ICS 35.040

L80

中华人民共和国国家标准

GB/T 20985.2—XXXX/ISO/IEC 27035-2:2016

信息技术　安全技术　信息安全事件管理 第2部分：事件响应规划和准备指南

Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response

（ISO/IEC 27035-2:2016，MOD）

在提交反馈意见时，请将您知道的相关专利与支持性文件一并附上。

（报批稿）

2019-10-03

XXXX－XX－XX 发布　　XXXX－XX－XX 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

GB/T 20985《信息技术　安全技术　信息安全事件管理》分为多个部分：

——第1部分：事件管理原理；

——第2部分：事件响应规划和准备指南；

——后续部分。

本部分为GB/T 20985的第2部分。

本部分按照GB/T 1.1—2009《标准化工作导则　第1部分：标准的结构和编写》和GB/T 20000.2—2009《标准化工作指南　第2部分：采用国际标准的规则》给出的规则起草。

本部分使用重新起草法修改采用国际标准ISO/IEC 27035-2:2016《信息技术　安全技术　信息安全事件管理　第2部分：事件响应规划和准备指南》。

本标准与ISO/IEC 27035-2:2016的技术性差异及其原因如下：

——为了适应我国国情，在规范性引用文件中增加了我国国家标准GB/Z 20986—2007《信息安全技术　信息安全事件分类分级指南》，同时正文中的相关引用处也做了相应调整。

——在“1　范围”中弥补国际标准的缺失，增加了“经验总结”阶段的用途和要点。

本部分由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本部分起草单位：中电长城网际系统应用有限公司、中电数据服务有限公司、中国信息安全研究院有限公司、中国电子技术标准化研究院、国家计算机网络应急技术处理协调中心、三六零科技有限公司、公安部第三研究所、国家信息中心、陕西省网络与信息安全测评中心、北京江南天安科技有限公司

本部分主要起草人：闵京华、周亚超、王惠莅、上官晓丽、舒敏、陈悦、张屹、王艳辉、陈长松、杜佳颖、刘蓓、李怡、魏玉峰、陈冠直

引　言

GB/T 20985属于信息安全管理体系（ISMS）系列标准的延伸，聚焦于信息安全事件管理，GB/T 22080将其确定为信息安全管理体系的关键成功因素之一。

组织的事件计划与该组织确信已做好事件准备之间可能存在很大差距。因此，GB/T 20985的本部分提供指南，以增强组织对信息安全事件响应做好实际准备的信心。为此，本部分关注于事件管理相关的策略和计划，以及如何建立事件响应小组并通过经验总结和评价不断改进其成效。

信息技术　安全技术　信息安全事件管理　第2部分：事件响应规划和准备指南

1　范围

本部分基于GB/T 20985.1中给出的“信息安全事件管理阶段”模型的“规划和准备”阶段和“经验总结”阶段，为规划和准备事件响应以及事后总结经验和进行改进提供指南。

“规划和准备”阶段的要点包括：

——信息安全事件管理策略和最高管理者的承诺；

——在公司层面以及系统、服务和网络层面都要更新的信息安全策略，包括那些与风险管理相关的；

——信息安全事件管理计划；

——事件响应小组（IRT）的建立；

——建立与内部和外部组织的关系和联络；

——技术及其他方面（包括组织和运行方面）的支持；

——信息安全事件管理的意识教育和培训；

——信息安全事件管理计划的测试。

“经验总结”阶段的要点包括：

——经验教训的总结；

——信息安全的总结和改进；

——信息安全风险评估和管理评审结果的总结和改进；

——信息安全事件管理计划的总结和改进；

——IRT表现和有效性的评价。

本部分给出的原理是通用的，适用于任何类型、规模或性质的组织。组织可根据其业务的类型、规模和性质，关联信息安全风险状况，调整本部分给出的指南。本部分也适用于提供信息安全事件管理服务的外部组织。

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（包括所有的修改单）适用于本文件。

GB/T 29246—2017　信息技术　安全技术　信息安全管理体系　概述和词汇（ISO/IEC 27000:2016，IDT）

GB/T 20985.1—2017　信息技术　安全技术　信息安全事件管理　第1部分：事件管理原理（ISO/IEC 27035-1:2016，IDT）

GB/Z 20986—2007　信息安全技术　信息安全事件分类分级指南

3 术语、定义和缩略语

3.1 术语和定义

GB/T 29246、GB/T 20985.1界定的以及下列术语和定义适用于本文件。

3.1.1

用户 users

使用事件响应小组（IRT）所提供服务的人或组织。

注：用户可以是组织内部的或组织外部的。

3.2 缩略语

CD	光盘（compact disk）
CERT	计算机应急响应小组（computer emergency response team），有时也被称为事件响应小组（IRT）或计算机安全响应小组（CSIRT）
DNS	域名系统（domain name system）
DVD	数字多功能光盘（digital versatile disk）
ICMP	互联网控制消息协议（internet control message protocol）
IDS	入侵检测系统（intrusion detection system）
IPv4	互联网协议第4版（internet protocol v4）
IPv6	互联网协议第6版（internet protocol v6）
IRT	事件响应小组（incident response team）
ISP	互联网服务提供商（internet service provider）
PoC	联系点（point of contact）
SMTP	简单邮件传输协议（simple mail transfer protocol）
SSL	安全套接层协议（secure sockets layer protocol）
TCP	传输控制协议（transmission control protocol）
TLP	交通灯协议（traffic light protocol）
TLS	传输层安全协议（transport layer security protocol）
UDP	用户数据报协议（user datagram protocol）
WiFi	无线保真（wireless fidelity）

4 信息安全事件管理策略

4.1 概述

注：第4章对应于GB/T 20985.1—2017，5.2 a)。

组织的信息安全事件管理策略宜提供正式文件化的原则和意图，用于指导信息安全事件管理决策，并确保其过程和规程等的实施与策略是一致的且相适的。

任何信息安全事件管理策略宜是组织信息安全策略的一部分，也支持上级组织现有使命并符合现有的策略和规程。

组织宜实施信息安全事件管理策略来概述过程、责任人、权威机构以及当信息安全事件发生时的报告路径（特别是报告可疑事件的联系点）。宜定期审查策略，以确保它反映可能影响事件响应的最新组织结构、过程和技术。另外，策略宜概述组织内任何与事件响应相关的意识和培训计划（见第10章）。

组织宜以独立文件的形式文件化其信息安全事态、事件和漏洞的管理策略，并作为其总体信息安全管理体系策略的一部分(见GB/T 22080—2016，5.2)，或作为其信息安全策略的一部分(见GB/T 22081—2016，5.1.1)。组织的规模、结构和业务性质及其信息安全事件管理计划程度是决定上述选项的因素。组织宜为每个具有合法访问信息系统和相关地点的人，提供信息安全事件管理策略指导。

信息安全事件管理策略制定前,组织宜确定信息安全事件管理的以下方面：

a) 目标；
b) 内部和外部的利益相关方；
c) 需要重点关注的特定事件类型和脆弱性；
d) 需要重点关注的任何特定角色；
e) 组织的整体利益和部门利益。

4.2 相关方

宜作为一个企业级过程创建和实施一个成功的信息安全事件管理策略。为此，所有利益相关方或其代表宜参与策略制定，从最初规划阶段直到任何过程或响应小组的落实。这可能包括法律顾问、公共关系和营销人员、部门经理、保安人员、系统和网络管理员、信息通信技术（ICT）人员、服务台人员、上层管理人员，甚至在某些情况下的设施相关人员。

组织宜确保其信息安全事件管理策略得到最高管理层的批准，并获得最高管理层所有人员的承诺。

确保持续的管理层承诺对于接受一个结构化的信息安全事件管理方法来说至关重要。人员需要识别事件，知道该做什么并理解这一方法对组织的好处。管理层需要为信息安全事件策略提供支持，以确保组织对提供资源和维护事件响应能力的承诺。

信息安全事件管理策略宜提供给每位员工和承包商，并关注信息安全意识教育和培训。

4.3 信息安全事件管理策略内容

信息安全事件管理策略宜是高层的。详细信息和分步指示宜包含在组成信息安全事件管理计划的一系列文件中，见第6章所述。

组织宜确保其信息安全事件管理策略内容包括（但不限于）以下方面：

a) 策略的目的、目标和范围（包括适用对象和适用情况）；
b) 策略所有者和审查周期；
c) 信息安全事件管理对组织的重要性和最高管理层对信息安全事件管理的承诺，以及相关计划文档；
d) 安全事件的定义；
e) 安全事件类型或类别的描述（或引用有更加深入描述的其他文档）；
f) 事件如何报告的描述，包括报告什么，报告采用的机制，以及在哪里和向谁报告；
g) 事件管理过程流的高层概述或可视化展示（显示安全事件处理的基本步骤），从发现到报告、信息采集、分析、响应、通告、升级和解决；
h) 信息安全事件解决后的活动要求，包括经验总结和过程改进；
i) 适当时，脆弱性报告和处理的总结（虽然这可能是一个独立策略文件）；
j) 为信息安全事件管理过程的每个阶段及相关活动明确的角色、责任和决策机构（适当时，包括脆弱性报告和处理）；
k) 对描述事态和事件分类、严重程度评级(如使用)和相关术语文件的引用。宜有一个描述事件组成的概述或引用对此有描述文件；
l) IRT概述,包括IRT组织结构、关键角色、责任、权威机构，以及职责概要，包括但不限于：
   1) 有关已确认事件的报告和通告要求；

2) 关于事件向最高管理层做简要汇报；
3) 处理询问、推动跟进和解决事件；
4) 联络外部组织（必要时）；
5) 为确保IRT执行的所有信息安全事件管理活动得到正确记录供以后分析提出的要求和理由。

m) 对跨组织协同工作来发现、分析和响应信息安全事件的组件的要求；
n) 适用时，对任何监督或治理结构及其权力和职责的描述；
o) 与提供特定外部支持的组织的联系，诸如取证团队、法律顾问、其他IT运营者等；
p) 与信息安全事件管理活动相关的法律法规合规要求或授权的概要（更多细节参见附录A）；
q) 支持信息安全事件管理过程和相关活动的其他策略、规程和文件的列表和引用。策略中列出的许多事项可能有自己更详细的规程或指导文件。

此外，还有其他相关的策略或规程可支持信息安全事件管理策略，如果适用于组织但还没有，也可作为准备阶段的一部分来建立。这包括但不限于：

——第6章所述的信息安全事件管理计划。
——持续监控策略，声明组织采取这种活动，并描述基本监控任务。持续监控确保在需要法律起诉或内部纪律处分时电子证据的保全。
——对IRT的授权，以便有来自其他操作部分的需要时能够访问监控输出或请求访问日志（本条款也可放入信息安全事件管理策略）。
——信息共享、信息披露和沟通策略，概述事件管理活动相关信息如何、何时和与谁共享。信息宜保密，只能根据相关法律进行披露。在许多情况下,法规要求任何个人可识别信息被泄露时都需要告知受影响的各方。除了法律要求,信息也宜遵循组织对信息披露的任何要求。在事件处理过程中，当引入或变更第三方时，信息需要被共享。信息共享的范围、环境和目的需要在适当的策略和规程中得到描述或引用。使用交通灯协议（TLP）是信息披露指导和标记的例子。
——信息存储和处理策略，要求记录、数据以及其他调查相关数据被安全地存储并根据其敏感性进行相应地处理。如果组织有文件标签或分类模式,这一策略对信息安全事件管理活动和人员来说也很重要。
——IRT章程，详细说明IRT要做什么和其操作权限。至少,章程宜包括使命陈述、IRT范围的定义、IRT的最高管理层发起者细节、IRT的权限、IRT的联系信息、IRT的服务和核心活动列表、IRT的权限和操作的范围、IRT的目的和目标，以及有关任何治理结构的讨论。
——团队的目标和目的非常重要,需要清晰、明确的定义。
——IRT的范围通常涵盖了所有组织的信息系统、服务和网络。在某些情况下,组织可以要求范围不同（扩大或缩小）,在这种情况下,它宜清楚地记录范围内和范围外分别是什么。
——IRT治理可能包括识别具有对IRT有决策权力和建立权限等级的执行官、董事会成员或总经理。知道这一点有助于组织内所有人员了解IRT的背景和建立,这些信息对在IRT中建立信任是至关重要的。宜注意的是,详细信息公布之前,宜从法律的角度予以审查。在某些情况下,团队权限的披露会使其直接面对责任要求。
——信息安全事件管理意识和培训计划概述，宜包括任何对全体人员意识培训和对IRT成员事件管理培训的培训任务、政策或要求。

5 信息安全策略更新

5.1 概述

注：第5章对应于GB/T 20985.1—2017，5.2 b)。

组织宜在整体层面以及具体的系统、服务和网络层面将信息安全事件管理内容包含在其信息安全策略中，并将这些内容关联到事件管理策略。这种整合宜针对如下目标：

a) 描述为什么信息安全事件管理很重要，尤其是信息安全事件报告和处理计划；
b) 表明最高管理层对需要做好适当的信息安全事件准备和响应（即信息安全事件管理计划）的承诺；
c) 确保各种策略的一致性；
d) 确保有计划地、系统地和沉着地响应信息安全事件,从而最小化事件的负面影响。

关于信息安全风险评估和管理的指导，见GB/T 31722。

5.2 策略文档的关联

组织宜更新和维护企业级信息安全和风险管理策略,配上具体的系统、服务或网络的信息安全策略,以确保它们是一致的和最新的。这些企业级策略宜明确地关联到信息安全事件管理策略和相关计划。

企业级策略宜包括需要建立适当审查机制的要求。这些审查机制需要确保来自发现、监控和解决信息安全事件的信息，以及来自处理被报告的信息安全脆弱性的信息，为维护策略持续有效性的过程提供输入。

6 制定信息安全事件管理计划

6.1 概述

注：第6章对应于GB/T 20985.1—2017，5.2 c)。

信息安全事件管理计划的目标是将信息安全事态、事件和脆弱性的处理活动和规程以及它们之间的沟通形成文件。该计划源于也是基于信息安全事件管理策略。

总体而言，该计划的文档宜包含多个文件，包括用于信息安全事件的发现和报告、评估和决策、响应和经验总结的表单、规程、组织要素和支持工具。

该计划可以包括事件管理活动基本流程顶层概要，来提供结构和指针指向计划的各种细节组件。这些组件为事件处理者提供要遵循的分步指示，包括根据情况使用特定的工具、遵循特定的流程或处理特定类型的事件。

一旦发现信息安全事态或收到信息安全脆弱性报告时，信息安全事件管理计划便开始生效。

组织宜使用该计划指导以下事项：

a) 响应信息安全事态；
b) 判断信息安全事态是否成为信息安全事件；
c) 管理信息安全事件直到结束；
d) 应对信息安全脆弱性；
e) 对报告事件的要求；
f) 在整个事件管理过程中，对存储信息（包括其格式）的要求；
g) 与内外部的团体或组织共享信息的规则和环境；
h) 识别经验教训，以及任何对计划和（或）安全所需的改进；
i) 实施已识别的改进。

事件响应计划的规划和准备宜由过程责任者承担,基于信息安全事件管理策略定义范围的事件响应的一个或多个明确的目标。

6.2 基于共识建立信息安全事件管理计划

GB/T 20985的本部分为信息安全事件管理策略制定提供建议。然而，在没有相关的指导方针或标准、现行法律或其他权威来源的情况下，事件管理规划过程宜基于共识，以确保有效的运行、沟通和与外部组织的关系。

术语和定义宜在IRT成员和伙伴组织之间加以规范，包括组织和团队的名称和标识、信息资产、业务过程等。当术语有难度或容易误解时，事件管理计划宜在一个词汇表中包括标准术语和定义。

事件管理过程责任者宜定义角色及与外部IRT和其他响应组织的关系，以及响应活动的结构和边界。参与各方的责任可能重叠，宜在事件管理规划过程中基于共识进行调整。当在事件相应决策边界上有重叠时，计划宜确定责任方。

参与方和外部IRT经常有不同的度量体制。计划参与者宜评价来自各自当事方或外部组织的可用度量体制，或者在现有度量体制的特定集合上达成共识，或者同意使用可逆映射来链接不同的度量体制。不管采用怎样的方法，宜通过选择或连接定量度量体制的计划，使不同度量体制的范围相同，并且选择或连接完全等价定性度量体制。

6.3 参与方

组织宜确保信息安全事件管理计划是被全员以及相关承包商、ICT服务提供商、电信供应商和外包公司承认的，因此涵盖以下职责：

a) 发现和报告信息安全事件（这是组织中任何长久人员或合同人员的责任）；

b) 评估和响应信息安全事态和事件，参与事件后的解决活动，包括总结经验，并改进信息安全和信息安全事件管理计划本身（这是PoC成员、IRT、管理者、公关人员和法定代表人的责任）；

c) 报告信息安全脆弱性（这是组织中任何长久人员或合同人员的责任）。

该计划还宜考虑任何第三方用户，以及由第三方组织、政府和商业性信息安全事件与脆弱性信息提供组织报告的信息安全事件和相关脆弱性。

参与各方被期望积极参与处理信息安全事件，因此宜对角色和职责做出清晰的划分，并使每个人都意识到其角色和职责。角色划分宜伴有约定的事件切换协议，以便以合理的方式进行信息交换。如果适当并可能，宜自动化事件切换和信息交换来提高这个过程的速度。如果组织或IRT的某些能力外包给第三方，则可能出现这种场景。这种场景的实例有，当组织使用第三方运行的云系统时，或者当第三方为组织进行数字取证时，或者在事件处理过程中与服务提供者一起工作时。

6.4 信息安全事件管理计划内容

在规划和准备过程考虑特定事件类型和相应的响应过程之前，宜定义和审核支持预期管理阶段的关键决策准则和过程。这需要有可用的策略，对资产和控制的正式或非正式的理解，并获得参与者和管理者的支持。

信息安全事件管理计划的内容宜包括概述以及详细的活动说明。如上所述，计划文档宜由包括表单、规程、组织要素和支持工具等多个文档组成。

详细的活动、规程和信息宜关联到以下方面：

a) 规划和准备

1) 标准化的信息安全事态/事件分类分级方法，以便能够提供一致的结果。在任何情况下，决策宜基于对组织的业务运营造成的实际或预期不利影响以及相关指南。

注：GB/Z 20986—2007给出了信息安全事态和事件的分类分级方法，附录C还给出了其他方法示例。

2) 为信息交换而构造的信息安全数据库结构可能提供以下方面的能力：共享报告/预警，比较结果，改进预警信息，以及更准确地看待信息系统面临的威胁和存在的脆弱性。数据库的实

际格式和使用取决于组织的需求。例如，一个非常小的组织可能使用各种文件，而一个复杂的组织可能使用更复杂的技术，诸如关系数据库和应用工具。

3) 有关决定每个相关过程中是否需要升级，升级给谁以及相关规程的指南。基于信息安全事件管理计划中提供的指南，评估信息安全事态、事件或脆弱性的任何人宜知道在哪种情况下有必要升级，以及宜升级给谁。此外，有不可预见的情况下这种升级可能是必要的。例如，一个小的信息安全事件如果处理不当或者一周内未跟进而导致重大的信息安全事件，就会演变为重大或危机情况。

4) 后续的规程，以确保所有信息安全事件管理活动由指定的人员正确记录，并进行日志分析；

5) 过程和机制，以确保变更控制机制得到维护，包括信息安全事态、事件和脆弱性跟踪，以及信息安全报告更新和计划本身更新。

6) 信息安全证据分析规程。

7) 使用入侵检测系统(IDS)和入侵预防系统(IPS)的规程和指南，以确保相关的法律法规方面问题得到解决。指南宜包括对从事攻击者监视活动的优点和缺点的论述。ISO/IEC 27039中有关于IDS的更多信息。

8) 建立、实施和运行这些机制以防止信息安全事件发生和减少其可能性，并处理发生的信息安全事件。

9) 信息安全事态、事件和脆弱性管理意识和培训计划材料。

10) 信息安全事件管理计划的测试规程和规范。

11) 信息安全事件管理的组织结构规划；

12) IRT整体或成员的工作范围和责任；

13) 重要的联系信息；

14) 与组织的公共事务办公室、法律部门和最高管理层或有关部门协商一致的信息共享规程和指南。

b) 发现和报告

1) 对发现和报告的规划和准备要求宜使能并支持寻找或接受信息安全事件信息的过程开发和运行。

2) 宜基于报告的完整性和对一个或多个信息安全事态的验证来定义接受事件报告的准则。为了支持随后的决策，在规划过程前宜定义任何事态发现预警或人工报告的最低接受准则，并至少包括对受影响的环境或资产的识别，对一个或多个疑似或确定的事态或相适应的事态类型的清单，以及报告的接收时间。为了支持决策，规划过程宜包括一种方法以返回信息不足的发现或报告。

3) 宜根据组织的语境、事件响应策略以及技术和管理角色的分配来定义报告输出或通知。报告和通知的格式宜符合事件分级标度或一种连续的相关度量。

4) 发现和报告信息安全事件的发生（通过人工或自动方式）。

5) 响应报告过程的不正确使用（可能包括在事件管理计划范围之外采取行动）。

6) 收集信息安全事态信息。

7) 发现和报告信息安全脆弱性。

8) 将收集的信息记录到信息安全数据库中。

c) 评估和决策

1) 对评估和决策的规划和准备要求，宜使能并支持一系列过程的开发和运行，来评价和指导信息安全事件响应行动。

2) 在评估和决策过程开发之前，过程责任者宜确保定义了信息安全事件识别和分级的最小信息，由必需和支持信息的具体项目组成。这个定义将允许响应规划者为所发现和报告事态的

完整性和分级开发一致的过程。宜定义区分正判和误判报告所需信息的充足性，并允许信息积累以支持对误判的发现和报告进行评估和响应。

3) 如果事件计划过程依赖于自动化信息管理和决策支持系统，宜明确这些系统的功能、实现和持续运行。事件处理过程责任者宜确保在开放响应过程之前，充分定义了其依赖的信息安全数据库。

4) 进行信息安全事态评估（包括需要时的升级）的PoC，宜使用信息安全事态/事件分级标度（包括基于受影响的资产/服务来确定事态影响），来判断事态是否为信息安全事件。

5) 评估信息安全事态的IRT宜确认一个事态是否为信息安全事件。为此，宜使用信息安全事态/事件分级标度再次评估来确认事态（疑似事件）类型和受影响资源（分类）的细节。继而对以下事项做出决策：如何处理已确认的信息安全事件，由谁处理，什么优先级，以及升级水准。

6) 评估信息安全漏洞（尚未被利用导致信息安全事态和潜在的信息安全事件），并对以下事项做出决策：需要做什么处理，由谁处理，如何处理和采取什么优先级处理。

7) 在信息安全数据库中完整记录所有评估结果和相关决策。

d) 响应

1) 对响应的规划和准备要求宜使能并支持响应信息安全事件的过程开发和运行。在对响应进行规划之前，事件处理过程责任者宜在以下方面收集定义、建立工作阈值或进行分类：信息和信息系统优先级、每一入侵类型的影响、损害规模、入侵报警级别和严重性。这些可以定性的或定量的，只要它们与评估和决策准备一致，并使IRT管理者能够为响应者分配事件行动或任务。

2) 在规划过程之前还宜定义响应级别，由成本、时间、技术资源的最小值和其他度量组成，以便能够相对于所报告和评估事件的已知信息来分配响应级别。宜包括立即或延迟响应，以及对在响应过程中如何管理单个或循环事件任务的定义。

3) 经IRT审查确定信息安全事件是否在控制之下：

i) 如事件在控制之下，则立即（实时或接近实时）或者稍后触发所需的事件响应；

ii) 如事件不在控制之下，或者会对组织的核心业务造成严重影响，则通过升级到危机处理功能来触发危机活动。

4) 定义在事件的管理过程中所涉及的所有内部和外部的功能和组织。

5) 酌情遏制和根除信息安全事件，以减轻或阻止信息安全事件范围和影响的扩大。

6) 需要时，进行信息安全证据分析。

7) 需要时，进行升级。

8) 确保所有涉及到的活动都得到正确记录以供日后分析。

9) 确保电子证据得到识别、收集/获得和保全。

10) 确保变更控制机制得到维护，从而使信息安全数据库保持最新。

11) 就存在的信息安全事件或任何相关细节与其他内部和外部人员或组织进行沟通。

12) 处理信息安全脆弱性。

13) 一旦事件得到成功地处理，便将其正式结束，并记录在信息安全数据库中。

14) 需要时，事件后续活动宜包括进一步的分析。

15) 组织宜确保信息安全事件管理计划允许信息安全事件响应既可以是即刻的，也可以是长期的。所有的信息安全事件宜经历过对业务运营的潜在不利影响的早期评估，包括短期的和长期的（例如，在某个初始信息安全事故后有时可能会发生重大破坏）。此外，宜允许对完全不可预见的信息安全事件作出某些必要的响应，这种情况下需要特别控制。即使对于这种情况，组织宜在计划文档中包含对必要步骤的通用指导。

e) 经验总结；

1) 从信息安全事件和脆弱性中吸取经验教训。
2) 审查、识别并进行对信息安全控制措施实施的改进（新的和（或）更新控制措施），以及对信息安全事件管理策略的改进，作为经验总结的结果。
3) 审查、识别并（如果可能）进行对组织现有信息安全风险评估和管理评审结果的改进，作为经验总结的成果。
4) 审查信息安全事件恢复和信息安全脆弱性处理的相关过程、规程、报告格式和（或）组织结构的有效性，并基于经验总结识别和进行信息安全事件管理计划及其文档的改进。
5) 更新信息安全数据库。
6) 在可信社区中沟通和共享审查结果（如果组织希望如此）。

6.5 事件分级标度

信息安全事态/事件分级标度宜用于对事态/事件依等级排列。在任何情况下，宜基于对组织业务运营的实际或预计的不利影响做出事件等级决定。

注：GB/Z 20986—2007 给出了信息安全事态和事件的分类分级方法，附录 C 还给出了其他方法示例。

6.6 事件表单

如果使用事件表单，宜在需要之前创建。表单的数量、类型和格式宜由IRT确定，并定期修订，以确保其实用性。宜附加一个允许描述性文本的表单类型。其目的是当现有表单不充分或适用的表单尚未建立时，提供一种在实例中获取信息的机制。

表单宜得到宣贯并对用户可用，以使报告信息安全事件的人熟悉它们。

表单示例参见附录B。

建议事件信息的电子交换和输入使用国际标准化的格式，并直接链接到电子的信息安全数据库。使用标准化的电子交换格式允许提高处理数据的自动化，减少多个团队合作处理事件时关联信息的工作量。在不能使用电子方式的情况下，可能需要纸质方式。

6.7 过程和规程

注：简便起见，术语“文件”在文中用来指过程和规程，除非两者有明显区别。

在能够开始信息安全事件管理计划运行之前，重要的是，组织已经记录并检查了必要的过程和规程是可用的。每个文件宜表明负责其使用和管理的团体或个人。

重要的是，要明白并非所有的文件在组织内或对于一般公众是现成可用的。例如，没有必要让所有的组织人员为与IRT交互而了解其内部运行。IRT宜确保可用的指南（包括信息安全事件分析的结果信息）在现成可用的表单中，例如，适当时，可以放在组织内部和（或）公共网站上。也许同样重要的是，对信息安全事件管理计划的某些细节保密，以防止内部人员篡改调查过程。例如，如果盗用资金的银行员工知道如何进行调查的某些细节，那么在信息安全的调查和恢复事件中，该员工就能够更好地向调查人员隐瞒其活动，或妨碍信息安全事件的发现、调查和从中恢复。

操作规程的内容取决于若干准则，特别是关系到已知的潜在信息安全事态、事件和脆弱性，以及可能涉及的信息系统资产类型及其环境。因此，操作规程可能关系到事件或产品（例如，防火墙、数据库、操作系统、应用程序）的特殊类型，或一个具体特定产品。每个操作规程宜明确操作步骤和操作者。它宜反映来自外部（例如，政府和商业IRT或类似的，以及供应商）以及内部的经验。

宜有操作规程来处理已知的信息安全事态、事件和脆弱性类型。当信息安全事态、事件或脆弱性不是已知类型时，也宜有操作规程来遵循。在这种情况下，宜解决以下问题：

a) 例外情况处理的报告过程；

b) 得到管理层批准的时间表，以避免延误响应；

c) 预授权的决策代理，可不经过正常批准过程进行决策。

IRT的操作规程开发宜包括文件化过程、相关责任和指定人员进行各种活动的角色分配（可以给一个人分配多个角色，这取决于组织的规模、结构和业务性质）。例如，IRT操作规程包括如下方面：

——关闭受影响的系统、服务和（或）网络，在某些情况下需要与相关IT和（或）业务管理事先协商一致；

——保留受影响的系统、服务和（或）网络继续连接和运行；

——监视受影响的系统、服务和（或）网络进出及内部的数据流；

——按照系统、服务和（或）网络安全策略，起动正常备份和危机管理规程和行动；

——监视和维护的电子证据的安全保全，以备法律起诉或内部纪律处分的需要；

——与内部和外部的人员或组织就信息安全事件细节进行沟通。可能包括与不同类型外部方进行沟通，诸如其他事件响应小组、信息共享组织、互联网服务提供商、软件和支持厂商、执法机构、客户、媒体和其他相关方。宜对与外部各方的所有接触和沟通进行记录，以备追责和取证所需。

6.8 信任和信心

IRT在组织的整体信息安全中扮演至关重要的角色。IRT需要组织全员合作来发现、解决和调查信息安全事件。IRT得到整个组织的信任和外部实体的信赖是基础。组织内的信任来自最高管理层的权威支持，即给予信任。与IRT合作的外部实体（例如，其他组织的IRT）对IRT工作的专业性需要有信心，即赢得信任。

IRT可以通过透明和成熟的过程赢得信任。IRT宜努力教育用户（内部的和外部的），说明IRT是如何工作、如何保护所收集信息的保密性和如何管理安全事态、事件和脆弱性报告的。IRT宜将清楚表明报告可疑信息安全事件或脆弱性人员或相关方的匿名或缺名期望的条款文件化并公开。

IRT宜具备有效满足组织的功能、财务、法律和政治需要的能力，并能够在管理信息安全事件和脆弱性时行使组织的裁量权。IRT的功能也宜得到独立审计，以确认所有的业务需求得到有效满足。

此外，将事件和脆弱性报告链与生产线管理分开，并使最高管理层直接负责管理事件和脆弱性响应，是实现独立性的另一个方面的有效方式。还宜实现财力分离，以避免不当影响。

6.9 保密或敏感信息处理

信息安全事件管理计划可能包含敏感信息，参与处理事件和脆弱性的人员可能被要求处理好敏感信息。组织宜确保建立必要的过程和能力，在需要时匿名化敏感信息（例如，当离开IRT的保护域时）。如果信息安全事态/事件/脆弱性经由一般问题管理系统记录，难以限制谁有权访问它，敏感的细节可被略去。如果IRT仍要访问略去的信息，那么IRT将维持自己的信息安全数据库。

如在GB/T 20985的本部分中其他处所概述，组织还宜确保信息安全事件管理计划规定了控制与外部各方沟通事件和脆弱性的条款，包括媒体、商业伙伴、客户、执法机构和公众。

7 建立事件响应小组

7.1 概述

注：第7章对应于GB/T 20985.1—2017，5.2 d)。

建立IRT的目标是为组织提供信息安全事件的评估、响应和经验总结，以及必要的协调、管理、反馈和沟通的适当能力。IRT有助于减少物理上和财务上的损失，以及有时与信息安全事件相关的组织声誉损害。

IRT的结构可能依据组织的规模、工作人员和行业类型的不同而不同。

7.2 事件响应小组类型和角色

IRT宣明确主要负责的对象集。这种对象集可以以多种不同方式来定义，包括（但不限于）组织的员工、被分配的特定IP地址范围、归属IP路由的特定自治系统（AS）、归属特定域（例如，.org）、具有某产品的客户、具有商业事件响应服务的客户，或覆盖一个地区或国家的人口。成员可自愿加入，按照合同协议（例如，购买服务或产品），或依据立法（例如，建立一个国家CERT）。

对象集的特点和规模以及IRT对其成员的权威和控制程度，将影响IRT能提供的服务类型和组织交付的适当形式。例如，IRT可能自己着手响应事件（无论是内部的还是合同服务的），可能与其他IRT协同工作，或者按需提供信息和帮助个人成员（例如，产品IRT）。

无论提供怎样的服务，IRT都需要响应策略（定义事件的构成、所需的响应和IRT的权力）、响应过程（定义IRT如何响应事件并交付响应）和实现这一过程的运行能力。

尽管IRT的主要角色是响应事件（无论是通过其自身的监控系统发现的、还是来自其对象集报告的，还是由外部源报告的），许多IRT还扮演着预防角色，通过改进其对象集中安全标准和实践，来降低事件发生的可能性和（或）严重性。IRT也可能具有行政管理角色，例如，报告和管理其自身的策略、过程和资源。

IRT可以各种方式来构造，包括按部门、按对象集焦点、按组织架构或按其他属性。一种构造方法是通过监控范围的类型，在这种情况下，有三种不同的类型（如图1所示）：单一、分层和远程。建立IRT时，宜考虑组织的规模、信息的重要性以及与其他组织的互操作性。图1中的T是指由特定IRT监控的目标。

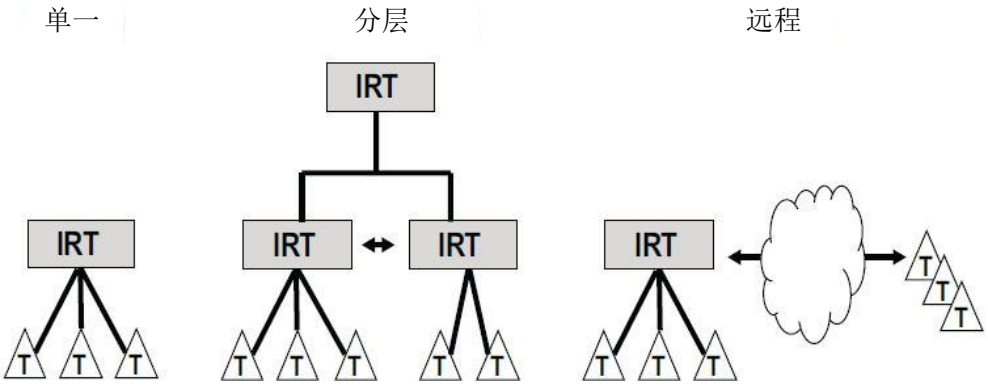

图 1 IRT 结构示例

——单一（单一类型IRT）：监控范围是单个组织或对多个组织或目标进行监控的单个IRT。这种类型一般用于事件管理、响应和操作的活动。

——分层（分层类型IRT）：一个或多个IRT重叠的监控范围。它可以增加对事件响应活动的可靠性；

——远程（远程类型IRT）：从远程位置收集安全事态。这种类型一般用于外包企业（专门的信息安全企业）来监控目标。

IRT的主要活动可包括但不限于以下方面：

——管理集成安全系统：在异构系统（例如，入侵检测系统、入侵防御系统、防火墙、网络资源等）上安装代理进行监控和信息安全事态管理。

——实行一贯的策略：根据定义的策略，通过一套一致的响应任务，最小化信息系统风险。

——及时响应：迅速响应威胁、破坏和攻击，以减少损失并降低恢复成本。

IRT的职责可能还包括如下监控和管理活动：

——集成管理和监控：24×7×365天监控目标、主动监控和响应事件、日志管理。

——报告管理：定期安全报告、安全补丁管理、事件报告。
——行政管理：各种系统环境的策略管理，包括任务控制和IRT操作。
——技术管理：网络、系统、应用、内容和服务的安全管理。
——系统运行和管理：系统容量、性能、安全配置和环境配置管理。
注：上述某些职责可以与 IRT 之外的其他组织单位共有或由其执行。

7.3 事件响应小组人员

有效的事件响应取决于IRT职员的能力和可靠性。当IRT的活动涉及建立安全事件管理策略、审计、与其他部门协调以及推进技术活动时，IRT职员及其能力变得更加重要。IRT成员所需的技能可能包括以下方面：

a）个人技能：沟通、问题解决、团队合作、时间和项目管理。
b）技术技能：安全原理、风险分析、威胁建模、脆弱性分析、日志分析。
c）事件响应能力：团队策略/程序、通讯、事件分析、事件记录和跟踪信息。
d）专业技能：表达、领导力、专长、编程。

为了响应各种类型的事件，IRT成员宜具备诸如下列的技术知识和技能：

——当前的网络安全问题，包括攻击、威胁、恶意软件和安全脆弱性；
——系统管理安全实践，诸如补丁管理、安全配置、备份和灾难恢复；
——密码技术（加密和散列算法）、数字签名、现行协议（诸如SSL/TLS）；
——通用网络协议，诸如以太网（IEEE 802.3）、WiFi（IEEE 802.11）、IPv4、IPv6、ICMP、UDP、TCP；
——公共网络应用协议，诸如DNS、SMTP、HTTP；
——数字取证、逆向工程；
——计算机科学和编程概念，诸如熵、安全开发，函数式和面向对象编程、系统架构和内存布局。

其他特定的知识和技能宜取决于IRT职责和组织使用的技术。上述所列示例是GB/T 20985本部分制定时的现状。IRT成员宜维持当前的知识和技能。

可参照表1所示的成员角色定义来组织IRT。表1定义的某些任务可以与IRT之外的其他组织共担或由其执行。IRT可以提供输入，但没有最终的权力。

表1　IRT职员角色与任务示例

角色	描述
IRT管理者	这个领导角色是负责管理职员，明确工作范围，向上级组织报告状态。
规划	负责IRT运行。建立或规划各种安全策略，并上报上级主管部门，与第三方合作，登记和批准脆弱性报告。该角色任务如下： a）建立和规划安全策略； b）执行安全过程； c）调整风险优先级； d）与上级组织和其他第三方机构沟通； e）支持行政管理； f）讨论/登记/批准关于目标组织的脆弱性报告； g）执行由IRT管理者安排的其他活动。
监控	负责实时监控和实际运行活动，诸如安全事态监控/发现/识别、事件登记和预防。执行实时安全监控活动如下： a）24小时×365天监控和运行； b）检测入侵、注册事件和第一时间响应； c）执行安全补丁和升级； d）实施安全策略和备份管理； e）服务台； f）设施管理； g）执行IRT管理者安排的活动。
响应	管理来自监控代理的事件（包括侵入、盗窃、数据外泄或暴露），做进一步的分析并采取行动（包括调查工作），采取恢复措施，并建立适当的策略。提供诸如实时响应、技术支持以及以下方面的服务： a）告知和报告事件； b）监测系统之间的关联分析； c）事件调查和恢复支持； d）关于目标组织和IRT的脆弱性分析； e）执行IRT管理者安排的活动。
分析	与响应团队的合作进行深入分析，包括对事件的关联分析。此外，还提供事件及以下方面的分析： a）为目标组织和IRT规划脆弱性分析； b）改进安全分析工具和检查清单； c）改进监控规则； d）发布简报； e）执行由IRT管理者安排的活动。

表2提供了IRT可能需要的各种岗位的职员类型、岗位范围和任务的示例。

表 2　IRT 职员岗位示例

职位	任务
管理者或团队领导	——提供战略方向 ——使能并促进团队成员的工作 ——监督团队 ——对管理层和其他方代表IRT ——面试和聘用新的团队成员
管理者助理、监督者或组长	——支持指定功能区域的战略方向 ——根据需要支持团队领导 ——为团队成员提供了指导和辅导 ——分配任务和职责 ——参与新的团队成员的面试
服务台或分诊职员	——处理事件或安全报告的IRT主电话 ——根据技能提供初步援助 ——承接初始数据输入并对收到信息进行分类和优先顺序
事件处理者	——开展事件分析、跟踪、记录和响应 ——协调为对象集提供的反应性和主动性指导（开发诸如文档、检查清单、最佳实践和指南等材料） ——传播信息 ——适当时，根据团队领导或其他管理职员的安排，与IRT团队、外部专家和其他方（诸如网站、媒体、执法或法律人员）配合 ——开展技术观察活动，如果被安排 ——（为IRT职员和（或）对象集）开发适当的培训材料 ——按照安排，辅导新的IRT职员 ——监控入侵检测系统，如果此服务是IRT活动的一部分 ——执行渗透测试，如果此服务是IRT活动的一部分 ——按照指示参与新职员的面试
脆弱性处理者	——分析、测试、跟踪和记录脆弱性报告和脆弱性制品 ——作为脆弱性响应的一部分，研究或开发补丁和修复 ——根据需要，与对象集、IRT团队、软件应用程序开发者、外部专家（其他IRT、研究者、厂商）及其他方（媒体、执法、或法律人员）配合 ——传播脆弱性和相应的修复、补丁或解决办法的信息 ——开展技术观察活动，如果被安排 ——按照安排，辅导新的IRT职员 ——参与新的IRT职员的面试
技术文档编写者	——协助和促进IRT开发出版物，诸如建议、最佳实践和技术提示

8 建立与其他组织的关系

8.1 概述

注：第8章对应于GB/T 20985.1—2017，5.2 e)。

与直接参与信息安全事项、事件和脆弱性管理的内部和外部组织建立并保持适当的关系和联络是必要的。

8.2 与组织其他部门的关系

事件管理不是一个封闭的过程。宜为整个组织建立关系、沟通渠道、数据共享协议以及策略和规程。这些内部协作可包括以下方面：

——业务管理者。他们需要了解IRT是什么，以及它怎样能够为支持他们的业务过程提供帮助。有关IRT对业务系统的权力，以及关键业务系统需要断网或关机时将由谁决定，宜做出协定。

——IT代表。宜明确IT职员和IRT之间的交互和工作流程，包括IT职员将采取什么行动和IRT成员将采取什么行动，IT职员可为IRT提供什么信息和IRT可为IT团队提供什么信息，以及他们的角色和权力分别是什么。

——法律部门代表。这些代表可为责任和合规问题提供指导，识别在事件过程中服务水平协议(SLA)受到影响没有，针对隐私权和公民自由权提供指导，以确保调查和响应措施不侵犯员工的权利。

——人力资源代表。他们将需要参与制定相关策略和规程，以辞退被发现从事未授权或非法计算机活动的员工。

——公共关系代表。他们宜做好准备处理任何媒体咨询，并帮助开发信息披露策略和实践。

——现有安全小组，包括物理安全。IRT需要与这些小组交换有关计算机事件的信息，并可能与他们分担责任来解决涉及计算机或数据窃取的问题。

——审计和风险管理专家。他们可以帮助开发威胁度量，并识别对象集系统的风险。

——任何执法联络员或调查员。他们要了解与执法机构宜如何合作，何时联系，以及谁来做调查和取证分析。

——对象集总代表。他们可以深入其需要和要求。

IRT宜有责任确保事件得到解决。为此，IRT管理者和其成员宜有权采取被认为对响应信息安全事件适合的必要措施。然而，可能对整体组织有不利影响（无论是经济上还是在声誉方面）的措施，宜得到最高管理层的同意。出于这个原因，信息安全事件管理的策略和计划有必要细化IRT管理者向哪个适当权威机构报告严重信息安全事件。权威机构，就其本身而言，宜承诺其对IRT成员可用，并及时提供指导。

与媒体打交道的规程和责任也宜由最高管理层同意并形成文件。这些规程指定组织内谁处理媒体咨询，以及如何与媒体接触。所有IRT成员宜学会如何根据媒体策略应对媒体提问。

8.3 与外部利益相关方的关系

组织宜在IRT和适当的外部利益相关方之间建立关系。IRT经常需要就事件与外界沟通，任何适合的时候，他们都宜这样做，诸如联系执法机构、应对媒体询问和寻求外部专家。另一个例子是与其他参与方讨论事件，诸如互联网服务提供商（ISP），有脆弱性软件的厂商或其他IRT。IRT也可主动与同行分享相关事件指示信息，以改进事件的发现和分析。

宜只在遵循组织和IRT的策略和过程，遵循任何适用的法律法规的情况下，与外部各方进行信息沟通。

IRT成员宜寻求加入可信任的从事IRT领域的同行社区，以增强他们的专业精锐和建立信息交换的信任关系。在事件处理的发现和报告阶段，与可信任的IRT伙伴交流技术信息，可以提高响应效率并有助于最小化对其他组织的影响。由于许多网络空间安全威胁同时影响多个组织，这种类型的信息共享被认为是负责任的IRT运行的关键。如果可行，宜建立自动的事件信息交流，以通过集体的IRT活动提高新事件的发现速度。

外部利益相关方包括但不限于：

a) 签约的　外部支持人员；
b) 外部组织的IRT；
c) 托管服务供应商，包括电信服务提供商、互联网服务供应商（ISP）、销售商和供应商；
d) 执法机构；
e) 紧急救援机构；
f) 适当的政府组织；
g) 法律人员；
h) 公共关系官员和（或）媒体人员；
i) 业务伙伴；
j) 客户；
k) 一般公众。

9　明确技术和其他支持

9.1　概述

注：第9章对应于GB/T 20985.1—2017，5.2 f)。

为了确保能够快速和有效地响应信息安全事件，组织宜获取、准备和测试所有必要的技术上和其他方面的支持手段。所有内部和外部方的支持和报告宜被明确，沟通渠道和工作流程宜达成一致。这些活动包括以下方面：

——访问组织资产的详细信息，其具有最新的资产登记和连接到业务功能的信息；
——访问与危机管理相关的文件化规程；
——访问文件化并发布的沟通过程，包括与组织关于媒体互动和信息披露策略符合的媒体沟通规程。例如，组织可能希望其公共事务办公室和法律部门参与媒体的所有事件讨论；
——使用信息安全数据库，并采用技术手段来迅速增添和更新数据库、分析信息和帮助响应（在某些情况下，组织可以要求手工记录），并的确保持数据库安全；
——使用标准格式和交换协议来接收和处理事态/事件/脆弱性警报或信息，感知信息安全运行环境的态势，以便基于风险主动采取补救措施；
——采用有助于信息安全/数字证据收集和分析的工具；
——为信息安全数据库安排足够的危机管理（有关业务持续性管理的指南，见ISO/IEC 27031、ISO 22301和ISO 22313）；
——明确支持和报告的外部各方，以及组织之间的联系点，包括如何和何时沟通。

组织宜确保用于迅速增添和更新数据库、分析信息和帮助响应信息安全事件的技术手段，支持以下方面：

a) 快速获取信息安全事态/事件/脆弱性报告；
b) 以适当的方式（例如，电子邮件、传真或电话）通知事前选定的外部人员，因此需要维护一个可靠的、易于访问的联系人数据库（包括纸质版和其他备份），以及能够以安全和适当的方式将信息传递到个人的设施；

c) 采取与评估的风险相适应的预防措施，以确保电子通信，无论采用的是互联网络还是非互联网络，都不能被窃听，并保持系统、服务和（或）网络在受到攻击时依然可用（这可能需要预先计划的替代通信机制准备就绪）；
d) 确保对有关信息系统、服务和（或）网络的所有数据的收集及其存储和处理是适当的；
e) 根据评估的风险如果需要，使用基于密码的完整性控制措施来帮助确定系统、服务和（或）网络是否以及哪部分和哪些数据发生了变化；
f) 促进所收集信息的归档和保护（例如，对日志和其他证据在离线存储到诸如CD或DVD-ROM只读介质之前应用数字签名）；
g) 能够打印输出（例如日志），包括那些说明事件进展情况、解决过程和监管链的输出；
h) 将信息系统、服务和（或）网络恢复到正常操作，并符合相关危机管理的如下规程：
   1) 备份测试；
   2) 恶意代码控制；
   3) 系统和应用软件的原始介质；
   4) 启动介质；
   5) 干净、可靠和最新的系统和应用程序补丁。

组织可从安装介质创建一个标准的基准镜像，并将该镜像作为创建系统的干净基础。使用这种镜像而非原有介质经常是优选的，因为镜像已经过了修补、强化、测试等。

被攻击的信息系统、服务或网络可能无法正常工作。因此，响应信息安全事件的必要技术手段（软件和硬件）宜尽可能地不依赖于组织的“主流”系统、服务和（或）网络来操作，并与评估的风险相适。所有的技术手段宜慎重选择、正确实施和定期测试（包括所制作备份的测试）。如果可能的话，技术手段宜完全独立。

注：本节所述技术不包括用于直接发现信息安全事件和入侵，并自动通知相关人员的技术手段。这种技术手段在ISO/IEC 27039中予以描述。

9.2 技术支持示例

这种机制可包括以下方面：
a) 内部信息安全审核机制，用来评估安全级别并跟踪脆弱的系统；
b) 脆弱性管理（包括安全更新和脆弱系统的安全修补）；
c) 技术手段的监视，以发现新型威胁和攻击；
d) 入侵检测系统（详见ISO/IEC 27039）；
e) 网络安全设备、保护手段和监控工具（详见ISO/IEC 27033）；
f) 防恶意代码软件；
g) 审核日志记录和日志监控软件。

9.3 其他支持示例

这种机制可包括运行支持团队的文件化职责和操作规程。

10 建立信息安全事件意识和培训

注：第10章对应于GB/T 20985.1—2017，5.2 g)。

信息安全事件管理不仅涉及技术手段，也涉及人。因此，宜得到组织内具备适当的信息安全意识和受训人员的支持（在GB/T 22080—2016，7.2中也被指出过）。

所有组织人员的意识和参与对一个结构化的信息安全事件管理方法的成功至关重要。用户宜意识到他们及他们的部门如何才能从结构化的信息安全事件管理方法中受益。此外，信息安全事件管理的结构化方法的效率和质量取决于许多因素，包括通知事件利益相关者的义务、通知的质量、易用性、速度和培训。其中有些因素与用户是否意识到信息安全事件管理的价值并积极报告事件有关。

组织宜积极推进信息安全事件管理成为企业级信息安全意识和培训计划的一部分。相关时，意识培训计划及相关材料宜提供给所有人员，包括新员工、第三方用户和承包商。必要时，宜针对PoC、IRT成员、信息安全人员和特定管理人员提供特定的培训计划。直接参与事件管理的不同人群可能需要不同级别的培训，这取决于他们与信息安全事件管理计划互动的类型、频率和关键性。

组织的意识教育宜包括以下方面：

a) 信息安全事件管理结构化方法给组织和个人带来的益处；

b) 信息安全事件管理计划是如何工作的，包括其范围、安全事态、事件和脆弱性管理工作流程；

c) 如何报告信息安全事态、事件和脆弱性；

d) 信息安全数据库中保存的事件信息及其输出；

e) 对相关事件源的保密控制；

f) 规划的服务水平协议；

g) 在哪些情况下对起源提供建议的结果告知；

h) 非披露协议规定的任何限制；

i) 信息安全事件管理组织的权威性和其报告路径；

j) 根据信息安全事件管理计划，由谁接收报告以及报告是如何分发的。

在某些情况下，组织可能期望在其他培训计划（例如，面向个人的计划或总的企业级安全意识计划）中包含信息安全事件管理特有的意识细节。这种意识方法能为特定的人群带来价值，进而提高培训计划的效果和效率。

信息安全事件管理计划开始运行之前，组织宜确保所有相关人员都熟悉涉及信息安全事件发现和报告的规程，并且有专门的选定人员对后续活动非常熟悉。随后宜是定期的意识教育和培训课程。培训宜为PoC和IRT成员以及信息安全人员和特定管理人员提供特定演练和测试的支持。

此外，宜通过建立和运行由信息安全事件管理人员支持的“热线”，对意识和培训计划进行补充，以尽量减少报告和处理信息安全事态、事件和脆弱性的延误。

11 测试信息安全事件管理计划

11.1 概述

注：第11章对应于GB/T 20985.1—2017，5.2 h)。

组织宜安排计划来定期检查和测试信息安全事件管理过程和规程，以突显可能在信息安全事态、事件和脆弱性管理过程中出现的潜在缺陷和问题。宜组织定期测试来检查过程/规程，并验证IRT响应。这些模拟场景可从基于现实攻击、失败或故障的严重、复杂事件到桌面演练。模拟的形式将取决于演练的预定目标。测试不仅涉及IRT，也涉及参与信息安全事件管理的某些或所有的内部和外部组织。组织宜确保对测试评审结果导致的任何变更进行了充分的检查，包括进一步的测试，然后再将变更的计划付诸实施。

当进行演练时，非常重要的是，所有参与者都意识到他们不是在处理真正的攻击。建立和保持这种差异是重要的，以防止人们触发可能对组织产生更大影响的行动（如启动建筑疏散）。这个规则只能在特定情况下可忽视，即当演练在严格控制的环境中进行时，以防止演练的影响波及到运行环境。

主要演练类型如下：

——基于讨论的；

——桌面推演的；

——现场实操的；

——上述组合的。

采用哪种演练类型取决于想要实现的目标以及可用的时间和资源。

每次演练经历以下阶段：

——规划和准备；

——执行；

——听取汇报和事后分析。

演练的规划和准备是基于当前的事件响应计划以及对未来威胁和趋势的设想。将事后分析的结果作为输入，以改进事件响应计划。

11.2 演练

11.2.1 定义演练的目标

一般而言，演练可有以下三个主要目标：

a) 确认：确认事件响应计划并识别潜在的遗漏；

b) 培训：让相关人员练习并顺利承担其角色；

c) 测试：测试当前现有过程和规程。

一次演练通常有多个目标。演练目标很大程度上取决于组织准备的整体状态。当组织在准备新的事件响应计划或更新现有计划时，可通过演练确认计划。计划出台并实施后，组织将通过演练对人员进行培训。现有的过程和规程确立之后，需要定期测试以确保其持续的有效性。

表3给出了采用哪种类型演练实现哪些目的的指南。

表 3 演练目标映射到演练类型

目标	演练类型
确认新计划	基于讨论 桌面
人员培训	基于讨论 桌面 现场
确认现有计划是否仍有效	桌面 现场

11.2.2 定义演练的范围

演练范围主要由其目标定义。当定义演练范围时，需要考虑以下方面：

a) 演练是仅限于组织内部人员，还是有外部组织参与；

b) 谁确实需要参与，即：只是IRT，还是需要有来自其他团体的人员，如果有的话，是哪些团体；

c) 需要多少位演练领导。

范围直接影响到哪些组织将参与演练以及什么样的参与者。

11.2.3 执行演练

当进行演练时，非常重要的是，让所有参与者都知道，所处理的场景只是一个演练，而不是真实的事态。如果参与者无法分辨模拟事态与真实事态，他们的行动有可能导致后果扩大或将演练以外的人员卷入。最坏的情况，可能导致公众恐慌。

成功的演练需要完成一些任务。下面的列表仅提供主要任务的一般概述：

a) 在开始的时候，向参与者简要说明演练目标；
b) 确保所有参与者的安全（当有志愿者参与现场演练时尤为重要）；
c) 确保所有参与者都知道自己的角色；
d) 确保有足够数量的人员在整个演练过程中引导参与者；
e) 宜为演练过程中的讨论分配足够的时间，但也不能因过量而扰乱演练；
f) 演练后留出足够的时间和资源来听取所有参与者的情况汇报，并收集他们的反馈（注意，反馈包括两方面：演练的目的是什么和演练本身是如何进行的）；
g) 创建并分发演练报告给利益相关者。

11.3 事件响应能力监测

11.3.1 实施事件响应能力监测计划

事件响应能力不仅包括IRT的能力，而且还包括应IRT请求在事件处理过程中提供帮助的个人和团体的能力。虽然大多数的事件响应能力将集成在IRT中，但有可能缺少某些狭窄领域的专业知识。出于这个原因，IRT可能聘用能够填补这一空白的个人或其他团队。

通过监控事件特征和事件发生时这些特征发生的频率，有可能勾勒出IRT需要具备的能力。这些能力将随时间改变。有些改变的发生是由于组织内的技术因被放弃或引入新技术而改变引起的。将所有数据从SQL数据库中转移到非SQL数据库是放弃技术的一个例子。允许员工使用移动电话来执行他们的任务是引入以前在组织内不存在的新技术的例子。可要求IRT能力改变的另一个原因是开发新的攻击技术。

并非所有的能力都是技术性的。某些威胁，特别是那些不依赖于技术的威胁（例如社会工程），最好用非技术手段来应对。

11.3.2 事件响应能力监测的度量和治理

IRT的能力宜足以应对组织面临的当前威胁。随着威胁的变化，团队能力也在改变以使组织能够有效地响应新的威胁。同时，当威胁或者永久地被减少到可以忽略的程度，或者风险的根本原因被移除时，某些功能可能就不再需要。另外，尽管IRT宜是专业知识的焦点中心和事件处理能力的主要承担者，但并不要求其拥有所有的知识和能力。很少使用的专业知识和能力可能分散在组织内部或外部的不同个人或团体当中。其主要原因是成本效益。

针对这种能力分散和不断变化的需求，组织宜建立一个能反映组织当前能力的注册表。以下未穷举列表说明这个注册表可能包含哪些信息：

a) 什么能力对组织可用；
b) 谁拥有它们；
c) 它们是组织内部的还是外部的；
d) 怎样聘用能力具备者；
e) 能力在多大程度保持不过时（或其最后使用过后的代理措施）；
f) 在过去一段时间间隔中，能力被需求的频繁程度。

然后，将这些信息用于IRT能力开发的规划中。很少使用的能力可能会任其消失，经常使用但IRT尚不具备的能力可以得到，依此类推。

12 经验总结

12.1 概述

注：第12章对应于GB/T 20985.1—2017，5.6)。

一旦结束一个信息安全事件，重要的是，组织在处理完信息安全事件后宜迅速找出和总结经验，并确保所得结论付诸行动。此外，还可从报告的信息安全脆弱性的评估和解决方案中总结经验。经验总结可能产生以下一个或多个结果：

a) 新的或变更的信息安全控制措施要求，可能是技术的或非技术的（包括物理的）控制措施。依靠经验总结，这些控制措施可能包括需要快速更新和交付信息安全意识教育材料（为用户及其他人员），以及快速修订和发布安全指南和（或）标准；

b) 新的或变更的威胁和脆弱性信息，从而导致组织现有的信息安全风险评估和管理评审结果的改变；

c) 信息安全事件管理计划及其过程、规程、报告形式和（或）组织结构，以及信息安全数据库的变更。

12.2 识别经验教训

组织不宜只看单一的信息安全事件或脆弱性，宜检查其趋势/模式，这本身可能有助于识别是否需要变更控制或方法。IT信息安全事件之后，进行信息安全测试，特别是脆弱性评估，也是一种明智的做法。因此，组织宜定期分析信息安全数据库中的数据，来做以下方面的事情：

——识别趋势/模式；

——识别关注的领域；

——分析在哪里可以采取预防措施，以减少未来事件发生的可能性。

宜将在整个信息安全事件的过程中获取的相关信息引入趋势/模式分析（类似于处理报告的信息安全脆弱性的方式）。基于以往的经验和记载的知识，将显著地有助于早期识别的信息安全事件，并提供可能引起进一步信息安全事件的警告。

也宜利用来自政府、其他IRT和供应商的信息安全事件和相关脆弱性信息。

信息系统、服务和（或）网络的脆弱性评估/安全性测试，不宜只限于受到信息安全事件影响的信息系统、服务和（或）网络。宜扩展到包括任何相关的信息系统、服务和（或）网络。当信息安全事件发生在其他信息系统、服务和/或网络中时，完整的脆弱性评估被用来注意在信息安全事件过程中是否在其他信息系统、服务和（或）网络中存在脆弱性被利用的情况，以确保没有新　　的脆弱性被引入。

需强调的是，宜定期进行脆弱性评估，以及信息安全事件发生后脆弱性的再评估宜是持续评估过程的一部分，而不是一种替代。

整个组织的信息安全策略中规定的组织信息安全管理论坛和（或）其他论坛的每次会议上，宜产生信息安全事件和脆弱性的分析总结。

12.3 识别并实施信息安全控制措施的改进

在解决了一个或多个信息安全事件或脆弱性后的评审过程中，可能识别出所需要的新的或变更的控制措施。立即实现这些建议和相关的控制要求可能在经济上或操作上是不可行的，在这种情况下，它们宜作为组织的长期目标。例如，迁移到更安全、更强大的防火墙，可能在短期内经济上不可行，但需要纳入组织的长期信息安全目标。

按照商定的建议，组织宜实施更新和（或）新的控制措施。这可能是技术的（或物理的）控制措施，可能需要安全意识简报材料的快速更新和分发（为用户，以及其他人员），以及安全指南和（或）标准

的快速修订和发行。此外，组织的信息系统、服务和（或）网络宜定期进行脆弱性评估，以帮助识别脆弱性并提供持续的系统/服务/网络强化的过程。

此外，尽管对信息安全相关规程和文档的评审可以在信息安全事件善后或脆弱性解决后立即进行，这更像是所需的后续响应。信息安全事件或脆弱性得到解决后，如果相关，组织宜更新其信息安全策略和规程，以考虑在事件管理过程中收集的信息和识别的任何问题。同组织信息安全管理者一道，共同确保这些信息安全策略和规程的更新在整个组织中得到传播，宜是IRT的长期目标。

在经验总结阶段可能识别到其他改进，例如，信息安全策略、标准和规程的更改，IT硬件和软件配置的更改。组织宜确保这些得到执行。

经验总结的一种特殊情况是信息安全事件管理计划的非标准应用的分析。这种情况发生在报告过程被用于报告像IT问题（例如计算机或应用程序故障）、组织内部的不当行为（揭发者）这类事态或其他与信息安全不相关的事态。这种使用实例的增加能说明组织其他方面中的问题，或者缺少对报告过程的正确目的和使用的培训。这一分析的潜在结果可能会向最高管理层突显其他非安全相关的过程或组织某些方面中的不足。

12.4 识别并实施信息安全风险评估和管理评审结果的改进

根据信息安全事件的严重程度和影响（或与报告的信息安全脆弱性相关的严重程度和潜在影响），信息安全风险评估和管理评审结果的评估可能有必要考虑新的威胁和脆弱性。作为信息安全风险评估和管理评审更新完成的后续行动，可能有必要引入变更的或新的控制措施（见11.3）。

12.5 识别并实施信息安全事件管理计划的改进

作为后事件解决方案的一部分，IRT管理者或被任命者宜复查所有已经发生的一切以评估并进而量化对信息安全事件整体响应的有效性。

这种分析旨在确定哪部分信息安全事件管理计划是成功的，以及识别需要的任何改进。

后响应分析的一个重要方面是将信息和知识反馈回信息安全事件管理计划。如果事件非常严重，组织宜确保当事件解决后人们还记忆犹新的时候，立即安排一次所有相关方参与的会议。在这种会议上考虑的因素包括以下方面：

a) 信息安全事件管理计划中给出的规程按预期运行了吗？

b) 有什么规程或方法帮助了事件发现？

c) 有什么规程或工具在响应过程中具有帮助作用？

d) 有什么规程在事件被识别后帮助了信息系统恢复？

e) 在事件发现、报告和响应过程中，与所有相关方的事件沟通是否有效？

会议结果宜形成文件。组织宜确保被识别的信息安全事件管理计划改进区域得到评审，并且得到论证的改变纳入计划文档的更新。对信息安全事件管理过程、规程和报告表单的改变，在生效宜得到彻底检查和测试。

12.6 事件响应小组评价

相比于经验总结，评价是对IRT的有效性进行定期和更全面的评估。一旦IRT投入运行，团队和其管理人员宜评价团队的有效性以及它满足对象集需要的情况。评价可以定期进行或评价的某些方面也可以集成到运行和经验总结过程中。

评价活动的例子包括以下方面：

——确定哪些活动良好，哪些不是。

——适时修订策略并设计和实施计划。

——评价已生效的能力和服务。

——检查IRT在与对象集及任何外部合作伙伴和协作方合作方面做的怎样。

更具体的反馈机制的例子包括以下方面：

a) 基准测试；

b) 与对象集及外部合作伙伴和协作者的代表的一般性讨论或访谈；

c) 定期对对象集成员进行调查；

d) 创建一套准则或质量参数，供审计或第三方评价IRT时使用。

收集性能度量也能帮助评价IRT的成功。可能的度量可包括但不限于以下方面：

——事件统计，诸如不同类型事件的数量、响应时间、事件的生存时间、事件的解决方案或处置；

——向对象集报告的有关计算机安全问题或当前活动的信息量；

——当下的预防性技术和安全实践。

任何改变和改进宜基于评价的结果。

12.7 其他改进

有时事件分析的结果，可能与事件管理不太相关，但可以帮助组织理顺运行或其他改进。下面的列表给出了这种改进示例，并未穷举或排他：

——过长时间或不经常产生的补救措施可导致对软件或硬件厂商选择准则的改进；

——处理事件过程中人员配备不足可通过改进工作调度解决；

——知识的缺乏可以反映教育方面存在的差距。

附 录 A
（资料性附录）
法律法规方面

信息安全事件管理策略和相关方案中宜关注信息安全事件管理的如下法律法规方面。

a) **提供足够的数据保护和个人信息的隐私保护。**在那些有特定法律涵盖数据保密性和完整性的国家中，对于个人数据的控制常常受到限制。由于信息安全事件通常需要归因到个人，个人特性的信息可能因此需要被相应地记录和管理。因此，结构化的信息安全事件管理方法需要考虑适当的隐私保护。这可能包括以下方面：
   1) 如果实际情况可行，访问被调查人的个人数据的人员不宜与其存在私交；
   2) 在允许访问个人数据之前,宜签署保密协议；
   3) 信息宜仅用于其被获取的明示目的，即信息安全事件调查。

b) **维护适当的记录保存。**一些国家的法律，要求公司维护其活动的适当记录，在每年组织的审计过程中进行审查。政府机构也有类似的要求。在某些国家，要求组织报告或生成执法用的档案（例如，当涉及到对政府敏感系统的严重犯罪或渗透时）。

c) **控制措施到位以确保实现商业合同义务。**当对信息安全事件管理服务提出要求时，例如，满足所需的响应时间，组织宜确保提供适当的信息安全来保证在任何情况下满足这种义务要求。与此相关，如果组织寻求外部方支持并签署合同，例如外部IRT，那么宜确保在与外部方签署的合同中涵盖了所有要求，包括响应时间；

d) **处理与策略和规程相关的法律问题。**与信息安全事件管理方案相关的策略和规程宜就潜在的法律法规问题得到检查，例如，是否有关于对那些引起信息安全事件的事项采取惩戒和（或）法律诉讼的声明。在一些国家，解雇人员并不是一件容易的事情；

e) **检查免责声明的法律效力。**信息事件管理团队和任何外部支持人员所采取行动的免责声明的法律效力宜得到检查。

f) **与外部支持人员的合同涵盖所有要求的方面。**与任何外部支持人员的合同，例如来自外部IRT人员，在免除责任、保密、服务可用性和错误建议的影响方面宜得到彻底检查。

g) **保密协议可强制执行。**信息安全事件管理团队成员在入职和离职时，可被要求签署保密协议。在一些国家，已签署的保密协议可能在法律上无效，宜对此予以核实。

h) **满足执法的要求。**执法机构可能会合法地请求来自信息安全事件管理方案的信息，与其相关的问题需要澄清。可能的情况是，宜明确按照法律规定的最低水平要求，来记录事件和保持记录存档的时长。

i) **明确责任。**需要明确潜在的责任和所需的相关控制措施是否到位。可能具有相关责任问题的事态示例如下：
   1) 如果一个事件可能影响到其他组织（例如，披露共享信息，但没有及时通知，导致其他组织受到不利影响）；
   2) 如果在产品中发现新的脆弱性，但供应商未得到通知，随后发生了重大相关事件，给一个或多个其它组织带来重大影响；
   3) 没有编制报告，但在某些国家，在涉及到对政府敏感系统或关键国家基础设施组成部分的严重犯罪或渗透时，要求组织报告或生成执法用的档案；
   4) 披露的信息似乎表明某人或组织可能被卷入了攻击。这可能会损害涉案个人或组织的声誉和业务；

5) 披露的信息表明可能是特定软件的问题，但后来发现并非如此。

j) **满足具体法规要求。**当有具体法规要求时，宜将事件报告给指定机构，例如，在许多国家对核电工业、电信公司和互联网服务提供商有那样的要求。

k) 能够成功起诉或执行内部纪律规程。适当的信息安全控制措施宜到位，包括可证明防篡改的审计跟踪，以此能够成功地对“攻击者”起诉或执行内部纪律规程，无论攻击是技术的还是物理的。为支持这项工作，需要以在适当的国家法院或其他仲裁机构上可接受的方式收集证据。从而可以表明：

1) 记录是完整的且没有以任何方式被篡改；

2) 电子证据副本可证明与原件相同；

3) 任何收集证据的IT系统在证据被收集时是正常运行的。

l) **与监控技术相关的法律问题得到解决。**在有关国家立法的语境下，使用监控技术的影响需要解决。各种技术的合法性随着国家不同而不同。例如，在一些国家，有必要让人们意识到在发生监控活动，包括通过监视技术。需要考虑的因素包括谁/什么正在被监控，它们/它如何被监控，以及监控什么时候正在发生。还宜指出，在IDS语境下的监控/监视在ISO/IEC 27039中做了具体讨论。

m) **可接受的使用策略得到定义和沟通。**可接受的实践/使用宜得到定义，形成文件，并与所有预期用户沟通。例如，当加入一个组织或获得信息系统的访问权限时，宜告知用户可接受的使用策略，并要求提供书面确认，以表明他们理解和接受这一策略。

附 录 B
（资料性附录）
信息安全事态、事件和脆弱性报告及表单示例

B.1 概述

附录B包含信息安全事态、事件和脆弱性的记录事项及其报告表单示例。需要强调的是，这些仅是示例。还有其他例子，诸如事件对象描述和交换格式（IODEF）标准中的模式。

B.2 记录事项示例

B.2.1 信息安全事态记录事项示例

包括信息安全事态的基本信息，诸如事态何时发生、发生了什么、如何发生的和为什么发生，以及报告人的联系信息。

——基本信息
  ——事态日期
  ——事态编号
  ——相关事态和（或）事件编号（适用时）
——报告人详情
  ——姓名
  ——联系方式，诸如地址、单位、部门、电话和电子邮箱
——事态描述
  ——发生了什么
  ——如何发生的
  ——为什么发生
  ——对受影响组件或资产的初步意见
  ——对业务的不利影响
  ——识别的任何脆弱性
——事态详情
  ——事态发生的日期和时间
  ——事态被发现的日期和时间
  ——事态被报告的日期和时间

B.2.2 信息安全事件记录事项示例

包括信息安全事件的基本信息，诸如事件何时发生、发生了什么、如何发生的和为什么发生，以及事件类别、影响和事件响应结果。

——基本信息
  ——事件日期
  ——事件编号
  ——相关事态和（或）事件编号（适用时）

——报告人详情
——姓名
——联系信息，诸如地址、单位、部门、电话和电子邮箱
——联络点（PoC）成员详情
——姓名
——联系信息，诸如地址、单位、部门、电话和电子邮箱
——IRT成员详情
——姓名
——联系信息，诸如地址、单位、部门、电话和电子邮箱
——事件描述
——发生了什么
——如何发生的
——为什么发生
——对受影响组件或资产的初步意见
——对业务的不利影响
——识别的任何脆弱性
——事件详情
——事件发生的日期和时间
——事件被发现的日期和时间
——事件被报告的日期和时间
——事件类别
——受影响的组件或资产
——事件对业务的不利影响
——从事件中恢复的总成本
——事件解决方案
——涉及的人员或作案者（如果事件是由人引起的）
——作案者描述
——实际或感知的动机
——解决事件所采取的行动
——解决事件所计划的行动
——未完成的行动
——结论
——被告知的内部人员/实体
——被告知的外部人员/实体

B.2.3 信息安全脆弱性记录事项示例

包括信息安全脆弱性的基本信息，诸如脆弱性何时被识别、识别的是什么和如何被识别的，以及潜在影响和解决方案。

——基本信息
——脆弱性被识别的日期
——脆弱性编号
——报告人详情
——姓名

——联系信息，诸如地址、单位、部门、电话和电子邮箱

——脆弱性描述

——脆弱性解决方案

B.3 表单使用方法

B.3.1 日期和时间格式

日期输入格式宜为CCYY-MM-DD（和HH-MM-SS，需要时）。多个事件可能跨时区发生，如果这些事件相关，宜使用UTC时间（或至少说明所使用时间的UTC时差），以便进行比较（见ISO 8601）。

B.3.2 完成说明

信息安全事态和事件报告表单旨在向适当人员提供有关信息安全事态和事件(如果信息安全事态被确定为事件）的信息。

如果怀疑信息安全事态正在发生或可能已经发生,特别是可能给组织的资产或声誉造成重大损失或影响的，宜按照组织的信息安全事件管理计划中描述的规程立即填写并提交信息安全事态报告表单（见本附录第一部分）。

所提供的信息将用于启动适当的评估，来判断该事态是否属于信息安全事件，是否可以采取哪些必要的补救措施来避免或减少损失或损坏。鉴于此过程可能具有时间关键性，此时不必填完报告表单中的所有项。

当PoC成员审阅全部或部分完成的表单后，要决定该事态是否属于信息安全事件。如果被归属于事件，则宜尽可能详细填写信息安全事件表单，并将信息安全事态和事件表单一并提交给IRT。无论信息安全事态是否属于事件，都宜更新事件管理系统。

当IRT成员审阅PoC成员提交的信息安全事态和事件表单后,宜随着调查进展更新事件表单及事件管理系统中的相关项。

信息安全脆弱性表单旨在提供感知到的脆弱性信息，作为脆弱性解决方案的信息库。

填写表单时，请遵守以下指南：

——建议以电子方式填写并提交表单。当使用电子报告机制（例如电子邮箱）存在或认为存在问题时，包括当认为系统可能受到攻击，电子报告表单可能被未授权人员读到时，可使用替代的方法来进行报告。替代的方法可包括亲自、电话或短信。

注：例如，采用安全网页表单链接到电子的信息安全事态/事件/脆弱性数据库。在当今世界，还基于纸质的操作是耗费时间的。但是，基于纸质的计划可作为电子计划不可用时的备份。

——仅提供已知事实的信息，不要为了完成表单项而进行猜测。如果有必要提供未确认的信息，请清楚地说明该信息是未经确认的，以及其有可能是真实的理由。

——宜提供详细联系方式。为获得关于报告的进一步信息，可能有必要或者立即或者过后联系报告人。

如果后续发现提交的信息不准确、不完整或有误导，宜修正或重新提交表单。

B.4 表单示例

B.4.1 信息安全事态报告表单示例

<table>
<tr><td colspan="3">信息安全事态报告</td><td>第1页 共1页</td></tr>
<tr><td>1 事态日期</td><td></td><td rowspan="2">3 相关事态和（或）事件编号（适用时）</td><td rowspan="2"></td></tr>
<tr><td>2 事态编号[1]</td><td></td></tr>
<tr><td colspan="4">4 报告人详情</td></tr>
<tr><td>4.1 姓名</td><td></td><td>4.2 地址</td><td></td></tr>
<tr><td>4.3 单位</td><td></td><td>4.4 部门</td><td></td></tr>
<tr><td>4.5 电话</td><td></td><td>4.6 电子邮箱</td><td></td></tr>
<tr><td colspan="4">5 信息安全事态描述</td></tr>
<tr><td colspan="2">5.1 事态描述：
• 发生了什么
• 如何发生的
• 为什么发生
• 对受影响组件或资产的初步意见
• 对业务的不利影响
• 识别的任何脆弱性</td><td colspan="2"></td></tr>
<tr><td colspan="4">6 信息安全事态详情</td></tr>
<tr><td colspan="2">6.1 事态发生的日期和时间</td><td colspan="2"></td></tr>
<tr><td colspan="2">6.2 事态被发现的日期和时间</td><td colspan="2"></td></tr>
<tr><td colspan="2">6.3 事态被报告的日期和时间</td><td colspan="2"></td></tr>
<tr><td colspan="2">6.4 事态响应是否结束？</td><td colspan="2">是□ 否□ （适当时勾选）</td></tr>
<tr><td colspan="2">6.5 如果是，说明事态持续了多长时间（日/时/分）</td><td colspan="2"></td></tr>
</table>

1） 事态编号宜由组织的IRT管理者分配。

B.4.2 信息安全事件报告表单示例

<table>
<tr><td colspan="3">信息安全事件报告</td><td>第1页 共6页</td></tr>
<tr><td>1 事件日期</td><td></td><td rowspan="2">3 相关事态和（或）事件编号（适用时）</td><td rowspan="2"></td></tr>
<tr><td>2 事件编号[2]</td><td></td></tr>
<tr><td colspan="4">4 联络点（PoC）成员详情</td></tr>
<tr><td>4.1 姓名</td><td></td><td>4.2 地址</td><td></td></tr>
<tr><td>4.3 单位</td><td></td><td>4.4 部门</td><td></td></tr>
<tr><td>4.5 电话</td><td></td><td>4.6 电子邮箱</td><td></td></tr>
<tr><td colspan="4">5 IRT成员详情</td></tr>
<tr><td>5.1 姓名</td><td></td><td>5.2 地址</td><td></td></tr>
<tr><td>5.3 单位</td><td></td><td>5.4 部门</td><td></td></tr>
<tr><td>5.5 电话</td><td></td><td>5.6 电子邮箱</td><td></td></tr>
<tr><td colspan="4">6 信息安全事件描述</td></tr>
<tr><td colspan="2">6.1 进一步的事件描述
• 发生了什么
• 如何发生的
• 为什么发生
• 对受影响组件或资产的初步意见
• 对业务的不利影响
• 识别的任何脆弱性</td><td colspan="2"></td></tr>
<tr><td colspan="4">7 信息安全事件详情</td></tr>
<tr><td colspan="2">7.1 事件发生的日期和时间</td><td colspan="2"></td></tr>
<tr><td colspan="2">7.2 事件被发现的日期和时间</td><td colspan="2"></td></tr>
<tr><td colspan="2">7.3 事件被报告的日期和时间</td><td colspan="2"></td></tr>
<tr><td colspan="2">7.4 报告人的身份/联系方式</td><td colspan="2"></td></tr>
<tr><td colspan="2">7.5 事件响应是否结束？</td><td colspan="2">是□ 否□ （适当时勾选）</td></tr>
<tr><td colspan="2">7.6 如果是，说明事件持续了多长时间（日/时/分）</td><td colspan="2"></td></tr>
</table>

2) 事件编号宜由组织的IRT管理者分配，并链接到相关的事态编号。

信息安全事件报告	第2页 共6页
8 信息安全事件类别	
（勾选一项，然后完成下面的相关部分） **8.1 实际的** *（事件已经发生）*☐ **8.2 怀疑的** *（事件被认为已经发生但没有确认）*☐	
8.3 自然灾害 *（指出涉及的威胁类型）*☐	
☐**地震** ☐**火山** ☐**洪水** ☐**暴风** ☐**闪电** ☐**海啸** ☐**崩塌** ☐**其他**	
具体说明：	
8.4 社会动乱 *（指出涉及的威胁类型）*☐	
☐**示威游行** ☐**恐怖袭击** ☐**战争** ☐**其他**	
具体说明：	
8.5 物理损害 *（指出涉及的威胁类型）*☐	
☐**火灾** ☐**设备毁坏** ☐**设备盗窃** ☐**设备丢失** ☐**设备篡改** ☐**水灾** ☐**介质毁坏** ☐**介质盗窃** ☐**介质丢失** ☐**介质篡改** ☐**静电** ☐**恶劣环境（诸如污染、灰尘、腐蚀、冻结）** ☐**其他**	
具体说明：	
8.6 基础设施故障 *（指出涉及的威胁类型）*☐	
☐**电源故障** ☐**网络故障** ☐**空调故障** ☐**供水故障** ☐**其他**	
具体说明：	
8.7 辐射干扰 *（指出涉及的威胁类型）*☐	
☐**电磁辐射** ☐**电磁脉冲** ☐**电子干扰** ☐**电压波动** ☐ **热辐射** ☐**其他**	
具体说明：	
8.8 技术故障 *（指出涉及的威胁类型）*☐	
☐**硬件故障** ☐**软件故障** ☐**过载（信息系统容量饱和）** ☐**维护性破坏** ☐**其他**	
具体说明：	

信息安全事件报告	第3页　共6页
8 信息安全事件类别	
8.9 恶意软件（*指出涉及的威胁类型*）☐	
☐**计算机病毒**　☐**网络蠕虫**　☐**恶意代码内嵌网页**　☐**混合攻击** ☐**特洛伊木马**　☐**僵尸网络**　☐**恶意代码宿主站点**　☐**其他**	
具体说明：	
8.10 技术攻击（*指出涉及的威胁类型*）☐	
☐**网络扫描**　☐**脆弱性利用**　**后门利用**　☐**登录尝试**　☐**干扰**　☐**拒绝服务（DoS）**　☐**其他**	
具体说明：	
8.11 规则违背（*指出涉及的威胁类型*）☐	
☐**资源未授权使用**　☐**版权违反**　☐**其他**	
具体说明：	
8.12 功能损害（*指出涉及的威胁类型*）☐	
☐**权限滥用**　☐**权限伪造**　☐**行为抵赖**　☐**误操作**　☐**人员可用性破坏**　☐**其他**	
具体说明：	
8.13 信息损害（*指出涉及的威胁类型*）☐	
☐**拦截**　☐**窃听**　☐**伪装**　☐**网络钓鱼**　☐**数据丢失**　☐**数据错误**　☐**数据流分析** ☐**间谍**　☐**泄露**　☐**社会工程**　☐**数据窃取**　☐**数据篡改**　☐**位置检测**　☐**其他**	
具体说明：	
8.14 有害内容（*指出涉及的威胁类型*）☐	
☐**非法内容**　☐**恐慌内容**　☐**恶意内容**　☐**滥用内容**　☐**其他**	
具体说明：	
8.15 其他（*如果尚未确定事件是否属于上述类别，勾选这里*）☐	
具体说明：	

信息安全事件报告	第4页 共6页
9 受影响的组件/资产[3]	
受影响的组件/资产（如果有）	*（提供受事件影响或与事件相关的组件/资产的描述，包括相关的序列号、许可证和版本号。）*
9.1 信息/数据	
9.2 硬件	
9.3 软件	
9.4 通信	
9.5 文档	
9.6 过程	
9.7 其他	

10 事件对业务的负面影响				
对以下每个选项，如果相关则勾选。然后，考虑所有受事件影响方，使用影响类别指南，在“数值”一栏中以1至10标度填写对业务负面影响的级别。事件影响类别包括：业务运营的财务损失/中断、商业和经济利益、个人信息、法律法规义务、管理和业务运营、信誉损失。在“指南”一栏中填写适用指南的代码。如果知道实际成本，则填写在“成本”一栏中。				
		数值	**指南**	**成本**
10.1 保密性遭受破坏 *（即未授权披露）*	☐			
10.2 完整性遭受破坏 *（即未授权更改）*	☐			
10.3 可用性遭受破坏 *（即不可用）*	☐			
10.4 抗抵赖性遭受破坏	☐			
10.5 信息和（或）服务遭受破坏	☐			
11 事件恢复总成本				
如果可能，宜给出事件恢复的实际总成本，以1至10标度填写“数值”一栏，以实际情况填写“成本”一栏。		**数值**	**指南**	**成本**

3) 这一项是为了获得更多的受影响组件/资产细节（如果有），用于深入调查和分析（在事态和事件分析的初始阶段通常只收集到高层信息）。

信息安全事件报告	第5页　共6页
12 事件解决方案	
12.1 事件调查开始日期	
12.2 事件调查人员姓名	
12.3 事件结束日期	
12.4 影响结束日期	
12.5 事件调查完成日期	
12.6 调查报告的引用和位置	
13 （如果事件由人引起）涉及的人员/作恶者	
□个人　□合法建立的组织/机构　□有组织的团体 **□意外　□无作恶者***（例如，自然因素、设备故障、人无错误）*	
14 作恶者描述	
15 实际或察觉到的动机	
□犯罪/经济收益　□消遣/黑客攻击　□政治/恐怖主义　□报复　□其他 *具体说明:*	
16 为解决事件已采取的行动	
（例如，“无行动”、“内部行动”、“内部调查”、“由……进行的外部调查”）	
17 为解决事件计划采取的行动	
（例如，见上例）	
18 未完成的行动	
（例如，调查任在被其他人员要求）	

信息安全事件报告	第6页 共6页

19. 结论

（勾选指出事件是重大还是较小，并给出论证这一结论的简短叙述）

□ **重大** □ **较小**

（指出任何其他结论）

20. 被通知的内部人员/实体

（本细节由负责信息安全并规定所需行动的相关人员填写。相关时可能由组织的信息安全管理者或其他负责官员进行调整）	□ **信息安全管理者/其他负责官员** □ **IRT 管理者** □ **站点管理者** *（说明哪个站点）* □ **信息系统管理者** □ **报告发起人** □ **报告发起人的管理者/受影响的各级用户管理层** □ **其他** *（例如，服务台、人力资源部、管理层、内部审计）*
	具体说明:

21. 被通知的外部人员/实体

（本细节由负责信息安全并规定所需行动的相关人员填写。相关时可能由组织的信息安全管理者或其他负责官员进行调整）	□ **警察** □ **其他** *（例如，执法机构、外部 IRT）*
	具体说明:

22. 签署

发起人		**评审人**		**评审人**	
数字签名		**数字签名**		**数字签名**	
姓名		**姓名**		**姓名**	
角色		**角色**		**角色**	
日期		**日期**		**日期**	

B.4.3 信息安全脆弱性报告表单示例

<table>
<tr><td colspan="4">信息安全脆弱性报告</td><td>第1页 共1页</td></tr>
<tr><td colspan="2">1. 脆弱性被识别的日期</td><td></td><td>2. 脆弱性编号[4]</td><td></td></tr>
<tr><td colspan="5">3. 报告人详情</td></tr>
<tr><td>3.1 姓名</td><td colspan="2"></td><td>3.2 地址</td><td></td></tr>
<tr><td>3.3 单位</td><td colspan="2"></td><td>3.4 部门</td><td></td></tr>
<tr><td>3.5 电话</td><td colspan="2"></td><td>3.6 电子邮件</td><td></td></tr>
<tr><td colspan="5">4. 信息安全脆弱性描述</td></tr>
<tr><td colspan="2">4.1 脆弱性被报告的日期和时间</td><td colspan="3"></td></tr>
<tr><td colspan="2">4.2 对感知到的信息安全脆弱性的叙述性描述：
• 脆弱性是如何被告知的
• 脆弱性特征——物理、技术等方面
• 如果是技术方面，涉及到的IT/联网组件
• 如果脆弱性被利用，可能受影响的组件/资产
• 如果脆弱性被利用，对业务潜在的不利影响</td><td colspan="3"></td></tr>
<tr><td colspan="5">5. 信息安全脆弱性解决方案</td></tr>
<tr><td colspan="2">5.1 脆弱性是否被确认？</td><td colspan="3">是□ 否□ （适当时勾选）</td></tr>
<tr><td colspan="2">5.2 脆弱性被确认的日期和时间</td><td colspan="3"></td></tr>
<tr><td>5.3 授权人姓名</td><td></td><td rowspan="2">5.4 地址</td><td colspan="2" rowspan="2"></td></tr>
<tr><td>5.5 单位</td><td></td></tr>
<tr><td>5.6 电话</td><td></td><td>5.7 E-mail</td><td colspan="2"></td></tr>
<tr><td colspan="2">5.8 脆弱性是否已被解决？</td><td colspan="3">是□ 否□ （适当时勾选）</td></tr>
<tr><td colspan="2">5.9 对如何解决信息安全脆弱性的叙述性描述，包括日期和解决方案授权人的姓名</td><td colspan="3"></td></tr>
</table>

4) 脆弱性编号宜由组织的IRT管理者分配。

附 录 C
（资料性附录）
信息安全事态和事件分类分级方法示例

C.1 概述

附录C提供了信息安全事态和事件的分类分级方法，相关人员或组织能够以一致的方式记录信息安全事态和事件，从而带来以下好处：

1 促进信息安全事件信息的交换和共享。
2 便于自动化信息安全事件报告和响应。
3 提高信息安全事件处理和管理的效率和效果。
4 利于信息安全事件数据的收集和分析。
5 使用统一准则，标识信息安全事件的严重程度。

这些分类分级方法示例适用于信息安全事态和事件，但不适用于信息安全脆弱性。

相关工作可参见：

RFC 5070事件对象描述交换格式（IODEF）；
RFC 6545实时内部网络防御（RID）；
RFC 6546实时内部网络防御的传输；
Mitre的结构化威胁信息表达式（STIX）；
Mitre的可信自动化指示器信息交换（TAXII）。

C.2 信息安全事件分类

信息安全事件可能是由人为故意或意外的行为引起的，也可能是由技术或物理原因引起的。以下方法将威胁视为分类因素，对信息安全事件进行分类。（关于威胁，参见GB/T 31722—2015附录C典型威胁示例。）表C.1列举了信息安全事件类别

表 C.1 依据威胁的信息安全事件分类

类别	描述	示例
自然灾害事件	超出人类控制的自然灾害造成的信息安全损失。	地震、火山、洪水、暴风、闪电、海啸、崩塌等。
社会动乱事件	社会不稳定造成的信息安全损失。	示威游行、恐怖袭击、战争等。
物理损害事件	故意或意外的物理行动造成的信息安全损失。	火灾、水灾、静电、恶劣环境（诸如污染、灰尘、腐蚀、冻结），设备毁坏、介质毁坏、设备盗窃、介质盗窃、设备丢失、介质丢失、设备篡改、介质篡改等。
基础设施故障事件	支撑信息系统运行的基本系统和服务故障造成的信息安全损失。	电源故障、网络故障、空调故障、供水故障等。

表 C.1（续）

类别	描述	示例
辐射干扰事件	因辐射产生干扰造成的信息安全损失。	电磁辐射、电磁脉冲、电子干扰、电压波动、热辐射等。
技术故障事件	信息系统或相关技术设施故障以及意外的人为因素导致信息系统故障或毁坏造成的信息安全损失。	硬件故障、软件故障、过载（信息系统容量饱和）、维护性破坏等。
恶意软件事件	蓄意制造和传播的恶意程序造成的信息安全损失。将恶意程序插入信息系统以破坏数据、应用程序或操作系统的保密性、完整性或可用性，和（或）影响信息系统的正常运行。	计算机病毒、网络蠕虫、特洛伊木马、僵尸网络、混合攻击、恶意代码内嵌网页、恶意代码宿主站点等。 计算机病毒：在计算机程序中插入的一组计算机指令或者程序代码。不像正常程序，它具有自复制能力，并通常携带可能破坏计算机运行或毁坏数据的功能。 网络蠕虫：与计算机病毒相对应，一种利用信息系统缺陷，通过网络自动传播并复制的恶意程序。 特洛伊木马：一种在信息系统中伪装成良性功能的恶意程序，能够控制信息系统，包括从信息系统中窃取或截获信息。 僵尸网络：由一组网上被攻破的计算机（“僵尸”）组成，受到被称为僵尸网络控制者或牧人的集中控制。僵尸网络是通过感染网络上的大量计算机来蓄意形成的。僵尸网络可被用于投机性网络攻击、信息窃取以及特洛伊木马、网络蠕虫和其他恶意程序的传播。 混合攻击：可以兼有计算机病毒、网络蠕虫、特洛伊木马或僵尸网络等多种组合特征。混合攻击也可以是一系列不同恶意程序组合运行的结果。例如，一个计算机病毒或网络蠕虫在侵入计算机系统后在系统中安装木马程序。 恶意代码内嵌网页：因被嵌入恶意代码而受到污损的网页，该恶意代码在访问该网站的计算机系统中安装恶意软件。 恶意代码宿主站点：诱使网站存储恶意代码，导致目标用户下载的站点。

表 C.1（续）

类别	描述	示例
技术攻击事件	通过网络或其他技术手段对信息系统攻击（或者利用信息系统配置、协议或程序中的脆弱性，或者强力攻击导致信息系统状态异常或对当前系统运行带来潜在危害）造成的信息安全损失。	网络扫描、脆弱性利用、后门利用、登录尝试、干扰、拒绝服务（DoS）等。 网络扫描：利用网络扫描软件获取有关网络配置、端口、服务和现有脆弱性的信息。 脆弱性利用：发掘并利用诸如配置、协议或程序的信息系统缺陷。 后门利用：利用软件和硬件系统设计过程中留下的后门或有害程序。 登录尝试：尝试猜测、破解或暴力破解口令。 干扰：通过技术手段阻碍计算机网络、有线或无线广播电视传输网络或卫星广播电视信号。 拒绝服务（DoS）：因过度使用信息系统和网络资源（诸如CPU、内存、磁盘空间或网络带宽）而引起，进而影响信息系统的正常运行，例如，SYS-a、PING泛滥、电子邮件轰炸。
规则违反事件	故意或意外违规造成的信息安全损失	资源未授权使用、版权违反等。 资源未授权使用：为未授权的目的访问资源，包括营利冒险，例如，使用电子邮件参加非法传销的连锁信。 版权违反：因贩卖或安装未经许可的商业软件或其他受版权保护的材料而引起，例如，盗版软件。
功能损害事件	故意或意外地在安全方面损害信息系统功能造成的信息安全损失	权限滥用、权限伪造、行为抵赖、误操作、人员可用性破坏等 权限滥用：超出范围使用权限。 权限伪造：为了欺骗制造虚假权限。 行为抵赖：否认他/她所做的事情。 误操作：不正确或无意地执行操作。 人员可用性破坏：由人员缺失或缺席而造成。

表 C.1（续）

类别	描述	示例
信息损害事件	故意或无意损害信息安全（诸如保密性、完整性、可用性等）造成的信息安全损失	拦截、间谍、窃听、泄露、伪装、社会工程、网络钓鱼、数据窃取、数据丢失、数据篡改、数据错误、数据流分析、位置检测等。 拦截：在数据到达目标接收者之前捕获数据。 间谍：秘密收集和报告有关其他组织活动的信息。 窃听：在对方不知情的情况下偷听其谈话。 泄露：将敏感信息公之于众。 伪装：一个实体假装成另外一个实体。 社会工程：通过心理操纵人（以非技术方式）来泄露信息或执行行动，例如，谎言、诡计、贿赂或威胁。 网络钓鱼：利用欺诈性计算机网络技术诱使用户泄露重要信息，诸如通过欺骗性电子邮件获取用户的银行帐户详细信息和口令。 数据窃取：偷窃数据。 数据篡改未经授权接触或修改数据。 数据错误：输入或处理数据时发生错误。 位置检测：检测敏感信息或系统的位置。
有害内容事件	通过信息网络传播危害国家安全、社会稳定和（或）公共安全和利益的不良内容造成的信息安全损失。	非法内容、恐慌内容、恶意内容、滥用内容等。 非法内容：公布的内容违反国家或国际宪法、法律和法规，例如，儿童色情、暴力宣扬、伪造、欺诈。 恐慌内容：对互联网上的敏感问题进行恶意耸人听闻的讨论或评论，导致诸如社会动荡或恐慌。 恶意内容：传播恶意攻击社会或人的内容，例如，恶作剧、骚扰。 滥用内容：广播未经接收者准许的内容，例如，垃圾邮件。
其他事件	未分类到在上述类别中的事件。	

C.3 信息安全事件分级

下面介绍两个信息安全事件分级方法示例。

需要强调的是，这些仅是举例，它们可能为适合业务需要而被修改。此外，还有其他分级标准，诸如通用脆弱性评价体系（CVSS）。

C.3.1 方法示例1

C.3.1.1 分级因素

C.3.1.1.1 概述

本方法通过考虑以下三方面因素对信息安全事件进行分级：

a) 信息系统重要程度；
b) 业务损失；
c) 社会影响。

C.3.1.1.2 信息系统重要程度

受信息安全事件影响的信息系统的重要程度由信息系统所支撑运行的组织业务的重要程度决定。这种重要程度以关联到国家安全、社会秩序、经济发展和公众利益以及业务对信息系统的依赖程度来表达。信息系统重要程度划分为三个级别：特别重要的信息系统、重要的信息系统和一般的信息系统。

C.3.1.1.3 业务损失

信息安全事件导致的组织的业务损失由因信息系统的硬件/软件、功能和数据的损坏导致业务中断影响的严重程度决定，其大小可取决于恢复业务正常运行和消除信息安全事件负面影响所需代价，包括利益和（或）机会的丧失。业务损失划分为四个级别：特别严重的业务损失、严重的业务损失、较大的业务损失和较小的业务损失，说明如下：

a) 特别严重的业务损失：业务大面积瘫痪，导致业务能力丧失，和（或）关键业务数据的保密性、完整性、可用性遭到特别严重破坏，恢复业务正常运行和消除负面影响所需代价十分巨大，对于事发组织是不可承受的。
b) 严重的业务损失：造成业务运行长时间中断或局部业务瘫痪，导致业务能力受到极大影响，和（或）关键业务数据的保密性、完整性、可用性遭到严重破坏，恢复业务正常运行和消除负面影响所需代价巨大，但对于事发组织是可承受的。
c) 较大的业务损失：业务运行中断，导致业务能力受到较大影响，和（或）重要业务数据的保密性、完整性、可用性遭到较大破坏，恢复业务正常运行和消除负面影响所需代价较大，但对于事发组织是完全可以承受的。
d) 较小的业务损失：业务短暂中断，导致业务能力受到一些影响，和（或）重要业务数据的保密性、完整性、可用性遭到较小影响，恢复业务正常运行和消除负面影响所需代价较小。

C.3.1.1.4 社会影响

信息安全事件造成的社会影响由其对国家安全、社会秩序、经济发展和公众利益所造成影响的范围和程度决定。社会影响划分为四个级别：特别重大的社会影响、重大的社会影响、较大的社会影响和较小的社会影响，说明如下：

a) 特别重大的社会影响：波及到一个或多个省的大部分地区，极大威胁国家安全，引起社会动荡，对经济发展有极其恶劣的负面影响，和（或）严重损害公众利益。
b) 重大的社会影响：波及到一个或多个城市的大部分地区，威胁到国家安全，引起社会恐慌，对经济发展有重大的负面影响，和（或）损害到公众利益；
c) 较大的社会影响：波及到一个或多个城市的部分地区，有限地威胁到国家安全，某种程度地扰乱社会秩序，对经济发展有一定的负面影响，和（或）影响到公众利益；

d) 较小的社会影响：波及到一个城市的部分地区，对国家安全、社会秩序、经济发展和公众利益基本没有影响，但对个人、法人或其他组织的利益会造成损害。

C.3.1.2 分级

C.3.1.2.1 概述

按照以上分级因素，本方法将信息安全事件分为四级：

a) 特别重大（四级）

b) 重大（三级）

c) 较大（二级）

d) 一般（一级）

C.3.1.2.2 特别重大（四级）

特别重大的事件是指：

——发生在特别重要的信息系统上，和

——导致特别重大的业务损失，或

——造成特别重大的社会影响。

C.3.1.2.3 重大（三级）

重大的事件是指，

——发生在特别重要或重要的信息系统上，和

——导致重大的业务损失，或

——造成重大的社会影响。

C.3.1.2.4 较大（二级）

较大的事件是指，

——发生在重要或一般的信息系统上，和

——导致较大的业务损失，或

——造成较大的社会影响。

C.3.1.2.5 一般（一级）

一般的事件是指，

——发生在一般的信息系统上，和

——导致较小的业务损失或没有业务损失，或

——造成较小的社会影响或没有造成社会影响。

C.3.1.3 事件类别和严重级别

信息安全事件类别和严重级别往往是关联的。一个信息安全事件类别可能具有不同的严重级别，这不仅取决于业务，还取决于信息安全事件的性质，诸如：

- 故意性
- 目标性
- 时机
- 量级

表C.2提供了具有不同严重级别的信息安全事件类别的某些示例。

表 C.2　事件类别与严重级别示例

严重级别 事件类别	一般	较大	重大	特别重大
技术攻击	尝试失败	单次一般 （损害用户）	多次 （损害用户） 单次重大 （损害应用程序、特权访问）	大量 （损害应用程度、特权访问）
技术攻击		骚扰 （伤及表面）	扰乱 （全面影响）	可用性 （服务停止）
恶意软件	单次已知 （被抗病毒保护发现并拦截）	单次未知	多次感染 严重感染	大量感染

C.3.2　方法示例2

C.3.2.1　概述

本方法给出了信息安全事件负面后果评估指南示例，每项指南使用1（低）到10（高）尺度来对信息安全事件进行分级。在实践中，也可以使用其他尺度，如1到5；组织宜采取最适合起环境的尺度。

在阅读下列指南之前，宜注意以下要点说明：

——在下面列出的某些指南示例中，某些条目被标注为“无”。这是因为每项指南都被制定成以逐级上升的1至10尺度来统一表示C.3.2.2至C.3.2.7所示的所有六种类型的负面后果。然而，对于某些类型的某些级别（1至10尺度），被认为与相邻较低级别相比没有足够的差异，这时将其标注为“无”。类似地，对于某些类型的较高级别，如果认为没有比所示的最高条目有更为严重的后果，则将其标注为“无”。由此可见，删除“无”对应行来缩减尺度，在逻辑上是不正确的。

因此，当从以下方面考虑信息安全事件对组织业务的负面后果时，可把下面指南最为一套示例来使用：

——未授权披露信息；

——未授权更改信息；

——抵赖信息；

——信息和（或）服务不可用；

——信息和（或）服务遭受破坏。

首先是考虑以下哪种类型是与事件相关的。对于那些被认为是相关的，宜使用类型指南来确定对组织业务运行的实际负面影响，并以“数值”形式输入到信息安全事件报告表单中。

C.3.2.2　业务运营的财务损失/中断

此类信息的未授权披露和修改、抵赖以及不可用和遭受破坏的后果，很可能是财务损失，例如，由于没有或延迟的行为导致股价下跌、欺诈或违约。同样，特别是任何信息的不可用或遭受破坏的后果可能会对中断业务运营。要纠正和（或）从这种事件中恢复，需要花费时间和精力。在某些情况下这很重

要，宜予以考虑。为了取得一个共同衡量尺度，恢复时间宜以人员时间为单位来计算并转换为财务成本。这种成本宜参考组织内适当等级/级别的正常人月成本来计算。以使用以下指南：

1 导致的财务损失/成本为x_1或更低。
2 导致的财务损失/成本在x_1+1与x_2之间。
3 导致的财务损失/成本在x2+1与x3之间。
4 导致的财务损失/成本在x3+1与x4之间。
5 导致的财务损失/成本在x4+1与x5之间。
6 导致的财务损失/成本在x5+1与x6之间。
7 导致的财务损失/成本在x6+1与x7之间。
8 导致的财务损失/成本在x7+1与x8之间。
9 导致的财务损失/成本高于x8。
10 组织业务中断。

其中，x_i (i = 1, 2, ..., 8)表示财务损失/成本的8个等级/级别（由组织在其语境下决定）。

C.3.2.3 商业和经济利益

商业和经济信息需要得到保护，并通过考虑其对竞争对手的价值或受到危及可能对商业利益产生的影响来评估其价值。宜使用以下指南。

1 对竞争者有利益，但没有商业价值。
2 对竞争者有利益，其价值为y_1或更少（营业额）。
3 对竞争者有价值，其价值在y_1+1和y_2之间（营业额），或者导致财务损失，或者收入潜力损失，或者给个人或组织带来不正当收入或优势；或者违反对第三方信息的保密承诺。
4 对竞争对手有价值，价值在y_2+1和y_3之间（营业额）。
5 对竞争对手有价值，价值在y_3+1和y_4之间（营业额）。
6 对竞争对手有价值，价值高于y_4+1（营业额）。
7 无[5)]。
8 无。
9 可能极大破坏组织的商业利益，或者极大削弱组织的财务生存能力。
10 无。

其中，y_i (i = 1, 2, ..., 4)以营业额的4个等级/级别（由组织在其语境下决定）表示对于竞争者的价值。

C.3.2.4 个人信息

当持有和处理个人信息时，保护信息免受未授权披露在道德和伦理上是正确的，有时也被法律要求。未授权披露轻则可能导致尴尬，重则可能导致法律制裁，例如，数据保护法。同样地，需要保持个人信息的正确性，因为未授权修改导致的不正确信息可能造成与未授权披露类似的后果。同样重要的是，不得使个人信息不可用供或遭受破坏，因为这可能导致不正确决定或在所要求时间内无法采取行动，造成与未授权披露或修改类似的后果。宜使用以下指南。

1 给个人带来轻微痛苦或担忧（愤怒、挫折、失望），但没有违背法律法规要求。
2 给个人带来痛苦或担忧（愤怒、挫折、失望），但没有违背法律法规要求。
3 违背信息保护相关的法律法规要求、道德要求或公共意识，给个人带来轻微尴尬。
4 违背信息保护相关的法律法规要求、道德要求或公共意识，给个人带来显著尴尬或给群体带来轻微尴尬。

5) “无”表示该影响级别无对应项。

5 违背信息保护相关的法律法规要求、道德要求或公共意识，给个人带来严重尴尬。
6 违背信息保护相关的法律法规要求、道德要求或公共意识，给群体带来严重尴尬。
7 无。
8 无。
9 无。
10 无。

C.3.2.5 法律法规义务

组织持有和处理数据需遵守法律法规义务。有意或无意地不履行这种义务，可能导致对组织内相关人员采取法律诉讼或行政处罚的行动。这些行动可能导致罚款和（或）判刑入狱。宜使用以下指南。

1 无。
2 无。
3 执法通知、民事诉讼或刑事犯罪，导致z_1或更低的财务损失/罚款为。
4 执法通知、民事诉讼或刑事犯罪，导致z_1+1和z_2之间的财务损失/罚款。
5 执法通知、民事诉讼或刑事犯罪，导致z_2+1和z_3之间的财务损失/罚款，或最多2年监禁。
6 执法通知、民事诉讼或刑事犯罪，导致z_3+1和z_4之间的财务损失/罚款，或2年以上至10年监禁。
7 执法通知、民事诉讼或刑事犯罪，导致无法限制的财务损失/罚款，或10年以上监禁。
8 无。
9 无。
10 无。

C.3.2.6 管理和业务运营

信息受损可损害组织的有效运行。例如，与策略变更相关的信息如果泄露，可能会引起公众反应，导致该策略无法实施。与财务或计算机软件有关的信息的修改、抵赖或不可用，也有可能对组织运营带来严重后果。此外，抵赖承诺可能会对组织业务带来不利后果。宜使用以下指南。

1 组织的某个部分低效运营。
2 无。
3 消弱组织及其运营的正常管理。
4 无。
5 阻碍组织策略的有效制定或执行。
6 使组织在与其他组织进行商业或策略谈判时处于不利地位。
7 严重阻碍组织重大策略的制定或执行，或者关停或严重扰乱重大运营。
8 无。
9 无。
10 无。

C.3.2.7 信誉损失

信息的未授权泄露或修改、抵赖或确实不可用，可能导致组织信誉受损，从而带来其声誉损害、信用丧失和其他不良后果。宜使用以下指南。

1 无。
2 导致组织内的局部尴尬。
3 负面影响与股东、客户、供应商、员工、第三方用户、监管机构、政府部门、其他组织或公众的关系，导致本地/区域的负面宣传。

4 无。

5 负面影响与股东、客户、供应商、员工、第三方用户、监管机构、政府部门、其他组织或公众的关系，导致对国家的某种负面宣传。

6 无。

7 实质性影响与股东、客户、供应商、员工、第三方用户、监管机构、政府部门、其他组织或公众的关系，导致广泛的负面宣传。

8 无。

9 无。

10 无。

参 考 文 献

[1] ISO 8601, Data elements and interchange formats — Information interchange — Representation of dates and times

[2] GB/T 22080—2016 信息技术 安全技术 信息安全管理体系 要求（ISO/IEC 27001:2013，IDT）

[3] GB/T 22081—2016 信息技术 安全技术 信息安全控制实践指南（ISO/IEC 27002:2013，IDT）

[4] GB/T 31722—2015 信息技术 安全技术 信息安全风险管理（ISO/IEC 27005:2008，IDT）

[5] ISO/IEC 27031, Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity

[6] ISO/IEC 27033-1, Information technology — Security techniques — Network security — Part 1: Overview and concepts

[7] ISO/IEC 27033-2, Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security

[8] ISO/IEC 27033-3, Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues

[9] ISO/IEC 27033-4, Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways

[10] ISO/IEC 27039, Information technology — Security techniques — Selection, deployment and operations of intrusion detection systems (IDPS)

[11] Internet Engineering Task Force (IETF) Site Security Handbook. http://www.ietf.org/rfc/rfc2196.txt?number=2196

[12] Internet Engineering Task Force (IETF) RFC 5070, The Incident Object Description Exchange Format, http://www.ietf.org/rfc/rfc5070.txt?number=5070

[13] Mitre Corporation. STIX, Structured Threat Information eXpression, https://stix.mitre.org/

[14] Mitre Corporation. Trusted Automated eXchange of Indicator Information. http://taxii.mitre.org/

[15] Software Engineering Institute at Carnegie Mellon. “CERT Coordination Centre”, An Introduction to the Mission Risk Diagnostic for Incident Management Capabilities, http://resources.sei.cmu.edu/asset_files/technicalnote/2014_004_001_91462.pdf

[16] NIST SP 800-61, Computer Security Incident Handling Guide (2012) http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf