗传物质的总和,而且代表了它们内部及其之间的变异性。

3.1.19

业务连续性　business continuity

在承受冲扰(3.1.72)期间,组织(3.158)在可接受的时间段内按预先确定的水平,持续提供产品和服务(3.1.188)的能力。

3.1.20

业务连续性管理　business continuity management

实施和维持业务连续性(3.1.19)的过程(3.1.187)。

3.1.21

业务连续性管理体系　business continuity management system;BCMS

整个管理体系(3.1.143)中用于建立、实施、运行、监控、评审(3.1.208)、维持和改进业务连续性(3.1.19)的活动。

注:管理体系包括组织结构、政策、计划活动、职责、程序(3.1.186)、过程(3.1.187)和资源(3.1.204)。

3.1.22

业务连续性计划　business continuity plan

用于指导组织(3.1.162)在业务冲扰(3.1.72)时进行响应和恢复,并恢复提供满足业务连续性(3.1.19)目标(3.1.159)的产品和服务(3.1.188)的能力的成文信息(3.1.75)。

3.1.23

业务连续性方案　business continuity programme

由最高管理者(3.1.276)和适当的资源支撑的,为实施和保持业务连续性管理(3.1.20)所进行的持续不断的管理(3.1.141)和治理过程(3.1.187)。

注:在 ISO 22301:2019 中,该术语被业务连续性管理体系(3.1.21)代替。

3.1.24

业务影响分析　business impact analysis

分析冲扰(3.1.72)对组织(3.1.162)影响(3.1.115)的过程(3.1.187)。

注:业务影响分析的结果是业务连续性(3.1.19)要求(3.1.201)的声明和理由。

3.1.25

能力　capacity

组织(3.1.162)、社区(3.1.37)或社会可用于降低风险(3.1.212)水平或减小危机(3.1.58)影响的所有队伍和资源(3.1.204)的总和。

注：能力可能包括物质、制度、社会或经济手段以及技术人员(3.1.176)或领导、管理(3.1.141)等属性。

3.1.26

照顾者　carer

对弱势群体(3.1.290)提供支持的个人。

注：照顾者的支持行为可能是有偿的或无偿的。

3.1.27

货物运输单元　cargo transport unit

公路货运车、铁路货运车、货物集装箱、公路罐车、铁路罐车或便携储罐。

3.1.28

闭路电视系统　CCTV system

由摄像头、记录仪、连接线和显示器组成的，用于监视商场、公司、基础设施(3.1.125)和/或公共场所活动的监控系统。

3.1.29

挑战　challenge

可能影响(3.1.115)城市系统(3.1.282)应对新兴风险和机遇能力(3.1.25)的情况或环境变化。

3.1.30

民防　civil protection

为保护公民生命、健康和财产，以及环境免受不良事件(3.1.278)影响而采取的措施及实施的体系。

注：不良事件可能包括事故、突发事件(3.1.84)和灾害(3.1.70)。

3.1.31

客户　client

雇用、曾经雇用或有意愿雇用组织(3.1.162)代表自身执行安全运营(3.1.246)的实体(3.1.88)。

示例：消费者、承包商、最终用户、零售商、受益人和购买者。

注 1：客户可能是组织内部的一部分(如另一个部门)或外部组织。

注 2：包括以合适的形式将客户分包(3.1.267)给其他公司或当地组织。

3.1.32

色盲　colour blindness

区分特定色调(3.1.110)的能力完全或部分缺失。

3.1.33

色标　colour-code

用于表达特定含义的一组符号化的颜色。

3.1.34

指挥和控制　command and control

目标导向的决策活动(3.1.2)。

注 1：该过程(3.1.187)是持续重复的。

注 2：指挥和控制包括情况评估、计划(3.1.177)、决策和事件(3.1.119)处置效果的控制。

3.1.35

指挥和控制体系　command and control system

在准备、事件响应(3.1.123)、业务连续性(3.1.48)和/或恢复(3.1.198)过程(3.1.187)中，对所有应急

资产(3.1.13)进行有效应急管理(3.1.85)的支持体系。

3.1.36

沟通和咨询　communication and consultation

组织(3.1.162)管理(3.1.141)风险(3.1.212)时,提供、分享或获取信息(3.1.124),以及与利益相关方(3.1.129)和其他人进行对话的持续和往复的过程(3.1.187)。

注1:信息可能涉及风险管理和安全运营管理(3.1.247)的存在、性质、形式、可能性(3.1.139)、严重程度、评价(3.1.92)、可接受性、应对或其他方面。

注2:咨询是组织与其利益相关方在某一问题决策或确定方向之前所进行的充分的双向沟通。

咨询是:

——一个通过影响力而不是通过权力来影响决策的过程;

——对决策的输入,而不是共同决策。

3.1.37

社区　community

具有共同利益的组织(3.1.162)、个人和团体的群体。

注:受影响社区是受安全(3.1.236)服务、项目或运营影响的人员和相关组织的群体。

3.1.38

社区预警体系　community-based early warning system

社区警报体系 community-based warning system

通过建立的网络向公众传达信息(3.1.124)的方法。

注:警报体系可能包括风险知识、监测(3.1.152)和警报服务、传播和沟通,以及避免、减小风险(3.1.212)和应对灾害(3.1.70)的响应能力。

3.1.39

社区脆弱性　community vulnerability

处于危险源(3.1.107)的危害作用风险(3.1.212)中的个人、群体或基础设施(3.1.125)的自身特征或状态。

3.1.40

胜任力　competence

应用知识与技能,实现预期目标的能力。

注:该术语是ISO管理体系标准的高级结构的通用术语和核心定义之一。

3.1.41

复杂性　complexity

组织系统由许多不同的、相互独立但又彼此关联和依赖的部分组成,这些部分之间相互作用,并与外部元素进行多端非线性作用的状态。

注:复杂性是使系统无法通过个体行为变量累加的形式判断系统行为的特征。

3.1.42

合格　conformity

满足要求(3.1.201)。

注:该术语是ISO管理体系标准的高级结构的通用术语和核心定义之一。

3.1.43

后果　consequence

〈结果〉事件(3.1.93)对目标(3.1.159)影响的结果。

注1:事件对目标的影响可能是确定的或不确定的,可能是积极的或消极的,可能是直接的或间接的。

注2:后果能以定性或定量表达。

注 3：通过连锁反应和累积效应，最初的后果可能升级。

注 4：在中文中，表述中性“结果”的“后果”，直译为“结果”。

[来源：ISO 31000：2018，3.6]

3.1.44

后果　consequence

〈损失〉人员伤亡、财产损失或经济冲击，包括对交通系统的冲扰(3.1.72)，这可能是供应链(3.1.268)中的组织受到攻击(3.2.4)的结果，或利用供应链(3.1.268)作为攻击手段的结果。

3.1.45

环境　context

进行能力评估时要考虑的外部和内部因素。

注 1：外部环境包括以下内容：

——国际、国内、区域或本地的文化、社会、政治、法律、法规、金融、技术、经济、自然和竞争环境；

——对组织(3.1.162)的目标(3.1.159)有影响(3.1.115)的关键驱动因素和趋势；

——与外部利益相关方(3.1.129)的关系、理念和价值观。

注 2：内部环境包括：

——组织的授权；

——业务敏感性；

——治理、组织结构、作用和责任制；

——资源(3.1.204)和知识[例如：资金、时间、人员、过程(3.1.187)、系统和技术]；

——组织文化(3.1.163)。

3.1.46

偶发事件　contingency

未来可能发生的事件(3.1.93)、状况或突发情况。

3.1.47

持续改进　continual improvement

能够提高绩效(3.1.174)的经常性活动(3.1.2)。

注：该术语是 ISO 管理体系标准的高级结构的通用术语和核心定义之一。

3.1.48

连续性　continuity

组织(3.1.162)的管理(3.1.141)层预先批准的，对条件、情况和事件(3.1.93)进行计划和响应，以使组织在可接受的预定水平持续运营的战略和战术能力。

注：连续性是运营和业务连续性(3.1.19)的通用术语。它确保组织能够在正常情况正持续运营。它不仅适用于营利性公司，还适用于各种类型的组织，例如非政府组织、公益组织和政府组织。

3.1.49

控制　control

维持和/或改变风险(3.1.212)的措施。

注 1：控制措施包括但不限于任何过程(3.1.187)、策略(3.1.178)、设备、实践或其他能够维持和/或改变风险的条件和/或行动。

注 2：控制措施不会始终发挥预期或假定的改变效果。

3.1.50

合作　cooperation

基于协定，为共同利益和价值而协同工作或行动的过程(3.1.187)。

注：组织(3.1.162)根据合同或其他形式的协议，同意提供事件响应(3.1.123)所需资源(3.1.204)，同时保持内部层次

结构的独立性。

3.1.51

协调　coordination

不同组织(3.1.162)(公共的或私营的),或同一组织的不同部分,为实现共同目标(3.1.159)而共同工作或行动的方式。

注1:协调整合了相关方(包括公共或私人组织和政府)的响应活动(3.1.2),以在具有一致目标的事件响应(3.1.123)中,通过共享各自事件响应行动信息(3.1.124)实现协调一致的行动。

注2:所有组织都参与过程(3.1.187),就共同的事件响应目标达成共识,并通过这一共识制定、实施响应策略。

3.1.52

纠正　correction

为消除已发现的不符合(3.1.156)事项所采取的措施。

[来源:ISO 9000:2015,3.12.3,有修改]

3.1.53

纠正措施　corrective action

消除不符合(3.1.156)原因并防止其再次发生的措施。

注:该术语是ISO管理体系标准的高级结构的通用术语和核心定义之一。

3.1.54

假冒(动词)　counterfeit(verb)

未经授权,模仿、复制或修改物质产品(3.1.146)或其包装。

3.1.55

假冒产品　counterfeit good

模仿或复制真实的物料(3.2.7)的物质产品(3.1.146)。

3.1.56

对策　countermeasure

为降低安全威胁情景(3.1.255)的可能性(3.1.139)以实现目标(3.1.159),或减小安全威胁情景可能的后果(3.1.44)所采取的措施。

3.1.57

覆盖范围　coverage

责任主体(3.1.77)提供服务或产品的能力(3.1.25)。

注:它可能会受到财务能力、地理空间设置以及规范和制度框架的影响。

3.1.58

危机　crisis

由即将发生的突然或重大变化而导致的,需要紧急关注并采取措施以保护生命、资产(3.1.13)、财产或环境的不稳定情况。

3.1.59

危机管理　crisis management

通过有效的响应保护组织关键利益相关方(3.1.129)、信誉、品牌、价值创造活动(3.1.2),识别威胁组织(3.1.162)的潜在影响(3.1.115),提出韧性(3.1.203)建设框架,以及有效恢复运营能力的全面管理(3.1.141)过程(3.1.187)。

注:危机管理还涉及对事件(3.1.119)的准备(3.1.179)、减缓(3.1.151)响应以及连续性(3.1.48)或恢复(3.1.198)的管理,以及通过培训(3.1.277)、演练和评审(3.1.208)来管理整个计划,以确保准备、响应和连续性计划保持最新。

3.1.60

危机管理团队　crisis management team

负责指导制定和执行响应和业务连续性(3.1.48)计划,宣布运营冲扰(3.1.72)或突发事件(3.1.84)/危机(3.1.58)情况,并在恢复(3.1.198)过程(3.1.187)中,以及破坏事件(3.1.119)前后提供指导的团体。

注:危机管理团队可包括来自组织(3.1.162)的个人,也可包括立即和第一响应人员和利益相关方(3.1.129)。

3.1.61

关键控制点　critical control point;CCP

能够通过控制(3.1.49)使威胁(3.1.274)或危险被预防、消除或减缓到可接受水平的点、步骤或过程(3.1.187)。

3.1.62

关键客户　critical customer

失去其业务将威胁组织(3.1.162)生存的实体(3.1.88)。

3.1.63

关键设施　critical facility

对社区(3.1.37)或社会的社交和经济功能提供必要服务的物理结构、网络或其他资产(3.1.13)。

3.1.64

关键指标　critical indicator

为识别发生事件(3.1.119)、事故或突发事件(3.1.84)的可能的发展情况,监视危险源(3.1.107)并用于评估的定量、定性或描述性度量。

注:关键指标提供有关设施(3.1.102)结构状态的最重要的整体特征的信息(3.1.124)。

3.1.65

关键产品和服务　critical product and service

由供应商处获取,若未得到将中断组织的关键活动(3.1.2)并威胁组织(3.1.162)生存的资源(3.1.204)。

注:关键产品或服务是支持组织在业务影响分析(3.1.24)中确定的高优先级活动和过程(3.1.187)的重要资源。

3.1.66

关键供应商　critical supplier

关键产品或服务(3.1.188)的提供者。

注:关键供应商也包括与其客户属于同一组织(3.1.162)的"内部供应商"。

3.1.67

危害性分析　criticality analysis

基于任务或职能的重要性、处于风险的人(3.1.173)群规模,或不良事件(3.1.278)或冲扰(3.1.72)对其满足期望能力的影响程度而设计的,用于系统地识别和评估组织(3.1.162)资产(3.1.13)的过程。

3.1.68

关键地　critically

对目标(3.1.159)和/或结果至关重要。

3.1.69

数据分析　data analysis

对监测(3.1.152)实际或计划体系中的过程(3.1.187)和流程时获得的相关的、基于证据的信息(3.1.124)进行的系统调查。

3.1.70

灾害　disaster

造成大范围或大规模的人员、物质、经济或环境损失，超出了受影响组织(3.1.162)、社区(3.1.37)或社会使用其自身资源(3.1.204)进行响应和恢复的能力的情况。

3.1.71

减小灾害风险　disaster risk reduction

旨在预防新的灾害和减少现有灾害风险并管理剩余风险(3.1.202)的策略(3.1.178)。

注：减小灾害风险有助于增强韧性(3.1.203)，实现可持续发展。

3.1.72

冲扰　disruption

预期的或未预期的，导致组织(3.1.162)目标(3.1.159)内的产品和服务(3.1.188)不能按计划交付或发生负向偏离的事件(3.1.119)。

3.1.73

冲扰事件　disruptive event

预期或未预期的，造成计划的活动(3.1.2)、行动或功能中断的事件或变化。

3.1.74

文件　document

信息(3.1.124)及其承载媒介。

注 1：媒介可能是纸张、计算机磁盘、光盘或其他电子媒体，照片或标准样品，或其组合。

注 2：一组文件，如若干个规范和记录(3.1.197)，通常也称为“文档”。

3.1.75

成文信息　documented information

需要被组织(3.1.162)控制和维护的信息(3.1.124)及其承载媒介。

注 1：成文信息可能是多种格式的，也可能是任何来源的任何承载媒体。

注 2：成文信息指：

——管理体系(3.1.143)，包括相关过程(3.1.187)；

——为组织运作而创建的信息(文档)；

——取得结果的证据[记录(3.1.197)]。

注 3：该术语是 ISO 管理体系标准的高级结构的通用术语和核心定义之一。

3.1.76

训练　drill

练习并经常多次重复特定技能的活动(3.1.2)。

示例：在发生火灾的建筑中的进行安全疏散的消防训练。

3.1.77

责任主体　duty-bearer

有特别义务或责任尊重、促进和实现人权(3.1.112)并避免侵犯人权的个人。

注 1：该术语最常用于涉及国家行为者的情况，但非国家行为者也可能视为责任主体。

注 2：根据环境(3.1.45)，个人(例如父母)、本地组织(3.1.162)、私人公司、捐献者和国际机构也可能视为现任责任主体。

3.1.78

看护责任　duty of care

确保他人的安全、福祉或利益的道德或法律义务。

3.1.79

预警　early warning

通过本地网络提供信息(3.1.124),使受影响的个人能够采取措施避免或降低风险(3.1.212),并准备响应的措施。

3.1.80

经济多样性　economic diversity

特定地理区域的,分布于多个领域的经济活动。

示例:行业、部门、技能水平和就业水平。

3.1.81

生态系统　ecosystem

植物、动物和微生物群落及与之作为自然功能单元发生相互作用的非生物环境(例如土壤、空气、阳光)的动态复合体。

注:生活在生态系统中的一切都取决于其他物种和元素,它们也是该生态社区的一部分。

3.1.82

生态系统服务　ecosystem services

人们从生态系统(3.1.81)中获得的效益(3.1.17)。

注:这些服务包括:提供食物、水、木材和纤维;调节或影响气候、洪水、疾病、废物产生和水质;提供娱乐、美学和精神利益的文化服务,以及诸如形成土壤、光合作用和养分循环等。

3.1.83

有效性　effectiveness

完成计划活动(3.1.2)并获得预期结果的程度。

注:该术语是ISO管理体系标准的高级结构的通用术语和核心定义之一。

3.1.84

突发事件　emergency

突然发生,造成或者可能造成严重社会危害,需要采取应急处置措施予以应对的自然灾害、事故灾难、公共卫生事件和社会安全事件。

3.1.85

应急管理　emergency management

预防突发事件(3.1.84)并在发生时进行管理的全部方法。

注:通常,应急管理在潜在不稳定事件(3.1.93)和/或冲扰(3.1.72)之前、期间和之后采用风险管理(3.1.221)方法以实现预防(3.1.180)、准备(3.1.179)、响应和恢复(3.1.198)。

3.1.86

应急管理能力　emergency management capability

在潜在不稳定或冲扰事件(3.1.93)之前、期间和之后,有效管理预防(3.1.180)、准备(3.1.179)、应对和恢复(3.1.198)的总体能力。

3.1.87

员工援助方案　employee assistance programme

提供给组织(3.1.162)的,用以帮助员工解决生产问题,并帮助识别和解决个人关注的健康、婚姻、家庭、经济、饮酒、药物、法律、情感、压力或其他可能影响工作绩效的个人问题的合同支持服务。

注:源自国际劳工援助专业协会(International Employee Assistance Professionals Association, EAPA)。

3.1.88

实体　entity

独立、清晰地存在,并在环境(3.1.45)内可识别的事物。

注：实体可能是人、组织(3.1.162)、物理对象(3.1.158)、对象类或无形对象。

3.1.89

疏散　evacuation

有组织、分阶段、有监督地将人员由危险或潜在危险区域至安全地点的移动。

3.1.90

疏散指令　evacuation command

一系列疏散人员的命令。

3.1.91

疏散训练　evacuation drill

练习与疏散(3.1.89)相关的特定技能的活动(3.1.2)。

示例：练习从滑坡(3.1.138)地区安全撤离至邻近区域或村庄的训练(3.1.76)。

注：疏散训练通常涉及多次重复同一事项。

3.1.92

评价　evaluation

将测量(3.1.149)结果与既定指标相对比，确定预期绩效与实际绩效(3.1.174)之间差异的系统化过程(3.1.187)。

注：绩效差异应作为持续改进(3.1.47)过程的依据。

3.1.93

事件　event

一组特定情况的发生或变化。

注 1：一个事件可能是一个或多个情况，并且可能有多种原因和多种后果(3.1.43)。

注 2：事件也可能是预期但没有发生的事情，或是意料之外的事情。

注 3：事件可能是风险源(3.1.227)。

3.1.94

演练　exercise

培训、评估、实践和提高组织(3.1.162)绩效(3.1.174)的过程(3.1.187)。

注 1：演练能够用于验证策略(3.1.178)、计划、程序(3.1.186)、培训(3.1.277)、装备与组织间协议的有效性；明确人员(3.1.176)的岗位职责和开展相关的培训活动；改进组织间的协调(3.1.51)与沟通；识别资源(3.1.204)的不足；提高个人绩效并识别改进机会；以及有控制地练习即兴表演的机会。不需要设定演练通过或失败的预期。

注 2：另见测试(3.1.272)。

3.1.95

年度演练计划　exercise annual plan

演练(3.1.94)策略(3.1.178)计划已被细化为演练目标和方案，并包括特定年度演练方案(3.1.97)的文件(3.1.74)。

3.1.96

演练协调员　exercise coordinator

计划(3.1.177)、实施与评价演练(3.1.94)活动(3.1.2)的人员。

注 1：较大型演练中，演练协调员也可能称为“演练控制员”，可能由多名人员担任。

注 2：一些国家使用“演练指导员”或类似的称呼代替“演练协调员”。

注 3：演练协调员也负责协调内外部实体(3.1.88)间的合作(3.1.169)。

3.1.97

演练方案　exercise programme

为达成总体目标(3.1.159)而设计的一系列演练(3.1.94)活动(3.1.2)。

3.1.98

演练方案负责人　exercise programme manager

负责制定与改进演练方案(3.1.97)的人员。

3.1.99

演练项目团队　exercise project team

负责计划(3.1.177)、实施与评价演练(3.1.94)项目的团体。

3.1.100

演练安全员　exercise safety officer

确保演练(3.1.94)活动安全实施的人员。

注：包括多项功能的较大型演练可能安排一名以上的安全员。

3.1.101

外部攻击　external attack

与产品的合法制造商、原产地或权利所有人(3.1.211)没有直接或间接关系的个人或实体实施的攻击(3.2.4)。

3.1.102

设施　facility

工厂、机械、财产、建筑物、运输单元、海/陆/空港和其他基础设施(3.1.125)项目或具有独特和可量化的业务或服务功能的工厂和相关系统。

注：设施可能具有法律规定的正式界限。

3.1.103

司法的　forensic

与法律有关或在法庭上使用的。

注：适用于能够作为法律证据的视频监控(3.1.286)。

3.1.104

综合演练　full-scale exercise

包括多组织(3.1.162)或功能，并包括真实活动(3.1.2)的演练(3.1.94)。

3.1.105

功能性演练　functional exercise

用于培训、评估、练习和改进针对一个不良事件(3.1.278)的响应和恢复设计的单一功能绩效(3.1.174)的演练(3.1.94)。

注：功能性可能包括紧急行动中心(EOC)团队、危机管理团队(3.1.60)或消防洗消队伍等的职能。

3.1.106

地理位置　geo-location

由一个或多个方法确定的，表达经度、纬度、海拔高度和坐标系的特定位置。

注：地理位置通常是指地球上一个点或对象(3.1.158)的、有特定意义的规范。该术语本身不包含使用的坐标系。与地理位置关联的其他属性(3.2.5)不是地理位置规范的一部分。

3.1.107

危险源　hazard

潜在危害的来源。

注：危险源可能构成风险源(3.1.227)。

3.1.108

危险源监测功能　hazard monitoring function

获取指定区域内的有证可循的危险源(3.1.107)信息(3.1.124),用于公共预警(3.1.194)需要决策的活动(3.1.2)。

3.1.109

主办方　host

收到来自评审人(3.1.210)的反馈,并将之作为同行评审(3.1.171)的一部分的实体(3.1.88)。

注:实体可能是组织(3.1.162)、合作关系(3.1.170)、社区(3.1.37)、城市、地区、国家或其他机构。

3.1.110

色调　hue

视觉感觉与红色、黄色、绿色、蓝色之一或两种颜色组合相似的视觉感觉属性(3.2.5)。

3.1.111

人工解释　human interpretation

由检查员(3.2.24)评价的真实性。

3.1.112

人权　human rights

所有人固有的权利。

注 1:人人平等,享有不受歧视的人权。

注 2:人权是相互关联的,普遍的和不可剥夺的;相互依存,不可分割;平等和非歧视;享有权利和义务。

注 3:人权无论其国籍、居住地点、性别、民族或种族血统、肤色、宗教、语言或任何其他情况。

3.1.113

人权风险分析　human rights risk analysis;HRRA

人权风险评估　human rights risk assessment

人权影响评估　human rights impact assessment

人权风险和影响评估　human rights risk and impact assessment

识别、分析、评价人权相关风险(3.1.212)及其影响(3.1.115)并形成文件(3.1.74),以管理风险并预防或减轻不利的人权影响和违反法律的过程(3.1.187)。

注 1:人权风险分析是组织(3.1.162)要求(3.1.201)的一部分,该要求进行人权尽职调查,以识别、预防、减轻和说明其对人权的影响。

注 2:人权风险分析由相关的国际人权原则和公约构成,是组织全面风险评估(3.1.216)的基本组成部分。

注 3:人权风险分析包括对组织由于其安全运营(3.1.246)可能导致或促成的,或者通过组织的业务关系直接与组织的运营、项目或服务相关的,实际和潜在的人权影响的严重程度的分析等。人权风险分析过程宜考虑运营环境,应用必要的人权专业知识,并与可能面临权利风险的利益相关方(3.1.129)进行直接的、有意义的互动。

注 4:根据影响的严重程度,对人权影响的不利后果(3.1.43)进行评价和优先排序。

注 5:宜认识到人权风险可能会随着时间的推移而发生变化,并定期进行人权风险分析。

注 6:人权风险分析的复杂性(3.1.41)因组织规模、严重的人权影响风险以及运营的性质和环境(3.1.45)而异。

3.1.114

识别　identification

通过识别属性(3.2.5)来定义实体(3.1.88)的过程(3.1.187)。

3.1.115

影响　impact

冲扰(3.1.72)对目标(3.1.159)的作用结果。

3.1.116

影响分析　impact analysis

后果分析　consequence analysis

分析所有操作功能及操作中断可能对其影响的过程(3.1.187)。

注：影响分析，包括业务影响分析(3.1.24)，是风险评估(3.1.216)过程的一部分。影响分析识别损失和损害如何出现，事件(3.1.119)发生后的依次可能发生的损失或损害的潜在升级程度；使运营维持在可接受的最小水平所需的基本服务和资源(3.1.204)(包括人的、物理的和经济的)，以及应恢复的组织(3.1.162)的活动(3.1.2)、功能和服务的时间框架和范围。

3.1.117

公正性　impartiality

实际存在的或认识到存在的客观性。

注1：客观性意味着不存在或已解决利益冲突，不会对后续活动(3.1.2)产生不利影响；

注2：其他能用于表示公正性的术语有：客观、独立、无利益冲突、没有成见、无偏见、中立、公平、思想开放、平等、不受他人影响、平衡。

3.1.118

即兴活动　improvisation

几乎或完全没有准备的情况下对意外情况的反应。

注：例如发明，作曲或表演。

3.1.119

事件　incident

可能或将导致冲扰(3.1.72)、损失、突发事件(3.1.84)或危机(3.1.58)的事件(3.1.93)。

注：incident为可能引起负向后果的“事件”。本文件中将“incident”译为“事件”而非“事故”，以与《突发事件应对法》对突发事件的一般性表述一致。

3.1.120

事件指挥　incident command

作为事件管理体系(3.1.121)的一部分执行的，在事件(3.1.119)管理(3.1.141)期间逐步进行的过程。

3.1.121

事件管理体系　incident management system

规定了在事件(3.1.119)管理(3.1.141)过程中人员(3.1.176)的角色、职责和操作程序(3.1.186)的体系。

3.1.122

事件准备　incident preparedness

为事件响应(3.1.123)进行准备的活动(3.1.2)。

3.1.123

事件响应　incident response

为了阻止即将触发危险源(3.1.107)的成因和/或减轻潜在不稳定事件(3.1.93)或冲扰(3.1.72)的后果(3.1.44)，以及恢复到正常情况所采取的行动。

注：事件响应是应急管理(3.1.85)过程(3.1.187)的一部分。

3.1.124

信息　information

经处理、组织与关联而产生意义的数据。

3.1.125

基础设施　infrastructure

组织(3.1.162)运行所必需的设施(3.1.102)、设备和服务体系。

3.1.126

固有危险物　inherently dangerous property

如果在未经授权的人手中,将立即形成死亡或严重人身伤害威胁(3.1.274)的物品。

示例:致命武器、弹药爆炸物、化学制剂、生物制剂和毒素、核材料或放射性材料。

3.1.127

消息条　inject

输入演练活动的用于引起演练人员的反应以推动演练(3.1.94)的一段信息(3.1.124)。

注:消息条能通过书面、口头、视频或其他形式输入(例如传真、电话、电子邮件、声音、无线电广播或信号)。

3.1.128

完整性　integrity

保障资产(3.1.13)准确性和完全性的特性。

3.1.129

利益相关方　interested party

stakeholder

对决策或活动(3.1.2)产生影响、受到其影响,或自认为被影响的个人或组织(3.1.162)。

示例:消费者、所有者(3.1.166)、组织中的人员(3.1.176)、供货方、银行、监管方、工会、合作方或社团,存在竞争关系的社团或反对团体。

注 1:决策者可能是相关方。

注 2:受影响的社区和本地居民被视为利益相关方。

注 3:该术语是 ISO 管理体系标准的高级结构的通用术语和核心定义之一。通过补充示例和注,对原定义进行了修改。

3.1.130

内部攻击　internal attack

具有直接或间接关联的合法制造商、货物(3.3.8)原创者或权利所有人(3.1.211)(权利持有者、分包商、供应商等的员工)的人或实体(3.1.88)实施的攻击(3.2.4)。

3.1.131

内部审核　internal audit

为了管理(3.1.141)评审(3.1.208)或其他内部目的,由组织(3.1.162)自身或以组织名义进行的审核(3.1.14)。

注 1:在许多情况下,特别对一些小型组织,能够通过对被审核活动(3.1.2)不承担责任的来体现该活动的独立性。

注 2:内部审核能够作为组织自我合格(3.1.42)声明的基础。

3.1.132

国际供应链　international supply chain

在某些环节上跨越国际或经济体边界的供应链(3.1.268)。

注 1:从签订订单到目的地国家或经济体海关解除对货物(3.3.8)的控制,供应链的所有环节都是国际性的。

注 2:如果公约或地区协议免除了来自特定国家或经济体的产品报关,国际供应链的终点是进口国或进口经济体的进口岸。如果协议或公约没有此项规定,则产品在进口港需进行报关。

3.1.133

互通性　interoperability

〈多系统〉不同系统和组织(3.1.162)之间协同工作的能力。

3.1.134

互通性　interoperability

〈单一接入点〉单一接入点将具有唯一标识符(UID)(3.2.44)的对象(3.1.158)的查询路由到负责的权威来源(3.2.13),以实现可信验证功能(TVF)(3.2.43)的能力。

注:互通性包括多个安全验证系统向用户组传递类似响应的能力。

3.1.135

投资　investment

为实现既定目标(3.1.159)和其他效益(3.1.17)进行的资源(3.1.204)分配。

注:投资有两种主要形式:直接投资于建筑物、机器和类似资产(3.1.13);债券和股票等金融证券的间接支出。

3.1.136

调用　invocation

组织(3.1.162)宣布实施业务连续性(3.1.19)计划以继续提供关键产品和服务(3.1.188)的活动。

3.1.137

关键性能指标　key performance indicator;KPI

组织(3.1.162)用于衡量或比较绩效(3.1.174),用以实现其战略和运营目标(3.1.159)的可量化衡量指标。

3.1.138

滑坡　landslide

导致形成斜坡的物质(包括岩石、土壤、人工填充物质及其组合),向下和向外移动的各种过程(3.1.187)。

3.1.139

可能性　likelihood

某件事发生的机会。

注1:无论是以客观的或主观的、定性或定量的方式来定义、度量或确定,还是用一般词汇或数学术语来描述[如概率(3.1.185),或一定时间内的频率],在风险管理(3.1.221)术语中,"可能性"一词都用来表示某事发生的概率。

注2:"可能性"这一英语词汇在一些语言中没有直接与之对应的词汇,因此经常用"概率"这个词代替。不过,在英语中,"概率"常常被狭义地理解为一个数学词汇。因此,在风险管理术语中,宜应用"可能性"表达许多非英语语言中"概率"一词的含义。

3.1.140

逻辑结构　logical structure

优化给定用户(人或机器)的数据访问(3.1.1)或处理的数据排列。

3.1.141

管理　management

指挥与控制组织(3.1.162)的一系列协调活动(3.1.2)。

3.1.142

管理计划　management plan

通常涵盖实施管理(3.1.141)过程(3.1.187)所需的关键人员(3.1.176)、资源(3.1.204)、服务和行动的明确定义和记录的行动计划。

3.1.143

管理体系　management system

组织(3.1.162)建立方针、目标和过程(3.1.187)并实现这些目标(3.1.159)的相互关联或相互作用的

一组元素。

注 1：管理体系可能涉及一个或多个学科。

注 2：管理体系要素包括组织结构、角色和职责，以及计划(3.1.177)和实施。

注 3：管理体系的范围可能包括整个组织、组织内某些特定的职能、特定的部分，或是跨越多个组织的一个或多个职能。

注 4：该术语是 ISO 管理体系标准的高级结构的通用术语和核心定义之一。

3.1.144

管理体系咨询和/或相关的风险评估　management system consultancy and/or associated risk assessment

参与设计、实施或维护供应链(3.1.268)安全管理体系，以及实施风险评估(3.1.216)的活动。

示例：准备或编制手册或程序(3.1.186)；对供应链安全管理体系(3.1.143)的建立和实施提供具体的建议、指导或解决方案；实施内部审核(3.1.131)；进行风险评估与分析。

注：如果与供应链安全管理体系或审核有关的培训(3.1.277)课程仅限于提供可在公共场合自由获取的通用信息(3.1.124)，那么组织培训并作为培训者参与培训不被视为咨询，即培训者不针对特定的公司提出解决方案。

3.1.145

块体运动　mass movement

土壤、岩石、泥浆、雪或其混合物在重力作用下沿斜坡向下的位移。

3.1.146

物质产品　material goods

制造、种植的或由自然界获得的产品。

3.1.147

物质产品生命周期　material good life cycle

物质产品(3.1.146)的生命阶段。

注：物质产品生命周期包括构想、设计、制造、储存、服务、转售和处置。

3.1.148

最长可容忍中断时间　maximum tolerable period of disruption；MTPD

最大可接受中断　maximum acceptable outage；MAO

不能提供产品/服务，或者活动(3.1.2)无法进行可能带来的负面影响(3.1.115)，变得不能接受之前的时间。

3.1.149

测量　measurement

确定一个量值的过程(3.1.187)。

注：该术语是 ISO 管理体系标准的高级结构的通用术语和核心定义之一。

3.1.150

最小业务连续性目标　minimum business continuity objective；MBCO

组织(3.1.162)在冲扰(3.1.72)期间，为达到其业务连续性目标(3.1.159)而接受的最低标准的服务和(或)产品。

3.1.151

减缓　mitigation

限制特定事件(3.1.119)的任何负面后果(3.1.44)。

3.1.152

监测　monitoring

确定一个体系、过程(3.1.187)或活动(3.1.2)的状态。

注 1：可能需要通过检查、监督或密切观察来确定状态。

注 2：该术语是 ISO 管理体系标准的高级结构的通用术语和核心定义之一。

3.1.153

监测责任方　monitoring process owner

负责数据的接收、集成、生成、分析、传输和输出的个人或法人实体(3.1.88)。

注：监测过程(3.1.187)或监测过程中的系统所有者(3.1.166)可能由其代表，例如由分包商代表。

3.1.154

互助协议　mutual aid agreement

两个或多个实体(3.1.88)为了互相帮助而预先达成的共识。

3.1.155

指定紧急联系人　nominated emergency contact

在需要联系组织(3.1.162)时，被指定作为优先联系人的个人。

注：可能是合法亲属。

3.1.156

不符合　nonconformity

未满足要求(3.1.201)。

注：该术语是 ISO 管理体系标准的高级结构的通用术语和核心定义之一。

3.1.157

通知　notification

公共预警(3.1.194)中，为处于风险环境的人员(3.1.176)提供突发事件(3.1.84)应急决策和行动所需的基本信息(3.1.124)的活动。

3.1.158

对象　object

能够被识别的单一且不同的实体(3.1.88)。

3.1.159

目标　objective

想要取得的结果。

注 1：目标可能是战略的、战术的或操作层面的。

注 2：目标可能涉及不同学科[例如金融、健康、安全和环境目标)，并且应用于不同层级(例如战略、组织范围、项目、产品和过程(3.1.187)]。

注 3：目标可能用其他方式来表示，例如作为预期结果、意图、运行准则、作为业务连续性(3.1.19)的目标，或用其他意思相近的词来表达[例如指标(3.1.270)]。

注 4：在业务连续性管理体系(3.1.21)中，组织(3.1.162)根据业务连续性策略(3.1.178)确定业务连续性目标，以实现预期结果。

注 5：该术语是 ISO 管理体系标准的高级结构的通用术语和核心定义之一。

3.1.160

观察员　observer

见证演练(3.1.94)过程但独立于演练活动(3.1.2)的参与者(3.1.168)。

注：观察员能参与演练过程(3.1.187)评价(3.1.92)。

3.1.161

运营信息　operational information

已被情境化和分析的，用以了解情况及其可能的演化的信息(3.1.124)。

3.1.162

组织　organization

为了实现目标(3.1.159)形成的具有自身职能，按照一系列职责、权限和相互关系安排的个人或一组人员。

注 1：组织的概念包括但不限于个体商户、公司、集团、企事业单位、研究机构、合作关系(3.1.170)、慈善机构或是上述单位的结合体，无论其是否为联合的，公营还是私营的。

注 2：该术语是 ISO 管理体系标准的高级结构的通用术语和核心定义之一。

3.1.163

组织文化　organizational culture

有助于组织在所处的独特社会和心理环境中发挥积极作用的集体信念、价值观(3.1.284)，以及组织(3.1.162)的态度和行为。

3.1.164

组织韧性　organizational resilience

组织(3.1.162)在不断变化的环境中承受和适应能力。

3.1.165

外包　outsource

将组织的部分职能或过程(3.1.187)安排给外部组织(3.1.162)的活动。

注 1：虽然外包的职能和过程属于管理体系(3.1.143)的范围，但外部组织仍在此范围之外。

注 2：该术语是 ISO 管理体系标准的高级结构的通用术语和核心定义之一。

3.1.166

所有者　owner

对唯一标识符(UID)(3.2.44)相关联的对象(3.1.158)合法拥有许可、使用、分发等权限的实体(3.1.88)。

3.1.167

参量　parameter

描述系统元素的可测量指标或可描述的理论性特征。

3.1.168

参与者　participant

履行演练(3.1.94)相关职能的人员或组织(3.1.162)。

3.1.169

合作　partnering

为达到个体或集体的目标(3.1.159)而与其他组织在某一共同感兴趣的活动(3.1.2)或领域形成的协作。

3.1.170

合作关系　partnership

依据相关法律确定的两个机构(公共与公共、私人与公共、私人与私人)之间，关于预防和管理影响安全(3.1.236)和韧性(3.1.203)的事件(3.1.119)的范围、角色、程序(3.1.186)和工具的组织关系。

3.1.171

同行评审　peer review

评审人(3.1.210)检查主办方(3.1.109)绩效(3.1.174)，反馈分析领域(3.1.10)情况并基于自身环境(3.1.45)进行学习借鉴的过程(3.1.187)。

注 1：同行评审可能涵盖多个分析领域。

注 2：主办方能用“评估”“鉴定”或“分析”等同义词代替“评审”，以更好地描述活动(3.1.2)。

3.1.172

业务连续性的人因要素　people aspects of business continuity

用于最大程度地减少痛苦，最大化生产率和恢复(3.1.198)力，实现组织(3.1.162)业务连续性方案(3.1.23)中的恢复目标(3.1.159)的，与事件(3.1.119)涉及或受事件影响的人员管理(3.1.141)相关的元素。

3.1.173

处于风险的人　people at risk

可能受事件(3.1.119)影响的区域中的个人。

3.1.174

绩效　performance

可测量的结果。

注 1：绩效可能与定量或定性的结果有关。

注 2：绩效可能与管理活动(3.1.2)、过程(3.1.187)、产品(包括服务)、体系或组织(3.1.162)有关。

注 3：该术语是 ISO 管理体系标准的高级结构的通用术语和核心定义之一。

3.1.175

绩效评价　performance evaluation

根据设定的准则确定可测量结果的过程(3.1.187)。

3.1.176

人员　personnel

为组织(3.1.162)工作并受其管理的人。

注：人员的概念包括但不限于员工、兼职人员和派遣人员。

3.1.177

计划　planning

为实现组织的目标，设定目标(3.1.159)、指定必要的实施过程(3.1.187)和相关资源(3.1.204)的管理(3.1.141)体系的一部分。

3.1.178

策略　policy

由组织(3.1.162)最高管理者(3.1.276)正式表达的意图和方向。

注：该术语是 ISO 管理体系标准的高级结构的通用术语和核心定义之一。

3.1.179

准备　preparedness

准备就绪　readiness

在事件(3.1.119)发生前建立和实施的，旨在支持和提高与冲扰(3.1.72)、突发事件(3.1.84)或灾害(3.1.70)相关的预防(3.1.180)、保护(3.1.190)、减缓(3.1.151)、响应和恢复(3.1.198)活动(3.1.2)、程序和体系。

3.1.180

预防　prevention

使组织(3.1.162)能够避免、排除或限制不良事件(3.1.278)或潜在冲扰(3.1.72)影响(3.1.115)的措施。

3.1.181

预防危险源和威胁　prevention of hazards and threats

用于避免、减少或控制任何类型的危险源(3.1.107)和威胁(3.1.274)及其相关风险(3.1.212),减少其潜在可能性(3.1.139)或后果(3.1.44)的过程(3.1.187)、实践、技术、材料、产品、服务或资源(3.1.204)。

3.1.182

预防措施　preventive action

为消除潜在不符合(3.1.156)或其他潜在不良情况的原因所采取的措施。

注 1:一个潜在不符合可能由多个原因导致。

注 2:采取预防措施是为了防止发生,而采取纠正措施(3.1.53)是为了防止再次发生。

3.1.183

优先活动　prioritized activity

在冲击期间,为避免不可接受的业务影响而紧急开展的活动(3.1.2)。

3.1.184

私人安全服务提供商　private security service provider;PSSP

私人安保公司　private security company;PSC

业务活动(3.1.2)包括代表自身或其他组织提供安全(3.1.236)服务,实施或签订安全运营(3.1.246)合同的组织(3.1.162)。

注 1:私人安全服务提供商为客户(3.1.31)提供旨在确保客户或其他人安全的服务。

注 2:私人安全服务提供商通常在政府治理薄弱,或由于人为或自然事件(3.1.93)导致法治受损的情形下工作。按照合同条款能要求其工作人员(3.1.176)在履行职责绩效(3.1.174)时携带武器。

注 3:私人安全服务提供商提供的安全服务示例包括:警卫、近距离保护、实物保护、安全知识教育和培训(3.1.277)、风险(3.1.212)评估、安全评估、威胁(3.1.274)评估,为个人、外交和住宅周边提供保护性和防御性措施,运输护送,策略(3.1.178)分析。

注 4:合作企业被视为该组织的一部分。

3.1.185

概率　probability

对事件发生机会的度量。

注 1:参见可能性(3.1.139)。

注 2:概率用 0 到 1 之间的数字表示。0 表示不可能发生,1 表示确定发生。

3.1.186

程序　procedure

为进行某项活动(3.1.2)或过程(3.1.187)所规定的途径。

注 1:可能记录或不记录程序。

注 2:当程序被记录时,常称之为"记录程序"或"文档化程序"。包括程序的文档可能称为"程序文档"。

3.1.187

过程　process

将输入转化为输出的相互关联或相互作用的一组活动(3.1.2)。

注 1:该术语是 ISO 管理体系标准的高级结构的通用术语和核心定义之一。

注 2:在物流领域中,将 process 译为"加工"(参考 GB/T 18354—2021 中的 8.32、8.33 等)。本文件中"3.3 供应链相关术语"与物流密切相关,因此将 3.3 中提及的"3.1.187 process"译为"加工",其他条中提及的"3.1.187 process"译为"过程"。

3.1.188

产品和服务　product and service

组织(3.1.162)向利益相关方提供的产出或成果。

示例：制成品、汽车保险和社区护理。

3.1.189

产品欺诈　product fraud

利用物质产品(3.1.146)牟取金钱或个人利益的非法或犯罪性欺骗。

注 1：欺诈是指对经济或个人收益造成损失，对社会和经济造成危害的非法或犯罪性欺骗。

注 2：产品包括物质产品携带的电子媒体。

注 3：应单独考虑与数字化传输的电子媒体有关的欺诈行为。

3.1.190

保护　protection

保障组织(3.1.162)安全，并使其减少受到潜在冲扰(3.1.72)影响(3.1.115)的措施。

3.1.191

严重心理事件　psychological critical incident

可能导致严重的情绪或身体不适、心理障碍或正常行为障碍的单一或一系列事件(3.1.93)。

注：在该领域工作的心理健康专业人员通常将“创伤事件”称为严重心理事件。术语“严重心理事件”易于接受，因为它暗示了可能对参与者造成或不造成伤害的事件(3.1.119)。尽管在精神和科学界对创伤事件有几种定义，但“严重心理事件”的定义更符合实际。

3.1.192

心理教育　psychological education

提供有关心理健康的建议和指导。

注：通常包括对痛苦事件(3.1.93)的常见反应的概述以使其正常化，减少焦虑，提供最近几天简单的自我恢复建议，以及关于何时何处寻求进一步支持的建议。

3.1.193

心理急救　psychological first aid

类似于物理急救概念的临时的支持性心理干预。

注：其目标包括使危机(3.1.58)情况趋于稳定，减少情绪困扰，提供有关自我保健和心理教育(3.1.192)的建议，确定需要专业帮助的人员并在必要时寻求进一步的帮助 。

3.1.194

公共预警　public warning

作为事件响应措施发布的，使应急响应人和处于风险的人(3.1.173)采取安全措施的通知(3.1.157)和警报(3.1.6)信息。

注：公共预警包括提高公众应急意识和理解，或提供应急建议或强制性指令的信息(3.1.124)。

3.1.195

公共预警系统　public warning system

在突发事件(3.1.84)过程中，基于公共预警(3.1.194)策略(3.1.178)向处于风险的人(3.1.173)和第一响应人发送通知(3.1.157)和警报(3.1.6)消息的一套协议、过程(3.1.187)和技术。

3.1.196

原材料　raw material

物质产品(3.1.146)的要素、组成或部分。

3.1.197

记录　record

说明取得结果或证明活动(3.1.2)执行的文件(3.1.74)。

3.1.198

恢复　recovery

对受影响组织(3.1.162)的业务、设施(3.1.102)、生计或生活条件进行恰当的修复和改善,并尽力削弱风险(3.1.212)因素的活动。

3.1.199

恢复点目标　recovery point objective;RPO

恢复活动(3.1.2)信息到特定的点。

注:也可能被称为"最大数据损失"。

3.1.200

恢复时间目标　recovery time objective;RTO

事件(3.1.119)发生后,恢复产品和服务(3.1.188)或活动(3.1.2),或者恢复资源(3.1.204)的时间段。

注:对于产品、服务和活动,恢复时间目标小于组织不能接受的导致产品/服务停止供应、活动无法执行等负面影响(3.1.115)所需的时间。

3.1.201

要求　requirement

明确表述的、一般性隐含的或必须履行的需求和期望。

注 1:"一般性隐含"是隐含的需求或期望,对于组织(3.1.162)或利益相关方(3.1.129)的而言是惯例或一般做法。

注 2:规定要求是明确表述的要求,如记录信息(3.1.124)。

注 3:该术语是 ISO 管理体系标准的高级结构的通用术语和核心定义之一。

3.1.202

剩余风险　residual risk

保留风险　retained risk

风险处置(3.1.229)之后仍然存在的风险(3.1.212)。

注:剩余风险可能包括未识别的风险。

3.1.203

韧性　resilience

承受和适应环境变化的能力。

注:在城市韧性(3.1.281)的环境(3.1.45)下,在变化环境中的承受和适应能力由对威胁(3.1.274)的预测、准备和恢复等能力,以及城市系统(3.1.282)各部分的能力综合确定。

3.1.204

资源　resource

组织(3.1.162)为满足运行和实现目标(3.1.159)而需要的所有资产(3.1.13)(包括工厂和设备),包括人、技能、技术、场所、供应品和信息(3.1.124)(电子的或非电子的)。

3.1.205

响应计划　response plan

为事件(3.1.119)响应而编制、编译和维护的程序(3.1.186)和信息的(3.1.124)文件集合。

3.1.206

响应方案　response programme

为开展维护和保护生命、财产、运营和关键资产(3.1.13)的活动而准备的计划、过程(3.1.187)和资

源(3.1.204)。

注：响应步骤一般包括事件(3.1.119)识别、通知(3.1.157)、评估、声明、计划执行、通讯和资源管理(3.1.141)。

3.1.207

响应队伍　response team

负责制定、执行、演练和维护包括过程(3.1.187)和程序(3.1.186)在内的响应计划(3.1.205)的群体。

3.1.208

评审　review

为实现既定目标(3.1.159)而进行的决定管理体系(3.1.143)及其组成要素的适宜性、充分性和有效性(3.1.83)的活动(3.1.2)。

3.1.209

评审活动　review visit

评审人(3.1.210)参加的在主办方(3.1.109)所在地开展的同行评审(3.1.171)活动(3.1.2)。

注：评审活动包括演示、个人访谈、焦点小组讨论、实地访问以及对现场和桌面演练(3.1.94)的观察。

3.1.210

评审人　reviewer

基于专业知识和经验，提供分析领域(3.1.10)的同行评审反馈的实体(3.1.88)。

注：实体可能是组织(3.1.162)、合作关系(3.1.170)方、社区(3.1.37)、城市、区域、国家或其他机构。

3.1.211

权利所有人　rights holder

持有或授权使用一项或多项知识产权的法定实体(3.1.88)。

3.1.212

风险　risk

不确定性对目标(3.1.159)的影响。

注 1：该影响导致偏离预期。可能是正面的、负面的或两者兼有，能够应对、创造或导致机会和威胁(3.1.274)。

注 2：目标可能有不同的方面和类别，并能够应用于不同的层级。

注 3：风险常被表述为风险源(3.1.227)、潜在事件(3.1.93)、后果(3.1.43)及其可能性(3.1.139)。

注 4：该术语是 ISO 管理体系标准的高级结构的通用术语和核心定义之一。

3.1.213

风险接受　risk acceptance

接受某一特定风险(3.1.212)的决定。

注 1：风险接受可能在不经风险处置(3.1.229)或在风险处置过程(3.1.187)中发生。

注 2：对接受的风险进行监测(3.1.152)和评审(3.1.208)。

3.1.214

风险分析　risk analysis

理解风险(3.1.212)性质、确定风险等级的过程(3.1.187)。

注 1：风险分析是风险评价(3.1.219)和风险处置(3.1.229)策略的基础。

注 2：风险分析包括风险估计。

3.1.215

风险偏好　risk appetite

组织(3.1.162)愿意接受或承担风险(3.1.212)的数量和类别。

3.1.216

风险评估　risk assessment

包括风险识别(3.1.220)、风险分析(3.1.214)和风险评价(3.1.219)的全过程(3.1.187)。

注 1：风险评估包括识别内部和外部威胁(3.1.274)和脆弱性，识别由这些威胁和脆弱性引起的事件(3.1.93)的可能性(3.1.139)和影响(3.1.119)，明确组织(3.1.162)持续运营所需的关键功能，明确减小风险暴露需要控制的区域，并评估区域控制所需成本。

注 2：ISO 31000:2018 中对风险评估有详细规定。

3.1.217

风险沟通　risk communication

在决策者和其他利益相关方(3.1.129)之间的风险(3.1.212)信息(3.1.124)交换。

注：信息可能与风险的存在、属性、形式、概率(3.1.185)、严重度、可接受性、处置或其他方面有关。

3.1.218

风险准则　risk criteria

评价风险(3.1.212)重要性的依据。

注 1：基于组织的目标(3.1.159)、外部环境和内部环境确定风险准则。

注 2：风险准则可能源于标准、法律、策略(3.1.178)和其他要求(3.1.201)。

3.1.219

风险评价　risk evaluation

对比风险分析(3.1.214)结果和风险准则(3.1.218)，以确定风险(3.1.212)和/或其大小是否可以接受或容忍的过程(3.1.187)。

注：风险评价有助于风险处置(3.1.229)决策。

3.1.220

风险识别　risk identification

发现、确认和描述风险(3.1.212)的过程(3.1.187)。

注 1：风险识别包括对风险源(3.1.227)、事件(3.1.93)及其原因和潜在后果(3.1.43)的识别(3.1.114)。

注 2：风险识别可能涉及历史数据、理论分析、专家意见以及利益相关方(3.1.129)的需求。

3.1.221

风险管理　risk management

指导和控制一个组织(3.1.162)相关风险(3.1.212)的协调活动(3.1.2)。

3.1.222

风险减缓　risk mitigation

减少或最小化危险事件(3.1.93)的不利影响(3.1.115)。

3.1.223

风险责任人　risk owner

具有管理风险(3.1.212)的责任和权力的实体(3.1.88)。

3.1.224

风险降低　risk reduction

为降低与风险(3.1.212)相关的概率(3.1.185)、负面后果(3.1.43)或两者兼有的情况而采取的行动。

3.1.225

风险登记　risk register

已识别风险(3.1.212)的信息(3.1.124)记录(3.1.197)。

注：风险评估(3.1.216)过程(3.1.187)中风险识别、分析和评价的相关信息，内容包括可能性(3.1.139)、后果(3.1.43)、处置和风险责任人(3.1.223)等。

3.1.226

风险分担　risk sharing

与其他相关方按协议分配风险(3.1.212)的风险处置(3.215)形式。

注 1：法律、法规要求(3.1.201)可能会限制、禁止或强制进行风险分担。

注 2：风险分担能通过保险或其他形式的合同实现。

注 3：风险分配的程度取决于分担方案的可信性和明确性。

注 4：风险转移是风险分担的一种形式。

3.1.227

风险源　risk source

可能单独或共同引发风险(3.1.212)的要素。

3.1.228

风险承受能力　risk tolerance

为实现目标(3.1.159)，组织(3.1.162)或利益相关方(3.1.129)在风险处置(3.1.229)之后做出的承担风险(3.1.212)的准备。

注：风险承受能力会受到客户(3.1.31)、利益相关者、法律和法规要求的影响。

3.1.229

风险处置　risk treatment

处理风险(3.1.212)的过程。

注 1：风险处置可能包括：

——通过不开始或不再继续导致风险的活动(3.1.2)来规避风险；

——为寻求机会而承担或增加风险；

——消除风险源(3.1.227)；

——改变可能性(3.1.139)；

——改变后果(3.1.43)；

——与其他一方或多方分担风险(包括合同和风险融资)；

——慎重考虑后决定保留风险。

注 2：针对负面后果的风险处置有时指“风险减缓”“风险消除”“风险预防”和“风险降低(3.1.224)”。

注 3：风险处置可能产生新的风险或改变现有风险。

3.1.230

鲁棒性　robustness

系统抵御虚拟或物理、内部或外部攻击(3.2.4)的能力。

注：特别是抵制企图模仿、复制、入侵或绕过原路径的能力。

3.1.231

情景　scenario

预先设定、推动演练(3.1.94)实施的过程情节。

注：情景能促进实现演练项目绩效(3.1.174)目标(3.1.159)。

3.1.232

演练范围　scope of exercise

反映演练需求与目标(3.1.159)的规模、资源(3.1.204)与内容。

3.1.233

服务范围　scope of service

供应链中的组织(3.3.9)执行的一项或多项功能及其对应的场合。

3.1.234

脚本　script

当演练(3.1.94)按照事件(3.1.93)列表中内容要素进行时，用于帮助指导工作人员理解事件应当如何发展的演练文本。

注：脚本通常是叙述模拟事件的书面文稿。

3.1.235

秘密　secret

防止向未经授权的实体披露的数据和/或知识。

3.1.236

安全　security

遵循程序(3.1.186)或实施合适的措施后，不被危险影响或不受威胁(3.1.274)的状态。

3.1.237

安全因素　security aspect

能够降低无意、故意和自然引发的，导致产品和服务(3.1.188)、运行、组织(3.1.162)及其利益相关方(3.1.129)的关键资产(3.1.13)和连续性(3.1.48)产生中断或后果(3.1.43)的风险(3.1.212)的特征、要素或属性。

3.1.238

安全排查　security cleared

验证接触安全敏感信息(3.1.257)的人员的可信度的过程(3.1.187)。

3.1.239

安全声明　security declaration

业务伙伴(3.3.3)做出的关于实施的安全(3.1.236)措施的书面承诺。

注 1：供应链中的组织(3.3.9)将使用安全声明评价与产品安全措施是否充分。

注 2：安全声明的内容至少包括如何保护国际贸易中的货物(3.3.8)、器具和相关的信息(3.1.124)，以及如何证实和确认安全措施。

3.1.240

安全事件　security incident

产生后果(3.1.44)的行动或环境。

3.1.241

安全管理　security management

组织(3.1.162)指导和控制安全(3.1.236)和韧性(3.1.203)的协调活动(3.1.2)。

3.1.242

安全管理目标　security management objective

实现安全管理策略(3.1.243)所需的特定安全(3.1.236)结果或成果。

注：有必要将这些结果直接或间接地与向消费者或最终用户提供的商品、供应和服务相关联。

3.1.243

安全管理策略　security management policy

与组织安全(3.1.236)及其过程(3.1.187)和活动(3.1.2)的控制框架相关的，与组织的策略(3.1.178)和规定要求(3.1.201)一致的，组织(3.1.162)的总体意图和方向。

3.1.244

安全管理方案　security management programme

实现安全管理目标(3.1.242)的过程(3.1.187)。

3.1.245

安全管理指标　security management target

实现安全管理目标(3.1.242)所需的具体绩效(3.1.174)水平。

3.1.246

安全运营　security operation

与保护(3.1.190)人民、有形和无形资产(3.1.13)相关的活动(3.1.2)和功能。

注 1：安全(3.1.236)操作可能要求在履行职责实现绩效(3.1.174)时携带和使用武器。

注 2：该概念包括国际行为准则(ICoC)对安全服务的定义：保卫和保护人和对象(3.1.158)，如输送工具、设施(3.1.102)、指定场所、财产或其他方面(无论武装与否)，或工作人员(3.1.176)在履行职责时必须携带或操作武器的任何其他活动。

3.1.247

安全运营管理　security operations management

指导和控制组织(3.1.162)安全运营(3.1.246)的协调活动(3.1.2)。

注：安全运营管理的指导和控制活动一般包括制定策略(3.1.178)、计划(3.1.177)和确定目标(3.1.159)，以指导操作过程(3.1.187)和持续改进(3.1.47)。

3.1.248

安全运营目标　security operations objective

与安全运营(3.1.246)有关的目标(3.1.159)。

注 1：安全运营目标通常基于组织(3.1.162)的安全运营策略(3.1.250)。

注 2：通常根据组织的相关功能和水平确定安全运营目标。

3.1.249

安全运营人员　security operations personnel

代表组织(3.1.162)直接或间接从事安全运营(3.1.246)活动的人员。

3.1.250

安全运营策略　security operations policy

由最高管理者(3.1.276)正式表达的，与安全运营(3.1.246)相关的组织(3.1.162)的总体宗旨和方向。

注 1：一般地，安全运营策略与组织的总体策略一致，并提供确定安全运营目标(3.1.248)的框架。

注 2：本文件中的安全运营管理(3.1.247)原则，能作为建立符合国际行为准则(ICoC)和蒙特勒文件中概述的原则和义务的安全运营策略的基础。

3.1.251

安全运营方案　security operations programme

由最高管理者(3.1.276)支持的持续的管理(3.1.141)和治理过程(3.1.187)，并确保实现安全运营(3.1.246)体系目标(3.1.159)的必要协调活动所需的资源。

3.1.252

安全人员　security personnel

供应链中的组织(3.3.9)中承担安全(3.1.236)相关职责的人员。

注：这些人可能是组织(3.1.162)的员工。

3.1.253

安全计划　security plan

确保安全(3.1.236)管理充分实施的计划安排。

注 1：通过采取安全措施，保护组织(3.1.162)免受安全事件(3.1.240)的影响。

注 2：安全计划可能包含在其他运营计划中。

3.1.254

安全敏感信息　security sensitive information

安全敏感材料　security sensitive material

由供应链(3.1.268)安全过程(3.1.187)产生的或纳入供应链安全过程的信息(3.1.124)或资料。

注：安全敏感信息/安全敏感材料包含有关安全(3.1.236)过程、装运或政府指令，以及不便公开或可能被某些人利用制造安全事件的信息。

3.1.255

安全威胁情景　security threat scenario

可能发生潜在安全事件(3.1.240)的情况。

3.1.256

自我保护　self-defence

保护(3.1.190)自身或个人财产免受它方伤害的活动。

3.1.257

敏感信息　sensitive information

由于可能对组织(3.1.162)、国家安全或公共安全产生不利影响而不能公开披露的信息(3.1.124)。

3.1.258

就地避险(名词)　shelter in place(noun)

在事件(3.1.119)期间，为保护人员安全，将人员转移到建筑物/场所内的预定区域的行动。

注：也称为“疏散”。

3.1.259

就地避险(动词)　shelter in place(verb)

在与风险(3.1.212)相关的受保护位置停留或立即避险。

3.1.260

冲击　shock

不确定的、突然的或长期的，可能会影响(3.1.115)城市系统(3.1.282)的目标(3.1.159)的事件(3.1.93)。

3.1.261

模拟　simulation

通过一个系统或过程(3.1.187)的功能来模仿性表达。

3.1.262

社会保护　social protection

预防、管理和克服不利于人们福祉的情况。

注：通过促进有效的劳动力市场、减少人们承受的风险(3.1.212)、增强经济和社会风险(如失业、排斥、疾病、残疾和老龄化)的管理能力(3.1.25)，来减轻贫困和脆弱性(3.1.287)的策略和计划。

3.1.263

源　source

自身或组合后具有潜在风险(3.1.212)的事物。

注 1：来自 ISO/Guide 73:2009 中的 3.5.1.2。

注 2：风险源(3.1.227)可能是有形的或无形的。

3.1.264

自发志愿者　spontaneous volunteer;SV

不属于现有事件(3.1.119)响应组织或自愿组织，未经预先计划即对事件的响应和恢复(3.1.198)提供支持的个人。

注：自发志愿者也可能称为聚集志愿者、临时志愿者、偶发志愿者、短期志愿者或非附属志愿者。

3.1.265

战略演练　strategic exercise

涉及最高管理者(3.1.276)的战略层面的演练(3.1.94)。

注 1：战略层面的高层管理层通常包括部际危机(3.1.58)工作人员(3.1.176)、行政人员、跨部门管理(3.1.141)人员，以及企业管理团队的危机管理(3.1.59)组织(3.1.162)。

注 2：战略演练旨在评估极端情况下的危机响应。

注 3：战略演练旨在为公共、私营和非营利部门的组织建立全面的协调(3.1.51)和决策文化。

3.1.266

压力　stress

城市系统(3.1.282)的长期和持续的动态压力，对系统实现目标(3.1.159)的能力(3.1.25)具有潜在的累积影响(3.1.115)。

3.1.267

分包　subcontracting

就履行现有合同的部分义务与外部方签订合同。

注 1：当一方签订需执行一系列服务的合同时，它能将一项或多项服务分包给“分包商”或当地组织。

注 2：母公司的子公司可能被视为分包组织(3.1.162)。

3.1.268

供应链　supply chain

活动(3.1.2)中的组织(3.1.162)、人员、过程(3.1.187)、物流、信息(3.1.124)、技术和资源(3.1.204)的，以及通过得到产品和服务(3.1.188)而获取材料进而创造价值的双向关系。

注：供应链可能包括供应商、分包商、制造商、物流服务商、内部配送中心、分销商、批发商和其他关联最终用户的实体。

3.1.269

供应链连续性管理　supply chain continuity management；SCCM

业务连续性管理(3.1.20)在供应链(3.1.268)中的应用。

注 1：业务连续性管理宜适用于组织(3.1.162)供应链的所有层级。

注 2：实际上，组织通常只将其应用于供应商的第一层，并影响关键供应商进而使其相关的供应商应用供应链连续性管理。

3.1.270

指标　target

适用于组织(3.1.162)或其部分的，为实现其目标(3.1.159)而需设定或满足的具体绩效(3.1.174)要求(3.1.201)。

3.1.271

目标组　target group

接受演练(3.1.94)的个人或组织(3.1.162)。

3.1.272

测试(动词)　**test**(verd)

在设定演练目标(3.1.159)时设定了通过或不通过要素的特殊类型的演练(3.1.94)。

注：术语“测试”(动词)和“测试”(名词)(3.1.273)与“演练”(动词)和“演练”(名词)不同。

3.1.273

测试(名词)　**testing** (noum)

用以确定某事物的存在、质量或真实性的评价(3.1.92)程序(3.1.186)。

注 1：测试可能称为“试验”。

注 2：测试经常被用于支持计划。

3.1.274

威胁　threat

可能对个人、资产(3.1.13)、体系或组织(3.1.162)，环境或社区(3.1.37)造成伤害的不良事件(3.1.278)的潜在原因。

3.1.275

威胁分析　threat analysis

识别、定性和定量评价不良事件(3.1.278)的潜在原因的过程(3.1.187)。这些不良事件可能导致对个人、资产(3.1.13)、系统或组织(3.1.162)、环境或社区(3.1.37)的危害。

3.1.276

最高管理者　top management

在最高层指挥和控制组织(3.1.162)的一个人或一组人。

注 1：最高管理者有权力在组织内进行授权，并提供资源(3.1.204)。

注 2：如果管理体系(3.1.143)的范围只涵盖了组织的一部分，那么最高管理者指那些直接指导和控制该部分组织的人。

注 3：该术语是 ISO 管理体系标准的高级结构的通用术语和核心定义之一。

3.1.277

培训　training

旨在促进知识、技术和能力的学习与发展，提高完成特定任务或履行特定角色的绩效(3.1.174)的活动(3.1.2)。

3.1.278

不良事件　undesirable event

可能导致伤亡、有形或无形资产(3.1.13)损害，或对内部或外部利益相关方(3.1.129)的人权(3.1.112)和基本自由产生负面影响(3.1.115)的事件或变化。

3.1.279

城市群　urban agglomeration

城市区域或连续性(3.1.48)的大型城镇聚落的物理结构和组成。

注：这些区域或聚落建成区和拓展城镇区域、中心区域、郊区的人口由可持续的、相邻的城市发展相联系。

3.1.280

城市开放区　urban open area

城市边界内的公共或私人空置区域。

注 1：城市开放区域是指在城市系统(3.1.282)的范围和参量(3.1.167)中关联的所有边缘开放空间和可确定的开放空间。

注 2：本文件不将省公园、国家公园或超出城市范围的农村地区的空地视为城市开放区。

3.1.281

城市韧性　urban resilience

在变化的环境中，任何城市系统(3.1.282)及其居民在预测、准备、响应和吸收冲击(3.1.260)，面对压力(3.1.266)和挑战(3.1.29)时积极适应和转变，同时促进包容性和可持续发展的能力。

注 1：更具韧性的城市系统的特征在于，能够在短期到中期内持续应对冲扰(3.1.72)，同时有能力(3.1.25)减轻压力并适应变化和风险(3.1.212)，并能抓住机遇。因此，城市韧性不仅取决于城市系统应对冲击的能力，还取决于长期承受压力和挑战的能力。

注 2：城市韧性取决于复杂城市系统各个组成部分的单独和组合的韧性(3.1.203)。尽管城市区域内的市区、城镇或

社区(3.1.37)可能在各自边界内表现出更高的韧性,但城市韧性涵盖了城市群(3.1.279)的更广泛的地理范围。城市系统的韧性是通过每个独立的系统组成部分的韧性能力(3.1.25)来衡量的,并取决于系统范围内城市群中最弱的韧性。

注 3:宜通过定性和定量数据来衡量和分析城市系统的韧性,以便在系统遭受冲击、压力和挑战时评估韧性,计划并采取相应的行动。

3.1.282

城市系统　urban system

人类居住区、系统组件的集成和复杂集合,在物理、功能、组织和空间等维度具有普遍和相互依赖特征,并由经有效治理机制管理的人员、过程(3.1.187)和资产(3.1.13)组成。

注 1:城市系统的组成和要素是动态的,会随时间而变化。

注 2:无论规模、文化、位置、经济和/或政治环境,每个城市区域都具有城市系统的特征。

注 3:以城市系统为特征,城市地区确定管理其多个组成部分之间复杂的相互作用和相互依赖性的目标(3.1.159),以实现社会、经济、文化和环境等各方面的功能。

3.1.283

使用持续性力量　use of force continuum

为应用合理且必要的持续力度响应逆变而增加或减少力量水平的活动。

注 1:使用的力量宜为消除威胁(3.1.274)所需的最小合理量,从而最大限度地降低风险(3.1.212)和可能发生的伤害的严重程度。

注 2:宜在适合当前情况,确保响应能在几秒钟内从连续体的一部分移动到另一部分的前提下,增加或降低力量水平。

3.1.284

价值观　values

组织(3.1.162)遵守的信念和力求符合的标准。

3.1.285

核实　verification

通过提供证据对符合规定要求(3.1.201)的认定。

3.1.286

视频监控　video-surveillance

以视频方式开展的监控。

3.1.287

脆弱性　vulnerability

脆弱性分析　vulnerability analysis

识别和量化关于可能导致后果(3.1.43)的风险(3.1.212)源的敏感性的过程(3.1.187)。

3.1.288

脆弱性评估　vulnerability assessment

识别和量化脆弱性的过程(3.1.187)。

3.1.289

脆弱性群体　vulnerable group

具备一个或几个使其受到歧视或处在不利的社会、经济、文化、政治或健康环境,进而导致缺乏实现权利或享受平等机会的特征的群体。

3.1.290

弱势群体　vulnerable person

对于突发事件(3.1.84)影响(3.1.115)的预测、应对、抵抗或恢复能力较弱的个人。

注：在本文件中，根据突发事件(3.1.84)中的个人情况，而非脆弱性(3.1.287)的性质来定义弱势群体。

3.1.291

警报发布功能　warning dissemination function

根据基于危险源监测功能(3.1.108)获取的有依据的信息(3.1.124)，向处于风险的人(3.1.173)发布适当信息的活动(3.1.2)。

3.1.292

工作环境　work environment

工作时所处的一组条件

注：条件包括物理的、社会的、心理的和环境的因素(如温度、照明、识别方案、职业压力、人类工效学和大气成分)。

3.1.293

劳动力　workforce

致力于实现组织(3.1.162)目标(3.1.159)的个人。

注：劳动力包括直属员工、代理机构员工、承包商和志愿者。

3.1.294

世界海关组织　World Customs Organization；WCO

以提高海关当局的有效性(3.1.83)和效率为使命的独立于政府间的机构。

注：世界海关组织是处理海关事务的唯一的全球政府间组织(3.1.162)。

3.2　反伪造税票相关术语

3.2.1

激活　activation

可用税款(3.2.3)到期时，税票(3.2.39)的生产和使用阶段。

注：唯一标识符(UID)(3.2.44)的激活能和税票的激活分开进行。

3.2.2

篡改　alteration

蓄意用化学方法、物理磨损或是其他技术试图改变有效事项或事项包含的数据的活动。

注：本文件中，事项是指税票(3.2.39)。

3.2.3

可用税款　applicable tax

国家、省、市或地方法律中规定的产品的消费税或其他财政税款。

3.2.4

攻击　attack

成功或者不成功地试图规避验证方案(3.2.11)的行为。

注：攻击包括试图效仿、伪造或复制验证要素(3.2.9)。

3.2.5

属性　attribute

构成对象(3.1.158)特征识别(3.1.114)和验证体系的信息(3.1.124)类型。

3.2.6

属性数据管理系统　attribute data management system；ADMS

存储、管理和控制对象(3.1.158)相关数据的访问(3.1.1)的系统。

3.2.7

真实的物料　authentic material good

在合法制造商、货物（3.3.8）原产地和权利所有人(3.1.211)的控制下生产的物质产品(3.1.146)。

3.2.8

验证　authentication

以特定的或可理解的保证水平证实一个实体(3.1.88)或属性(3.2.5)的过程(3.1.187)。

注1：本文件中的实体是指税票(3.2.39)。

注2："特定的或可理解的保证水平"是指验证任何物品都不可能达到完全确认的情况。确认水平因为使用的验证方案(3.2.11)、验证人员的培训(3.1.277)情况和验证检查动机、可用设备的不同而不同。例如，消费者和司法的(3.1.103)实验室提供的验证水平就大不相同。

3.2.9

验证要素　authentication element

与物质产品(3.1.146)或其包装相关的有形对象(3.1.158)、可视特征或信息(3.1.124)。

注：验证要素能作为验证方案(3.2.11)的一部分。

3.2.10

验证功能　authentication function

执行验证(3.2.8)的功能。

3.2.11

验证方案　authentication solution

对物质产品(3.1.146)进行验证的一套完整的方法与程序(3.1.186)。

3.2.12

验证工具　authentication tool

防伪解决方案中，用于控制验证要素(3.2.9)的一套硬件和/或软件系统。

3.2.13

权威来源　authoritative source

维护属性(3.2.5)的正式的属性起源。

3.2.14

自动评估　automated interpretation

通过验证方案(3.2.11)的一个或多个组件自动评估真实性的过程(3.1.187)。

3.2.15

隐式验证要素　covert authentication element

通常是人类感官不可见的，能由知情人员使用工具或自动评估(3.2.14)进行揭示的验证元素(3.2.9)。

3.2.16

保管副本　custodian copy

从属权威来源(3.2.13)的副本。

3.2.17

直接标记　direct marking

通过使用激光标记、墨水印刷或其他标记直接在产品容器上印刷税票(3.2.39)。

3.2.18

错误接受率　false acceptance rate

将错误的验证(3.2.8)判定为正确的比例。

3.2.19

错误拒绝率　false rejection rate

将正确的验证(3.2.8)判定为错误的比例。

3.2.20

鉴证分析　forensic analysis

通过具有专门知识的熟练专家使用专业设备来确认验证要素(3.2.9)或内在属性(3.2.5),从而对物质产品(3.1.146)进行验证的科学方法。

3.2.21

识别码　identifier

为识别(3.1.114)实体(3.1.88)而分配给其的一组指定的属性(3.2.5)。

3.2.22

特征　identity

与实体(3.1.88)相关的一组属性(3.2.5)

注 1:特征可能具有使对象(3.1.158)与所有其他对象区分开的唯一属性。

注 2:能从人、组织(3.1.162)和对象(有形的和无形的)的角度来查看特征。

3.2.23

非法产品　illicit product

为避免支付全部或部分可用税款(3.2.3)而提供给市场的应税消费品。

注 1:作为风险评估(3.1.216)的一部分,税务机关(3.2.38)宜参考其辖区内的法律和法规,以确定哪些产品属于非法产品。

注 2:非法产品包括非法制造、掺假、重新填充、走私或非法进口的产品等。

3.2.24

检查员　inspector

使用目标检查功能(3.2.29)来评估对象(3.1.158)的人员。

3.2.25

检查员访问历史　inspector access history

对何时检查了唯一标识符(UID)(3.2.44),选择了由哪个(特权)检查员(3.2.24)检查,选择了从哪个特定位置进行检查的访问日志的详细说明。

注:通常使用时间标记。

3.2.26

集成验证要素　integrated authentication element

附加到物质产品(3.1.146)中的验证要素(3.2.9)。

3.2.27

固有验证元素　intrinsic authentication element

物质产品(3.1.146)固有的验证要素(3.2.9)。

3.2.28

主要利益相关方　lead interested party

组织对象(3.1.158)识别(3.1.114)和安全验证系统(I-P)互通性(3.1.134)的单个利益相关方(3.1.129),管理 I-OP 的一组利益相关方或专门的法人实体(3.1.88)。

3.2.29

目标检查功能　object examination function;OEF

查找或确定唯一标识符(UID)(3.2.44)或其他用于验证的属性(3.2.5)的过程(3.1.187)。

注：在此过程中，其他属性能辅助 UID 的评价(3.1.92)。

3.2.30

成品验证工具　off-the-shelf authentication tool

通过开放销售进行网络购买的安全验证工具(3.2.12)。

3.2.31

在线验证工具　online authentication tool

需要实时在线连接以便能够现场解释验证要素(3.2.9)的安全验证工具(3.2.12)。

3.2.32

宏观验证要素　overt authentication element

能够由一种或多种人类感官检测并验证，而无需使用任何工具(除了矫正不完善的人类感官的日常工具，例如眼镜或助听器之外)的验证要素(3.2.9)。

3.2.33

专用验证工具　purpose-built authentication tool

专用于特定验证方案(3.2.11)的安全验证工具(3.2.12)。

3.2.34

说明符　specifier

明确要应用于特定物质产品(3.1.146)的安全验证方案(3.2.11)要求(3.1.201)的个人或实体(3.1.88)。

3.2.35

独立安全验证工具　stand-alone authentication tool

能用于揭示相对人类感官的隐式验证要素(3.2.15)以进行人类核实(3.1.285)，或者集成了能够独立验证安全验证要素(3.2.9)所需功能的安全验证工具(3.2.12)。

3.2.36

底物　substrate

在税票申请者(是固定术语)(3.2.40)所在地以外制作税票(3.2.39)时所用的材料。

3.2.37

防揭标签　tamper evident

能够显示某件物品已被拆用的标签。

注：在本文档中，“物品”指税票(3.2.39)。

3.2.38

税务机关　tax authority

负责征收可用税款(3.2.3)并负责税票(3.2.39)规范和设计的政府(国家、省、市或地方)机构。

注：税务机关可能是独立机构，也可能是海关、财政部门或其他财政机关的一部分。

3.2.39

税票　tax stamp

用于表明已缴纳了适用的消费税的，贴在某些特定类型的货物(3.3.8)上的可见戳记、标签或标记。

注 1：它可能是应税物品的产品、包装或货柜上使用的标签、封条，戳记或标记的形式。

注 2：税票是政府系统中用于收集和保护(3.1.190)可用税款(3.2.3)的工具。

注 3：基于底物(3.2.36)的税票也被称为“税章”和“税印”。

3.2.40

税票申请者　tax stamp applier

对应税产品申请税票(3.2.39)的实体(3.1.88)。

注 1：能通过直接标记(3.2.17)或通过使用基于底物(3.2.36)的税戳来完成申请。

注 2：税票申请者通常是一种或多种应税产品的制造商、包装商或进口商，或者负责向税务机关(3.2.38)报告印花税申请的印花税供应商，如果税务机关要求，报告时需附加产品信息(3.1.124)。

3.2.41

税票利害关系方　tax stamp interested party

与实施、执行和使用税票(3.2.39)系统相关的实体(3.1.88)。

3.2.42

可信查询处理功能　trusted query processing function；TQPF

提供进行可信验证功能(TVF)(3.2.43)和属性数据管理系统(ADMS)(3.2.6)的网关的功能。

注：这包括在手持设备上本地运行的软件。

3.2.43

可信验证功能　trusted verification function；TVF

验证接收到的唯一标识符(UID)(3.2.44)是否有效并根据规则和访问权限管理响应的功能。

3.2.44

唯一标识符　unique identifier；UID

在对象识别(3.1.114)系统的特定域和范围内，在其生命周期内，代表单个对象(3.1.158)或一类对象相关的单个和特定属性(3.2.5)集的代码。

3.3　供应链相关术语

3.3.1

有关执法部门及其他政府官员　appropriate law enforcement and other government officials

对国际供应链(3.1.132)或其环节拥有特定法定管辖权的政府和执法部门的人员(3.1.176)。

3.3.2

经认证的经营者　authorized economic operator

以经批准的任何职能参与国际货物(3.3.8)运输并被海关当局认定符合世界海关组织或相应供应链(3.1.268)安全标准的一方。

注 1：经认证的经营者是在世界海关组织(WCO)(3.1.294)标准框架中定义的一个术语。

注 2：经认证的经营者包括制造商、进口商、出口商、报关行、承运商、理货人、中间商、口岸、机场、货站经营者、综合经营者、仓储业经营者和分销商等。

3.3.3

业务伙伴　business partner

与组织(3.1.162)签订合同并协助其成为供应链中的组织(3.3.9)的承包人、供应商或服务提供方。

3.3.4

认证客户　certified client

供应链(3.1.268)安全管理(3.1.241)体系已经过合格的第三方认证或注册的组织(3.1.162)。

3.3.5

输送工具　conveyance

国际贸易中，将货物(3.3.8)从一个地点运输到另一个地点的工具。

示例：货箱、货盘、货物运输单元(3.1.27)、货物装卸设备、卡车、船舶、飞机和轨道车。

3.3.6

保管　custody

供应链中的组织(3.3.9)直接控制供应链(3.1.268)中货物(3.3.8)的制造、搬运、加工和运输以及与

之相关的货运信息的一段时期。

3.3.7

下游　downstream

超出供应链中的组织(3.3.9)保管期(3.3.6)的供应链中货物(3.3.8)的搬运、加工和移动。

3.3.8

货物　goods

供应链(3.1.268)中在买方下订单后为供买方使用或消费而制造、加工、搬运或运输的物品或物料。

3.3.9

供应链中的组织　organization in the supply chain

进行以下活动的实体(3.1.88)：

——为一个需要在某些环节跨越国际或经济体边界的采购订单进行制造、搬运、加工(3.1.187)、装载、集货、卸载或接收货物(3.3.8)；

——在国际供应链(3.1.132)中以任何方式进行货物运输，不管这个供应链(3.1.268)中的任何特定环节是否跨越国界(或经济体边界)；或

——提供、管理或实施海关部门或商业管理中所用的货运信息(3.1.124)的生成、发布或流动。

3.3.10

一级供应商　tier 1 supplier

通常通过合同安排直接向组织(3.1.162)提供产品和服务(3.1.188)的供应商。

3.3.11

二级供应商　tier 2 supplier

通过一级供应商(3.3.10)间接向组织(3.1.162)提供产品和服务(3.1.188)的供应商。

3.3.12

跟踪和追踪　track and trace

以了解关注对象在给定时间的位置(跟踪)以及在供应链(3.1.268)中途经的位置为目标的，识别每一单个物质产品(3.1.146)或批次的方法。

3.3.13

上游　upstream

供应链中的组织(3.3.9)在接手货物(3.3.8)保管期(3.3.6)前所发生的货物搬运、加工和移动。

注：按英文原文，此项术语为“上游活动”。

3.4　闭路电视相关术语

3.4.1

动态元数据　dynamic metadata

除像素值外，与数字图像相关的，针对视频序列的每一帧发生变化的数据。

3.4.2

元数据　metadata

以 ISO 或其他权威机构定义的格式，描述视听内容和数据本质的信息(3.1.124)。

示例：时间和日期、文本字符串、位置识别数据、音频和任何其他相关的、链接的或处理过的信息。

3.4.3

场景定位　scene location

用于定义摄影机可视场景的周长的地理位置(3.1.106)集合。

注：集合中每个地理位置的坐标系相同。场景位置中至少有一个地理位置。地理位置按顺时针或逆时针顺序排

列。单个地理位置场景将地理位置解释为场景的中心。

3.4.4

语义互操作性　semantic interoperability

两个或多个系统或服务自动解释和使用已正确交换的信息(3.1.124)的能力。

3.4.5

静态元数据　static metadata

除像素值外,与数字图像相关的,针对视频序列的每一帧不随时间发生变化(或至少不会改变既定序列)的数据。

3.4.6

语法互操作性　syntactic interoperability

两个或多个系统或服务交换结构信息(3.1.124)的能力。

参 考 文 献

[1] 中华人民共和国突发事件应对法

[2] GB/T 18354—2021 物流术语

[3] ISO 9000：2015 Quality management systems—Fundamentals and vocabulary

[4] ISO 14050：2020 Environmental management—Vocabulary

[5] ISO 14055-1：2017 Environmental management—Guidelines for establishing good practices for combatting land degradation and desertification—Part 1：Good practices framework

[6] ISO 16678：2014 Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade

[7] ISO 19011：2018 Guidelines for auditing management systems

[8] ISO 22301：2019 Security and resilience—Business continuity management systems—Requirements

[9] ISO 31000：2018 Risk management—Guidelines

[10] ISO/IEC 38500：2015 Information technology—Governance of IT for the organization

[11] ISO/Guide 73：2009 Risk management—Vocabulary

索　　引

汉语拼音索引

A

安全 …… 3.1.236
安全管理 …… 3.1.241
安全管理策略 …… 3.1.243
安全管理方案 …… 3.1.244
安全管理目标 …… 3.1.242
安全管理指标 …… 3.1.245
安全计划 …… 3.1.253
安全敏感材料 …… 3.1.254
安全敏感信息 …… 3.1.254
安全排查 …… 3.1.238
安全人员 …… 3.1.252
安全声明 …… 3.1.239
安全事件 …… 3.1.240
安全威胁情景 …… 3.1.255
安全因素 …… 3.1.237
安全运营 …… 3.1.246
安全运营策略 …… 3.1.250
安全运营方案 …… 3.1.251
安全运营管理 …… 3.1.247
安全运营目标 …… 3.1.248
安全运营人员 …… 3.1.249

B

保管 …… 3.3.6
保管副本 …… 3.2.16
保护 …… 3.1.190
保留风险 …… 3.1.202
备用工作区 …… 3.1.9
闭路电视系统 …… 3.1.28
不符合 …… 3.1.156
不良事件 …… 3.1.278

C

参量 …… 3.1.167
参与者 …… 3.1.168
测量 …… 3.1.149
测试(动词) …… 3.1.272
测试(名词) …… 3.1.273
策略 …… 3.1.178
产品和服务 …… 3.1.188
产品欺诈 …… 3.1.189
场景定位 …… 3.4.3
成品验证工具 …… 3.2.30
成文信息 …… 3.1.75
城市开放区 …… 3.1.280
城市群 …… 3.1.279
城市韧性 …… 3.1.281
城市系统 …… 3.1.282
程序 …… 3.1.186
持续改进 …… 3.1.47
冲击 …… 3.1.260
冲扰 …… 3.1.72
冲扰事件 …… 3.1.73
处于风险的人 …… 3.1.173
篡改 …… 3.2.2
脆弱性 …… 3.1.287
脆弱性分析 …… 3.1.287
脆弱性评估 …… 3.1.288
脆弱性群体 …… 3.1.289
错误接受率 …… 3.2.18
错误拒绝率 …… 3.2.19

D

地理位置 …… 3.1.106
底物 …… 3.2.36
调用 …… 3.1.136
动态元数据 …… 3.4.1
独立安全验证工具 …… 3.2.35
对策 …… 3.1.56
对象 …… 3.1.158

E

二级供应商 …… 3.3.11

F

防揭标签 …… 3.2.37
访问 …… 3.1.1
非法产品 …… 3.2.23
分包 …… 3.1.267
分析领域 …… 3.1.10
分析系统 …… 3.1.11
风险 …… 3.1.212
风险承受能力 …… 3.1.228
风险处置 …… 3.1.229
风险登记 …… 3.1.225
风险分担 …… 3.1.226
风险分析 …… 3.1.214
风险沟通 …… 3.1.217
风险管理 …… 3.1.221
风险减缓 …… 3.1.222
风险降低 …… 3.1.224
风险接受 …… 3.1.213
风险偏好 …… 3.1.215
风险评估 …… 3.1.216
风险评价 …… 3.1.219
风险识别 …… 3.1.220
风险源 …… 3.1.227
风险责任人 …… 3.1.223
风险准则 …… 3.1.218
服务范围 …… 3.1.233
复杂性 …… 3.1.41
覆盖范围 …… 3.1.57

G

概率 …… 3.1.185
跟踪和追踪 …… 3.3.12
工作环境 …… 3.1.292
公共预警 …… 3.1.194
公共预警系统 …… 3.1.195
公正性 …… 3.1.117
功能性演练 …… 3.1.105
攻击 …… 3.2.4
供应链 …… 3.1.268
供应链连续性管理 …… 3.1.269
供应链中的组织 …… 3.3.9
沟通和咨询 …… 3.1.36
固有危险物 …… 3.1.126
固有验证元素 …… 3.2.27
关键产品和服务 …… 3.1.65
关键地 …… 3.1.68
关键供应商 …… 3.1.66
关键客户 …… 3.1.62
关键控制点 …… 3.1.61
关键设施 …… 3.1.63
关键性能指标 …… 3.1.137
关键指标 …… 3.1.64
观察员 …… 3.1.160
管理 …… 3.1.141
管理计划 …… 3.1.142
管理体系 …… 3.1.143
管理体系咨询和/或相关的风险评估 …… 3.1.144
国际供应链 …… 3.1.132
过程 …… 3.1.187

H

合格 …… 3.1.42
合作 …… 3.1.50,3.1.169
合作关系 …… 3.1.170
核实 …… 3.1.285
宏观验证要素 …… 3.2.32
后果 …… 3.1.43,3.1.44
互通性 …… 3.1.133,3.1.134
互助协议 …… 3.1.154
滑坡 …… 3.1.138
环境 …… 3.1.45
恢复 …… 3.1.198
恢复点目标 …… 3.1.199
恢复时间目标 …… 3.1.200
活动 …… 3.1.2
货物 …… 3.3.8
货物运输单元 …… 3.1.27

J

基本社会服务 …… 3.1.16
基础设施 …… 3.1.125
激活 …… 3.2.1
即兴活动 …… 3.1.118
集成验证要素 …… 3.2.26
计划 …… 3.1.177
记录 …… 3.1.197
绩效 …… 3.1.174
绩效评价 …… 3.1.175
假冒(动词) …… 3.1.54
假冒产品 …… 3.1.55
价值观 …… 3.1.284
监测 …… 3.1.152
监测责任方 …… 3.1.153
检查员 …… 3.2.24
检查员访问历史 …… 3.2.25
减缓 …… 3.1.151
减小灾害风险 …… 3.1.71
鉴证分析 …… 3.2.20
胶粘剂 …… 3.1.3
脚本 …… 3.1.234
解除警报 …… 3.1.7
经济多样性 …… 3.1.80
经认证的经营者 …… 3.3.2
警报 …… 3.1.6
警报发布功能 …… 3.1.291
静态元数据 …… 3.4.5
纠正 …… 3.1.52
纠正措施 …… 3.1.53
就地避险(动词) …… 3.1.259
就地避险(名词) …… 3.1.258

K

看护责任 …… 3.1.78
可能性 …… 3.1.139
可信查询处理功能 …… 3.2.42
可信验证功能 …… 3.2.43
可用税款 …… 3.2.3
客户 …… 3.1.31
控制 …… 3.1.49
块体运动 …… 3.1.145

L

劳动力 …… 3.1.293
利益相关方 …… 3.1.129
鲁棒性 …… 3.1.230
逻辑结构 …… 3.1.140

M

秘密 …… 3.1.235
民防 …… 3.1.30
敏感信息 …… 3.1.257
模拟 …… 3.1.261
目标 …… 3.1.159
目标检查功能 …… 3.2.29
目标组 …… 3.1.271

N

内部攻击 …… 3.1.130
内部审核 …… 3.1.131
能力 …… 3.1.25
年度演练计划 …… 3.1.95

O

偶发事件 …… 3.1.46

P

培训 …… 3.1.277
评价 …… 3.1.92
评审 …… 3.1.208
评审活动 …… 3.1.209
评审人 …… 3.1.210

Q

情景 …… 3.1.231
权利所有人 …… 3.1.211
权威来源 …… 3.2.13
全部危险 …… 3.1.8

R

人工解释 …… 3.1.111

人权 …… 3.1.112
人权风险分析 …… 3.1.113
人权风险和影响评估 …… 3.1.113
人权风险评估 …… 3.1.113
人权影响评估 …… 3.1.113
人员 …… 3.1.176
认证客户 …… 3.3.4
韧性 …… 3.1.203
弱势群体 …… 3.1.290

S

色标 …… 3.1.33
色调 …… 3.1.110
色盲 …… 3.1.32
上游 …… 3.3.13
设施 …… 3.1.102
社会保护 …… 3.1.262
社区 …… 3.1.37
社区脆弱性 …… 3.1.39
社区警报体系 …… 3.1.38
社区预警体系 …… 3.1.38
审核 …… 3.1.14
审核员 …… 3.1.15
生态系统 …… 3.1.81
生态系统服务 …… 3.1.82
生物多样性 …… 3.1.18
胜任力 …… 3.1.40
剩余风险 …… 3.1.202
识别 …… 3.1.114
识别码 …… 3.2.21
实体 …… 3.1.88
使用持续性力量 …… 3.1.283
世界海关组织 …… 3.1.294
事件 …… 3.1.93,3.1.119
事件管理体系 …… 3.1.121
事件响应 …… 3.1.123
事件指挥 …… 3.1.120
事件准备 …… 3.1.122
视频监控 …… 3.1.286
受影响区域 …… 3.1.4
疏散 …… 3.1.89
疏散训练 …… 3.1.91
疏散指令 …… 3.1.90
输送工具 …… 3.3.5
属性 …… 3.2.5
属性数据管理系统 …… 3.2.6
数据分析 …… 3.1.69
税票 …… 3.2.39
税票利害关系方 …… 3.2.41
税票申请者 …… 3.2.40
税务机关 …… 3.2.38
说明符 …… 3.2.34
司法的 …… 3.1.103
私人安保公司 …… 3.1.184
私人安全服务提供商 …… 3.1.184
所有者 …… 3.1.166

T

特征 …… 3.2.22
挑战 …… 3.1.29
通知 …… 3.1.157
同行评审 …… 3.1.171
投资 …… 3.1.135
突发事件 …… 3.1.84

W

外包 …… 3.1.165
外部攻击 …… 3.1.101
完整性 …… 3.1.128
危害性分析 …… 3.1.67
危机 …… 3.1.58
危机管理 …… 3.1.59
危机管理团队 …… 3.1.60
危险区域 …… 3.1.12
危险源 …… 3.1.107
危险源监测功能 …… 3.1.108
威胁 …… 3.1.274
威胁分析 …… 3.1.275
唯一标识符 …… 3.2.44
文件 …… 3.1.74
物质产品 …… 3.1.146
物质产品生命周期 …… 3.1.147

X

下游 …… 3.3.7
响应队伍 …… 3.1.207
响应方案 …… 3.1.206
响应计划 …… 3.1.205
消息条 …… 3.1.127
效益 …… 3.1.17
协调 …… 3.1.51
心理急救 …… 3.1.193
心理教育 …… 3.1.192
信息 …… 3.1.124
行动后报告 …… 3.1.5
训练 …… 3.1.76

Y

压力 …… 3.1.266
严重心理事件 …… 3.1.191
演练 …… 3.1.94
演练安全员 …… 3.1.100
演练范围 …… 3.1.232
演练方案 …… 3.1.97
演练方案负责人 …… 3.1.98
演练项目团队 …… 3.1.99
演练协调员 …… 3.1.96
演练最终报告 …… 3.1.5
验证 …… 3.2.8
验证方案 …… 3.2.11
验证工具 …… 3.2.12
验证功能 …… 3.2.10
验证要素 …… 3.2.9
要求 …… 3.1.201
业务伙伴 …… 3.3.3
业务连续性 …… 3.1.19
业务连续性的人因要素 …… 3.1.172
业务连续性方案 …… 3.1.23
业务连续性管理 …… 3.1.20
业务连续性管理体系 …… 3.1.21
业务连续性计划 …… 3.1.22
业务影响分析 …… 3.1.24
一级供应商 …… 3.3.10
隐式验证要素 …… 3.2.15
应急管理 …… 3.1.85
应急管理能力 …… 3.1.86
影响 …… 3.1.115
影响分析 …… 3.1.116
优先活动 …… 3.1.183
有关执法部门及其他政府官员 …… 3.3.1
有效性 …… 3.1.83
语法互操作性 …… 3.4.6
语义互操作性 …… 3.4.4
预防 …… 3.1.180
预防措施 …… 3.1.182
预防危险源和威胁 …… 3.1.181
预警 …… 3.1.79
元数据 …… 3.4.2
员工援助方案 …… 3.1.87
原材料 …… 3.1.196
源 …… 3.1.263
运营信息 …… 3.1.161

Z

灾害 …… 3.1.70
在线验证工具 …… 3.2.31
责任主体 …… 3.1.77
战略演练 …… 3.1.265
照顾者 …… 3.1.26
真实的物料 …… 3.2.7
直接标记 …… 3.2.17
指标 …… 3.1.270
指定紧急联系人 …… 3.1.155
指挥和控制 …… 3.1.34
指挥和控制体系 …… 3.1.35
主办方 …… 3.1.109
主要利益相关方 …… 3.2.28
专用验证工具 …… 3.2.33
准备 …… 3.1.179
准备就绪 …… 3.1.179
资产 …… 3.1.13
资源 …… 3.1.204
自动评估 …… 3.2.14
自发志愿者 …… 3.1.264

自我保护 …… 3.1.256
综合演练 …… 3.1.104
组织 …… 3.1.162
组织韧性 …… 3.1.164
组织文化 …… 3.1.163
最大可接受中断 …… 3.1.148
最高管理者 …… 3.1.276
最小业务连续性目标 …… 3.1.150
最长可容忍中断时间 …… 3.1.148

英文对应词索引

A

access …… 3.1.1
activation …… 3.2.1
activity …… 3.1.2
adhesive/glue …… 3.1.3
ADMS …… 3.2.6
affected area …… 3.1.4
after-action report …… 3.1.5
alert …… 3.1.6
all clear …… 3.1.7
all-hazard …… 3.1.8
alteration …… 3.2.2
alternate worksite …… 3.1.9
analysis area …… 3.1.10
analysis system …… 3.1.11
applicable tax …… 3.2.3
appropriate law enforcement and other government officials …… 3.3.1
area at risk …… 3.1.12
asset …… 3.1.13
attack …… 3.2.4
attribute …… 3.2.5
attribute data management system …… 3.2.6
audit …… 3.1.14
auditor …… 3.1.15
authentic material good …… 3.2.7
authentication …… 3.2.8
authentication element …… 3.2.9
authentication function …… 3.2.10
authentication solution …… 3.2.11
authentication tool …… 3.2.12
authoritative source …… 3.2.13
authorized economic operator …… 3.3.2

automated interpretation …… 3.2.14

B

basic social services …… 3.1.16
benefit …… 3.1.17
biodiversity/biological diversity …… 3.1.18
business continuity …… 3.1.19
business continuity management …… 3.1.20
business continuity management system …… 3.1.21
business continuity plan …… 3.1.22
business continuity programme …… 3.1.23
business impact analysis …… 3.1.24
business partner …… 3.3.3

C

capacity …… 3.1.25
carer …… 3.1.26
cargo transport unit …… 3.1.27
CCP …… 3.1.61
CCTV system …… 3.1.28
certified client …… 3.3.4
challenge …… 3.1.29
civil protection …… 3.1.30
client …… 3.1.31
colour blindness …… 3.1.32
colour-code …… 3.1.33
command and control …… 3.1.35
command and control system …… 3.1.35
communication and consultation …… 3.1.36
community …… 3.1.37
community vulnerability …… 3.1.39
community-based early warning system …… 3.1.38
community-based warning system …… 3.1.38
competence …… 3.1.40
complexity …… 3.1.41
conformity …… 3.1.42
consequence …… 3.1.43，3.1.44
context …… 3.1.45
contingency …… 3.1.46
continual improvement …… 3.1.47
continuity …… 3.1.48

control …… 3.1.49
conveyance …… 3.3.5
cooperation …… 3.1.50
coordination …… 3.1.51
correction …… 3.1.52
corrective action …… 3.1.53
counterfeit(verb) …… 3.1.54
counterfeit good …… 3.1.55
countermeasure …… 3.1.56
coverage …… 3.1.57
covert authentication element …… 3.2.15
crisis …… 3.1.58
crisis management …… 3.1.59
crisis management team …… 3.1.60
critical control point …… 3.1.61
critical customer …… 3.1.62
critical facility …… 3.1.63
critical indicator …… 3.1.64
critical product and service …… 3.1.65
critical supplier …… 3.1.66
critically …… 3.1.68
custodian copy …… 3.2.16
custody …… 3.3.6

D

data analysis …… 3.1.69
direct marking …… 3.2.17
disaster …… 3.1.70
disaster risk reduction …… 3.1.71
disruption …… 3.1.72
disruptive event …… 3.1.73
document …… 3.1.74
documented information …… 3.1.75
downstream …… 3.3.7
drill …… 3.1.76
duty of care …… 3.1.78
duty-bearer …… 3.1.77
dynamic metadata …… 3.4.1

E

early warning …… 3.1.79

economic diversity …… 3.1.80
ecosystem …… 3.1.81
ecosystem services …… 3.1.82
effectiveness …… 3.1.83
emergency …… 3.1.84
emergency management …… 3.1.85
emergency management capability …… 3.1.86
employee assistance programme …… 3.1.87
entity …… 3.1.88
evacuation command …… 3.1.90
evacuation drill …… 3.1.91
evaluation …… 3.1.92
event …… 3.1.93
exercise …… 3.1.94
exercise annual plan …… 3.1.95
exercise coordinator …… 3.1.96
exercise programme …… 3.1.97
exercise programme manager …… 3.1.98
exercise project team …… 3.1.99
exercise safety officer …… 3.1.100
external attack …… 3.1.101

F

facility …… 3.1.102
false acceptance rate …… 3.2.18
false rejection rate …… 3.2.19
forensic …… 3.1.103
forensic analysis …… 3.2.20
full-scale exercise …… 3.1.104
functional exercise …… 3.1.105

G

geo-location …… 3.1.106
goods …… 3.3.8

H

hazard …… 3.1.107
hazard monitoring function …… 3.1.108
host …… 3.1.109
HRRA …… 3.1.113
hue …… 3.1.110

human interpretation …… 3.1.111
human rights …… 3.1.112
human rights risk analysis …… 3.1.113

I

identification …… 3.1.114
identifier …… 3.2.21
identity …… 3.2.22
illicit product …… 3.2.23
impact …… 3.1.115
impact analysis …… 3.1.116
impartiality …… 3.1.117
improvisation …… 3.1.118
incident …… 3.1.119
incident command …… 3.1.120
incident management system …… 3.1.121
incident preparedness …… 3.1.122
incident response …… 3.1.123
information …… 3.1.124
infrastructure …… 3.1.125
inherently dangerous property …… 3.1.126
inject …… 3.1.127
inspector …… 3.2.24
inspector access history …… 3.2.25
integrated authentication element …… 3.2.26
integrity …… 3.1.128
interested party …… 3.1.129
internal attack …… 3.1.130
internal audit …… 3.1.131
international supply chain …… 3.1.132
interoperability …… 3.1.133，3.1.134
intrinsic authentication element …… 3.2.27
investment …… 3.1.135
invocation …… 3.1.136

K

key performance indicator …… 3.1.137
KPI …… 3.1.137

L

landslide …… 3.1.138

lead interested party …… 3.2.28
likelihood …… 3.1.139
logical structure …… 3.1.140

M

management …… 3.1.141
management plan …… 3.1.142
management system …… 3.1.143
management system consultancy and/or associated risk assessment …… 3.1.144
mass movement …… 3.1.145
material good life cycle …… 3.1.147
material goods …… 3.1.146
maximum acceptable outage …… 3.1.148
maximum tolerable period of disruption …… 3.1.148
measurement …… 3.1.149
metadata …… 3.4.2
MBCO …… 3.1.150
minimum business continuity objective …… 3.1.150
mitigation …… 3.1.151
monitoring …… 3.1.152
monitoring process owner …… 3.1.153
MTPD …… 3.1.148
mutual aid agreement …… 3.1.154

N

nominated emergency contact …… 3.1.155
nonconformity …… 3.1.156
notification …… 3.1.157

O

object …… 3.1.158
object examination function …… 3.2.29
objective …… 3.1.159
observer …… 3.1.160
OEF …… 3.2.29
off-the-shelf authentication tool …… 3.2.30
online authentication tool …… 3.2.31
operational information …… 3.1.161
organization …… 3.1.162
organization in the supply chain …… 3.3.9
organizational culture …… 3.1.163

organizational resilience …… 3.1.164
outsource …… 3.1.165
overt authentication element …… 3.2.32
owner …… 3.1.166

P

parameter …… 3.1.167
participant …… 3.1.168
partnering …… 3.1.169
partnership …… 3.1.170
peer review …… 3.1.171
people aspects of business continuity …… 3.1.172
people at risk …… 3.1.173
performance …… 3.1.174
performance evaluation …… 3.1.175
personnel …… 3.1.176
planning …… 3.1.177
policy …… 3.1.178
preparedness …… 3.1.179
prevention …… 3.1.180
prevention of hazards and threats …… 3.1.181
preventive action …… 3.1.182
prioritized activity …… 3.1.183
private security service provider …… 3.1.184
probability …… 3.1.185
procedure …… 3.1.186
process …… 3.1.187
product and service …… 3.1.188
product fraud …… 3.1.189
protection …… 3.1.190
PSSP …… 3.1.184
psychological critical incident …… 3.1.191
psychological education …… 3.1.192
psychological first aid …… 3.1.193
public warning …… 3.1.194
public warning system …… 3.1.195
purpose-built authentication tool …… 3.2.33

R

raw material …… 3.1.196
readiness …… 3.1.179

record …… 3.1.197
recovery …… 3.1.198
recovery point objective …… 3.1.199
recovery time objective …… 3.1.200
requirement …… 3.1.201
residual risk …… 3.1.202
resilience …… 3.1.203
resource …… 3.1.204
response plan …… 3.1.205
response programme …… 3.1.206
response team …… 3.1.207
retained risk …… 3.1.202
review …… 3.1.208
review visit …… 3.1.209
reviewer …… 3.1.210
rights holder …… 3.1.211
risk …… 3.1.212
risk acceptance …… 3.1.213
risk analysis …… 3.1.214
risk appetite …… 3.1.215
risk assessment …… 3.1.216
risk communication …… 3.1.217
risk criteria …… 3.1.218
risk evaluation …… 3.1.219
risk identification …… 3.1.220
risk management …… 3.1.221
risk mitigation …… 3.1.222
risk owner …… 3.1.223
risk reduction …… 3.1.224
risk register …… 3.1.225
risk sharing …… 3.1.226
risk source …… 3.1.227
risk tolerance …… 3.1.228
risk treatment …… 3.1.229
robustness …… 3.1.230
RPO …… 3.1.199
RTO …… 3.1.200

S

SCCM …… 3.1.269
scenario …… 3.1.231

scene location …… 3.4.3
scope of exercise …… 3.1.232
scope of service …… 3.1.233
script …… 3.1.234
secret …… 3.1.235
security …… 3.1.236
security aspect …… 3.1.237
security cleared …… 3.1.238
security declaration …… 3.1.239
security incident …… 3.1.240
security management …… 3.1.241
security management objective …… 3.1.242
security management policy …… 3.1.243
security management programme …… 3.1.244
security management target …… 3.1.245
security operation …… 3.1.246
security operations management …… 3.1.247
security operations objective …… 3.1.248
security operations personnel …… 3.1.249
security operations policy …… 3.1.250
security operations programme …… 3.1.251
security personnel …… 3.1.252
security plan …… 3.1.253
security sensitive information …… 3.1.254
security sensitive material …… 3.1.254
security threat scenario …… 3.1.255
self-defence …… 3.1.256
semantic interoperability …… 3.4.4
sensitive information …… 3.1.257
shelter in place(noun) …… 3.1.258
shelter in place(verb) …… 3.1.259
shock …… 3.1.260
simulation …… 3.1.261
social protection …… 3.1.262
source …… 3.1.263
specifier …… 3.2.34
spontaneous volunteer …… 3.1.264
stakeholder …… 3.1.129
stand-alone authentication tool …… 3.2.35
static metadata …… 3.4.5
strategic exercise …… 3.1.265

stress …… 3.1.266
subcontracting …… 3.1.267
substrate …… 3.2.36
supply chain …… 3.1.268
supply chain continuity management …… 3.1.269
SV …… 3.1.264
syntactic interoperability …… 3.4.6

T

tamper evident …… 3.2.37
target …… 3.1.270
target group …… 3.1.271
tax authority …… 3.2.38
tax stamp …… 3.2.39
tax stamp applier …… 3.2.40
tax stamp interested party …… 3.2.41
test …… 3.1.272
testing …… 3.1.273
threat …… 3.1.274
threat analysis …… 3.1.275
tier 1 supplier …… 3.3.10
tier 2 supplier …… 3.3.11
top management …… 3.1.276
TQPF …… 3.2.42
track and trace …… 3.3.12
training …… 3.1.277
trusted query processing function …… 3.2.42
trusted verification function …… 3.2.43
TVF …… 3.2.43

U

UID …… 3.2.44
undesirable event …… 3.1.278
unique identifier …… 3.2.44
upstream …… 3.3.13
urban agglomeration …… 3.1.279
urban open area …… 3.1.280
urban resilience …… 3.1.281
urban system …… 3.1.282
use of force continuum …… 3.1.283

V

values …… 3.1.284
verification …… 3.1.285
video-surveillance …… 3.1.286
vulnerability …… 3.1.287
vulnerability analysis …… 3.1.287
vulnerability assessment …… 3.1.288
vulnerable group …… 3.1.289
vulnerable person …… 3.1.290

W

warning dissemination function …… 3.1.291
WCO …… 3.1.294
work environment …… 3.1.292
workforce …… 3.1.293
World Customs Organization …… 3.1.294

中 华 人 民 共 和 国
国 家 标 准
安全与韧性 术语
GB/T 44483—2024
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址:www.spc.net.cn
服务热线:400-168-0010
2024年9月第一版
*
书号:155066·1-76759

GB/T 44483-2024