GB/Z 20985-2007

信 息 技 术 安 全 技 术　信 息 安 全 事 件 管 理 指 南

Information technology-Security techniques-Information security incident management guide

自　2007-6-14　起执行

目 次

前言
引言
1 范围
2 规范性引用文件
3 术语和定义
4 缩略语
5 背景
5.1 目标
5.2 过程
6 信息安全事件管理方案的益处及需要应对的关键问题
6.1 信息安全事件管理方案的益处
6.2 关键问题
7 规划和准备
7.1 概述
7.2 信息安全事件管理策略
7.3 信息安全事件管理方案
7.4 信息安全和风险管理策略
7.5 ISIRT 的建立
7.6 技术和其他支持
7.7 意识和培训
8 使用
8.1 概述
8.2 关键过程的概述
8.3 发现和报告
8.4 事态/事件评估和决策
8.5 响应
9 评审
9.1 概述
9.2 进一步的法律取证分析
9.3 经验教训
9.4 确定安全改进
9.5 确定方案改进
10 改进
10.1 概述

10.2 安全风险分析和管理改进
10.3 改善安全状况
10.4 改进方案
10.5 其他改进
附录 A(资料性附录)信息安全事态和事件报告单示例
附录 B(资料性附录)信息安全事件评估要点指南示例
附录 C(资料性附录) 本指导性技术文件与 ISO/IEC TR 18044：2004 的技术性差异及其原因
参考文献

前 言

本指导性技术文件修改采用 ISO/IEC TR18044：2004《信息技术 安全技术 信息安全事件管理指南》。

考虑到我国国家标准的编写要求，以及与其他信息安全事件相关标准技术内容的协调性，本指导性技术文件在采用国际标准时，对部分内容进行了修改。其中，技术性差异用垂直单线标识在它们所涉及的条款的页边空白处。在附录 C 中给出了技术性差异及其原因的一览表以供参考。

本指导性技术文件由全国信息安全标准化技术委员会提出并归口。

本指导性技术文件起草单位：中国电子技术标准化研究所、北京同方信息安全股份有限公司、北京知识安全工程中心，北京邮电大学。

本指导性技术文件主要起草人：上官晓丽、闵京华、赵战生、王连强、徐国爱。

前言

目前，没有任何一种具有代表性的信息安全策略或防护措施，能够对信息、信息系统、服务或网络提供绝对的保护。即使采取了防护措施，仍可能存在残留的弱点，使得信息安全防护变得无效，从而导致信息安全事件发生，并对组织的业务运行直接或间接产生负面影响。此外，以前未被认识到的威胁也可能会发生。组织如果对这些事件没有作好充分的应对准备，其任何实际响应措施的效率都会大打折扣，甚至还可能加大潜在的业务负面影响的程度。因此，对于任何一个重视信息安全的组织来说，采用一种结构严谨、计划周全的方法来处理以下工作十分必要：

•发现、报告和评估信息安全事件；

•对信息安全事件做出响应，包括启动适当的事件防护措施来预防和降低事件影响，以及从事件影响中恢复(例如，在支持和业务连续性规划方面)；

•从信息安全事件中吸取经验教训，制定预防措施，并且随着时间的变化，不断改进整个的信息安全事件管理方法。

信息技术安全技术 信息安全事件管理指南

1 范围

本指导性技术文件描述了信息安全事件的管理过程。提供了规划和制定信息安全事件管理策略和方案的指南。给出了管理信息安全事件和开展后续工作的相关过程和规程。

本指导性技术文件可用于指导信息安全管理者，信息系统、服务和网络管理者对信息安全事件的管理。

2 规范性引用文件

下列文件中的条款通过本指导性技术文件的引用而成为本指导性技术文件的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本指导性技术文件，然而，鼓励根据本指导性技术文件达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本指导性技术文件。

GB/T19716-2005 信息技术 信息安全管理实用规则(ISO/IEC：17799：2000，MOD)

GB/Z20986-2007 信息安全技术 信息安全事件分类分级指南

ISO/IEC 13335-1：2004 信息技术 安全技术 信息和通信技术安全管理 第1部分：信息和通信技术安全管理的概念和模型

3 术语和定义

GB/T19716-2005、ISO/IEC 13335-1:2004中确立的以及下列术语和定义适用于本指导性技术文件。

3.1

业务连续性规划 business continuity planning

这样的一个过程.即当有任何意外或有害事件发生，且对基本业务功能和支持要素的连续性造成负面影响时，确保运行的恢复得到保障。该过程还应确保恢复工作按指定优先级、在规定的时间期限内完成，且随后将所有业务功能及支持要素恢复到正常状态。

这一过程的关键要素必须确保具有必要的计划和设施，且经过测试，它们包含信息、业务过程、信息系统和服务、语音和数据通信、人员和物理设施等。

3.2

信息安全事态 information security event

被识别的一种系统、服务或网络状态的发生，表明一次可能的信息安全策略违规或某些防护措施失效，或者一种可能与安全相关但以前不为人知的一种情况。

3.3

信息安全事件 information security incident

由单个或一系列意外或有害的信息安全事态所组成，极有可能危害业务运行和威胁信息安全。

3.4

信息安全事件响应组(ISIRT)Information Security Incident Response Team

由组织中具备适当技能且可信的成员组成的一个小组，负责处理与信息安全事件相关的全部工作。有时，小组可能会有外部专家加入，例如来自一个公认的计算机事件响应组或计算机应急响应组(CERT)的专家。

4 缩略语

CERT 计算机应急响应组(computer Emergency Response Team)

ISIRT 信息安全事件响应组(Information Security Incident Response Team)

5 背景

5.1 目标

作为任何组织整体信息安全战略的一个关键部分，采用一种结构严谨、计划周全的方法来进行信息安全事件的管理至关重要。

这一方法的目标旨在确保：

•信息安全事态可以被发现并得到有效处理，尤其是确定是否需要将事态归类为信息安全事件[1)]；

1) 应该指出的是，尽管信息安全事态可能是意外或故意违反信息安全防护措施的企图

的结果，但在多数情况下，信息安全事态本身并不意味着破坏安全的企图真正获得了成功，因此也并不一定会对保密性、完整性和/或可用性产生影响，也就是说，并非所有信息安全事态都会被归类为信息安全事件。

•对已确定的信息安全事件进行评估，并以最恰当和最有效的方式做出响应；

•作为事件响应的一部分，通过恰当的防护措施——可能的话。结合业务连续性计划的相关要素——将信息安全事件对组织及其业务运行的负面影响降至最小；

•及时总结信息安全事件及其臂理的经验教训。这将增加预防将来信息安全事件发生的机会，改进信息安全防护措施的实施和使用，同时全面改进信息安全事件管理方案。

5.2 过程

为了实现 5.1 所述的目标，信息安全事件管理由 4 个不同的过程组成：

•规划和准备(Plan and Prepare)；

•使用(Use)；

•评审(Review)；

•改进(Improve)。

(注：这些过程与 ISO/IEC 27001：2005 中的“计划(Plan)一实施(Do)—检查(Check)—处置(Act)”过程类似。)

图 1 显示了上述过程的主要活动。

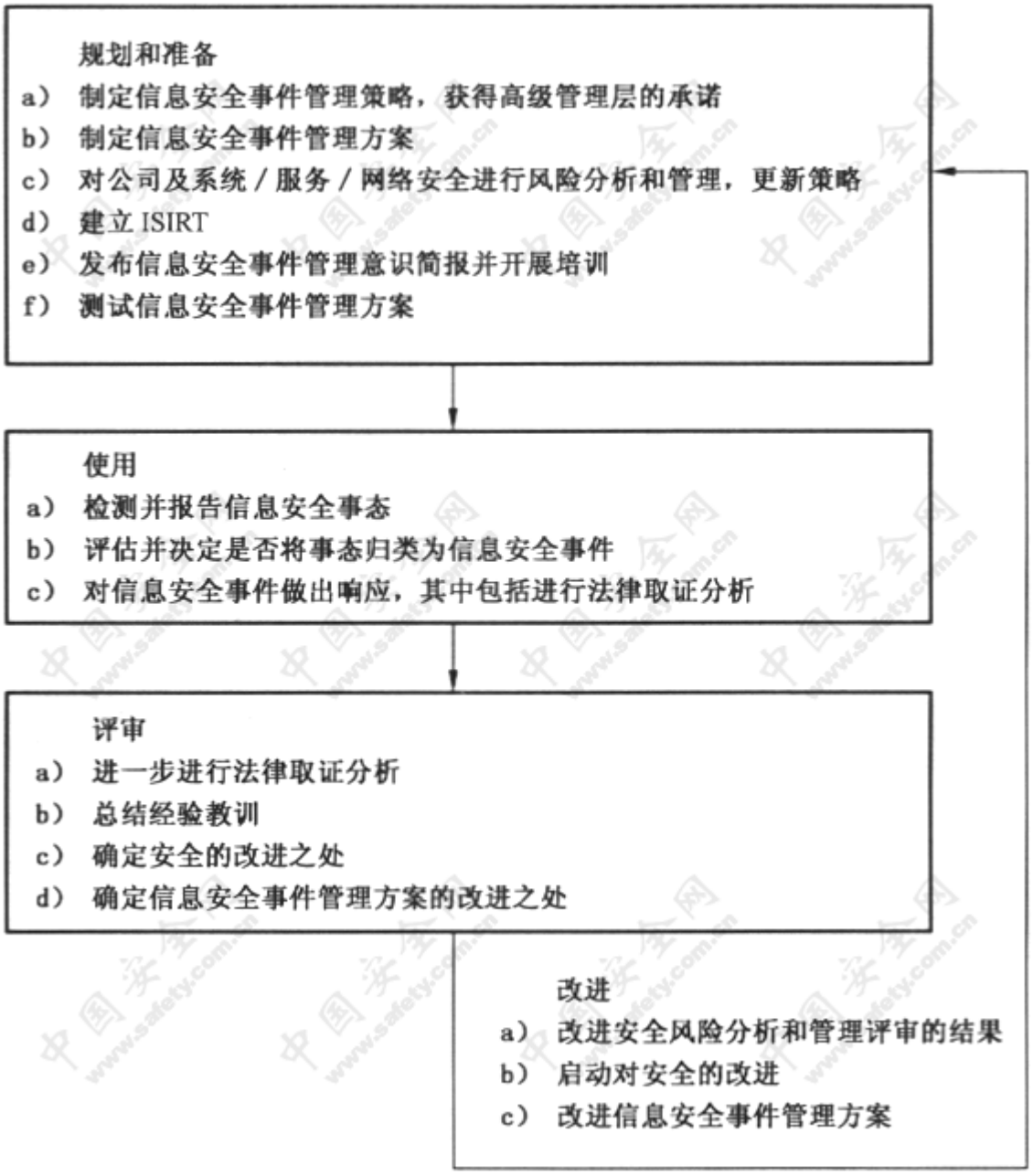

图1 信息安全事件管理过程

5.2.1 规划和准备

有效的信息安全事件管理需要适当的规划和准备。为使信息安全事件的响应有效，下列措施是必要的：

a)制定信息安全事件管理策略并使其成为文件，获得所有关键利益相关人，尤其是高级管理层对策略的可视化承诺；

b)制定信息安全事件管理方案并使其全部成为文件，用以支持信息安全事件管理策略。用于发现、报告、评估和响应信息安全事件的表单、规程和支持工具，以及事件严重性衡量尺度的细节[2)]，均应包括在方案文件中(应指出，在有些组织中，方案即为信息安全事件响应计划)；

2)应该建立“定级”事件严重性的衡量尺度。例如，可基于对组织业务运行的实际或预

期负面影响的程度，分为“严重”和“轻微”两个级别。

c)更新所有层面的信息安全和风险管理策略，即，全组织范围的，以及针对每个系统、服务和网络的信息安全和风险管理策略，均应根据信息安全事件管理方案进行更新；

d)确定一个适当的信息安全事件管理的组织结构，即信息安全事件响应组(ISIRT)，给那些可调用的、能够对所有已知的信息安全事件类型作出充分响应的人员指派明确的角色和责任。在大多数组织中，ISIRT 可以是一个虚拟小组，是由一名高级管理人员领导的、得到各类特定主题专业人员支持的小组，例如，在处理恶意代码攻击时，根据相关事件类型召集相关的专业人员；

e)通过简报和/或其他机制使所有的组织成员了解信息安全事件管理方案、方案能带来哪些益处以及如何报告信息安全事态。应该对管理信息安全事件管理方案的负责人员、判断信息安全事态是否为事件的决策者，以及参与事件调查的人员进行适当培训；

f)全面测试信息安全事件管理方案。

第 7 章中对规划和准备阶段作了进一步描述。

5.2.2 使用

下列过程是使用信息安全事件管理方案的必要过程：

a)发现和报告所发生的信息安全事态(人为或自动方式)；

b)收集与信息安全事态相关的信息，通过评估这些信息确定哪些事态应归类为信息安全事件；

c)对信息安全事件作出响应：

1)立刻、实时或接近实时；

2)如果信息安全事件在控制之下，按要求在相对缓和的时间内采取行动(例如，全面开展灾难恢复工作)；

3)如果信息安全事件不在控制之下，发起“危机求助”行动(如召唤消防队/部门或者启动业务连续性计划)；

4)将信息安全事件及任何相关的细节传达给内部和外部人员和/或组织(其中可能包括按要求上报以便进一步评估和/或决定)；

5)进行法律取证分析；

6)正确记录所有行动和决定以备进一步分析之用；

7)结束对已经解决事件的处理。

第 8 章中对使用阶段作了进一步描述。

5.2.3 评审

在信息安全事件已经解决或结束后，进行以下评审活动是必要的：

a)按要求进行进一步法律取证分析；

b)总结信息安全事件中的经验教训；

c)作为从一次或多次信息安全事件中吸取经验教训的结果，确定信息安全防护措施实施方面的改进；

d)作为从信息安全事件管理方案质量保证评审(例如根据对过程、规程、报告单和/或组织结构所作的评审)中吸取经验教训的结果，确定对整个信息安全事件管理方案的改进。

第 9 章中对评审阶段作了进一步描述。

5.2.4 改进

应该强调的是，信息安全事件管理过程虽然可以反复实施，但随着时间的推移，有许多信息安全要素需要经常改进。这些需要改进的地方应该根据对信息安全事件数据、事件响应

以及一段时间以来的发展趋势所作评审的基础上提出。其中包括：

a)修订组织现有的信息安全风险分析和管理评审结果；

b)改进信息安全事件管理方案及其相关文档；

c)启动安全的改进，可能包括新的和/或经过更新的信息安全防护措施的实施。

第 10 章对改进阶段作了进一步描述。

6 信息安全事件管理方案的益处及需要应对的关键同题

本章提供了以下信息：

• 一个有效的信息安全事件管理方案可带来的益处；

• 使组织高级管理层以及那些提交和接收方案反馈意见的人员信服所必须应对的关键问题。

6.1 信息安全事件管理方案的益处

任何以结构严谨的方法进行信息安全事件管理的组织均能收效匪浅。一个结构严谨、计划周全的信息安全事件管理方案带来的益处，可分为以下几类：

a)提高安全保障水平；

b)降低对业务的负面影响，例如由信息安全事件所导致的破坏和经济损失；

c)强化着重预防信息安全事件；

d)强化调查的优先顺序和证据；

e)有利于预算和资源合理利用；

f)改进风险分析和管理评审结果的更新；

g)增强信息安全意识和提供培训计划材料；

h)为信息安全策略及相关文件的评审提供信息。

下面逐一介绍这些主题。

6.1.1 提高安全保障水平

一个结构化的发现、报告、评估和管理信息安全事态和事件的过程，能使组织迅速确定任何信息安全事态或事件并对其做出响应，从而通过帮助快速确定并实施前后一致的解决方案和提供预防将来类似的信息安全事件再次发生的方式，来提高整体的安全保障水平。

6.1.2 降低对业务的负面影响

结构化的信息安全事件管理方法有助于降低对业务潜在的负面影响的级别。这些影响包括当前的经济损失，及长期的声誉和信誉损失。

6.1.3 强调以事件预防为主

采用结构化的信息安全事件管理有助于在组织内创造一个以事件预防为重点的氛围。对与事件相关的数据进行分析，能够确定事件的模式和趋势，从而便于更准确地对事件重点预防，并确定预防事件发生的适当措施。

6.1.4 强化调查的优先顺序和证据

一个结构化的信息安全事件管理方法为信息安全事件调查时优先级的确定提供了可靠的基础。

如果没有清晰的调查规程，调查工作便会有根据临时反应进行的风险，在事件发生时才响应，只按照相关管理层的“最大声音”行事。这样会阻碍调查工作进入真正需要的方面和遵循理想的优先顺序进行。

清晰的事件调查规程有助于确保数据的收集和处理是证据充分的、法律所接受的。如果随后要进行法律起诉或采取内部处罚措施的话，这些便是重点的考虑事项。然而应该认识到的是，从信息安全事件中恢复所必须采取的措施，可能危害这种收集到的证据的完整性。

6.1.5 预算和资源

定义明确且结构化的信息安全事件管理，有助于正确判断和简化所涉及组织部门内的预算和资源分配。此外，信息安全事件管理方案自身的益处还有：

•可用技术不太熟练的员工来识别和过滤虚假警报；

•可为技术熟练员工的工作提供更好的指导；

•可将技术熟练员工仅用于那些需要其技能的过程以及过程的阶段中。

此外，结构化的信息安全事件管理还包括“时间戳”，从而有可能“定量”评估组织对安全事件的处理。例如，它可以提供信息说明解决处于不同优先级和不同平台上的事件需要多长时间。如果信息安全事件管理的过程存在瓶颈，也应该是可识别的。

6.1.6 信息安全风险分析和管理

结构化的信息安全事件管理方法有助于：

•可为识别和确定各种威胁类型及相关脆弱性的特征，收集质量更好的数据；

•提供有关已识别的威胁类型发生频率的数据。

从信息安全事件对业务运行的负面影响中获取的数据，对于业务影响分析十分有用。识别各种威胁类型发生频率所获取的数据，对威胁评估的质量有很大帮助。同样，有关脆弱性的数据对保证将来脆弱性评估的质量帮助很大。

这方面的数据将极大地改进信息安全风险分析和管理层评审结果。

6.1.7 信息安全意识

结构化的信息安全事件管理可以为信息安全意识教育计划提供重要信息。这些重要信息将用实例表明信息安全事件确实发生在组织中，而并非“只是发生在别人身上”。它还可能表明，迅速提供有关解决方案的信息会带来哪些益处。此外，这种意识有助于减少员工遭遇信息安全事件时的错误或惊慌/混乱。

6.1.8 为信息安全策略评审提供信息

信息安全事件管理方案所提供的数据可以为信息安全策略(以及其他相关信息安全文件)的有效性评审以及随后的改进提供有价值的信息。这可应用于适合整个组织以及单个系统、服务和网络的策略和其他文件。

6.2 关键问题

在信息安全事件管理方法中得到的反馈，有助于确保相关人员始终将关注点集中在组织的系统、服务和网络面临的实际风险上。这一重要的反馈通过在事件发生时的专门处理是不能有效得到的。只有通过使用一个结构化的、设计明确的信息安全事件处理管理方案，且该方案采用一个适用于组织所有部分的通用框架，才能更有效得到。这样的框架应该能使该方案持续产生更加全面的结果，从而可以在信息安全事件发生之前迅速识别信息安全事件可能出现的情况——有时，这也被称作“警报”。

信息安全事件管理方案的管理和审核应该能为促进组织员工的广泛参与，以及消除各方对保证匿名性、安全和有用结果的可用性等方面的担忧，奠定必要的信任基础。例如，管理和运行人员必须对“警报”能够给出及时、相关’精确、简洁和完整的信息充满信心。

组织应避免在实施信息安全事件管理方案的过程中可能遇到的问题，如缺少有用结果和对隐私相关问题的关注等。必须使利益相关人相信，组织已经采取措施预防这些问题的发生。

因此，为实现一个良好的信息安全事件管理方案，必须将一些关键问题阐述清楚，这些问题包括：

a)管理层的承诺；

b)安全意识；

c)法律法规；

d)运行效率和质量；

e)匿名性；

f)保密性；

g)可信运行；

h)系统化分类。

下面将逐一讨论这些问题。

6.2.1 管理层的承诺

要使整个组织接受一个结构化的信息安全事件管理方法，确保得到管理层的持续承诺，这一点至关重要。组织员工必须能够认识到事件的发生，并且知道应该采取什么行动，甚至了解这种事件管理方法可以给组织带来的益处。然而，除非得到管理层的支持，否则这一切都不会出现。必须将这一理念灌输给管理层，以使组织对事件响应能力的资源方面和维护工作做出承诺。

6.2.2 安全意识

对于组织接受一个结构化的信息安全事件管理方法而言，另一个重要的问题是安全意识。即使要求用户参与信息安全事件管理，但是用户如果不了解自己以及自己所在部门会从该结构化的信息安全事件管理中得到哪些益处，他们的参与很可能不会有太好效果。

任何信息安全事件管理方案都应该具有意识计划定义文件，并在文件中规定以下细节：

a)组织及其员工可以从结构化的信息安全事件管理中得到的益处；

b)信息安全事态/事件数据库中的事件信息及其输出；

c)提高员工安全意识计划的战略和机制；根据组织的具体情况，它们可能是独立的，或者是更广泛的信息安全意识教育计划的一部分。

6.2.3 法律法规

以下与信息安全事件管理相关的法律法规问题应在信息安全事件管理策略和相关方案中进行阐述。

a)提供适当的数据保护和个人信息隐私。一个组织结构化的信息安全事件管理，必须考虑到满足我国在数据保护和个人信息隐私方面的相关政策、法律法规的要求，提供适当的保护，其中可能包括：

1)只要现实、可行，保证可以访问个人数据的人员本身不认识被调查者；

2)需要访问个人数据的人员在被授权访问之前，应签订不泄露协议；

3)信息应被仅用于获取它的特定目的，如信息安全事件调查。

b)适当保留记录。按国家相关规定，组织需要保留适当的活动记录，用于年度审计，或生成执法所用的档案(如可能涉及严重犯罪或渗透敏感政府系统的任何案件)。

c)有防护措施以确保合同责任的履行。在要求提供信息安全事件管理服务的合同中，例如，合同中对事件响应时间提出了要求，组织应确保提供适当的信息安全，以便在任何情况下，这些责任都能得到履行。(与之相应.如果组织与某外部方签订了支持合同(参见 7.5.4)，如 CERT，那么，应该确保包括事件响应时间在内的所有要求均包含在与该外部方签订的合同中。)

d)处理与策略和规程相关的法律问题。应检查与信息安全事件管理方案相关的策略和规程是否存在法律法规问题，例如，是否有对事件责任人采取纪律处罚和/或法律行动的有关声明。

e)检查免责声明的法律有效性。对于有关信息事件管理组以及任何外部支持人员的行动

的所有免责声明，均应检查其法律有效性。

f)与外部支持人员的合同涵盖要求的各个方面。对于与任何外部支持人员(如来自某CERT)签订的合同，均应就免责、不泄露、服务可用性、错误建议的后果等要求进行全面检查。

g)强制性不泄露协议。必要时，应要求信息安全事件管理组的成员签订不泄露协议。

h)阐明执法要求。根据相关执法机构的要求，对需要提供的信息安全事件管理方案相关的问题，进行明确说明。如，可能需要阐明如何按法律的最低要求记录事件以及事件文件应保存多长时间。

i)明确责任。必须将潜在的责任问题以及应该到位的相关防护措施阐述清楚。以下是可能与责任问题相关的几个例子：

1)事件可能对另一组织造成影响(如泄露了共享信息)，而该组织却没有及时得到通知，从而对其产生负面影响；

2)发现产品的新脆弱性后没有通知供应商，随后发生与该脆弱性相关的重大事件，给一个或多个其他组织造成严重影响；

3)按照国家相关法律法规，对于像严重犯罪，或者敏感的政府系统或部分关键国家基础设施被渗透之类案件，组织没有接要求向执法机关报告或生成档案文件；

4)信息的泄露表明某个人或组织与攻击相关联。这可能会危害所涉及的个人或组织的声誉和业务；

5)信息的泄露表明可能是软件的某个环节出了问题，但随后发现这并不属实。

J)阐明具体规章要求。凡是有具体规章要求的地方，都应将事件报告给指定部门；

k)保证司法起诉或内部处罚规程取得成功。无论攻击是技术性的还是物理的，都应采取适当的信息安全防护措施(其中包括可证明数据被篡改的审计踪迹)，以便成功起诉攻击者或者根据内部规程惩罚攻击者。为了达到目的，就必须以法院或其他处罚机关所接受的方式收集证据。证据必须显示：

1)记录是完整的，且没有经过任何篡改；

2)可证明电子证据的复制件与原件完全相同；

3)收集证据的任何 IT 系统在记录证据时均运行正常。

1)阐明与监视技术相关的法律问题。必须依照国家相关的法律阐明使用监视技术的目的。有必要让人们知道存在对其活动的监视，包括通过监控技术进行的监视行动，十分重要。采取行动时需要考虑的因素有：什么人/哪些活动受监视、如何对他们/它们进行监视以及何时进行监视。有关入侵检测系统中监视/监控活动内容的描述可参见 ISO/IEC TR 18043。

m)制定和传达可接受的使用策略。组织应对可接受的做法/用途做出明确规定、形成正式文件并传达给所有相关用户。例如，应使用户了解可接受的使用策略，且要求用户填写书面确认，表明他们在参加组织或被授予信息系统访问权时，了解并接受该策略。

6.2.4 运行效率和质量

结构化的信息安全事件管理的运行效率和质量取决于诸多因素，包括通知事件的责任、通知的质量、易于使用的程度、速度和培训。其中有些因素与确保用户了解信息安全事件管理的价值和积极报告事件相关。至于速度，报告事件所花费的时间不是唯一因素，还包括它处理数据和分发处理的信息所用的时间(尤其是在警报的情况下)。

应通过信息安全事件管理人员的支持“热线”来补充适当的意识和培训计划，以便将事件延迟报告的时间降至最低。

6.2.5 匿名性

匿名性问题是关系到信息安全事件管理成功的基本问题。应该使用户相信，他们提供的信息安全事件的相关信息受到完全的保护，必要时，还会进行相应处理，从而使这些信息与用户所在组织或部门没有任何关联——除非协议中有相关规定。

信息安全事件管理方案应该阐明这些情况，即必须确保在特定条件下报告潜在信息安全事件的人员或相关方的匿名性。各组织应做出规定，明确说明报告潜在信息安全事件的个人或相关方是否有匿名要求。ISIRT 可能需要获得另外的、并非由事件报告人或报告方最初转达的信息。此外，有关信息安全事件本身的重要信息可从第一个发现到该事件的人员处获得。

6.2.6 保密性

信息安全事件管理方案中可能包含敏感信息，而处理事件的相关人员可能需要运用这些敏感信息。那么在处理过程中，或者信息应该是“匿名的”，或者有权访问信息的人员必须签订保密性协议。如果信息安全事态是由一个一般性问题管理系统记录下来的，则可能不得不忽略敏感细节。

此外，信息安全事件管理方案应该做出规定，控制将事件通报给媒体、业务伙伴、客户、执法机关和普通公众等外部方。

6.2.7 可信运行

任何信息安全事件管理组应该能够有效地满足本组织在功能、财务、法律、策略等方面的需要，并能在管理信息安全事件的过程中，发挥组织的判断力。信息安全事件管理组的功能还应独立地进行审计，以确定所有的业务要求有效地得以满足。此外，实现独立性的另一个好办法是，将事件响应报告链与常规运行管理分离，且任命一位高级管理人员直接负责事件响应的管理工作。财务运作方面也应与其他财务分离，以免受到不当影响。

6.2.8 系统化分类

一种反映信息安全事件管理方法总体结构的通用系统化分类，是提供一致结果的关键因素之一。这种系统化另类连同通用的度量机制和标准的数据库结构一起，将提供比较结果、改进警报信息，和生成信息系统威胁及脆弱性的更加准确的视图的能力。[3)]

3)定义通用系统化分类不是本标准的目的。读者可参考有关该信息的其他相关资源。

7 规划和准备

信息安全事件管理的规划和准备阶段应着重于：

•将信息安全事态和事件的报告及处理策略，以及相关方案(包括相关规程)形成正式文件；

•安排合适的事件管理组织结构和人员；

•制定安全意识简报和培训计划。

这一阶段的工作完成后，组织应为恰当地管理信息安全事件作好了充分准备。

7.1 概述

要将信息安全事件管理方案投入运行使用并取得良好的效率和效果，在必要的规划之后，需要完成大量准备工作。其中包括：

a)制定和发布信息安全事件管理策略并获得高级管理层的承诺(参见 7.2)；

b)制定详细的信息安全事件管理方案(参见 7.3)并形成正式文件。方案中包括以下主题：

1)用于给事件“定级”的信息安全事件严重性衡量尺度。如 4.2.1 所述，可根据事件对组织业务运行的实际或预计负面影响的大小，将事件划分为“严重”和“轻微”两个级别；

2)信息安全事态[4)]和事件[5)]报告单[6)](附录 A 列举了几种报告单)、相关文件化规程和措施，连同使用数据和系统、服务和/或网络备份以及业务连续性计划的标准规程；

3)带有文件化的职责的 ISIRT 的运行规程，以及执行各种活动的被指定人员[7]的角色的分配，例如，包括：

——在事先得到相关 IT 和/或业务管理层同意的特定情况下，关闭受影响的系统、服务和/或网络；

——保持受影响系统、服务和/或网络的连接和运行；

——监视受影响系统、服务和/或网络的进出及内部数据流；

——根据系统、服务和/或网络安全策略启动常规备份和业务连续性规划规程及措施；

——监控和维护电子证据的安全保存，以备法律起诉或内部惩罚之用；

——将信息安全事件细节传达给内部和外部相关人员或组织。

4)报告单由报告人填写(即不是由信息安全事件管理组成员填写)。

5)信息安全事件管理人员使用报告单编写有关信息安全事态的初步报告，并保留事件评估等的运行记录，直至事件被完全解决。在每个阶段，都需更新信息安全事态/事件散据库。所填写的报告单/信息安全事态/事件数据库记录随后会用于事件的善后工作。

6)如果可能，应将这些报告单制成电子表单(如在安全的 web 网页上)，并且可与电子形式的信息安全事态/事件数据库链接。在当今世界上，基于纸质的方案耗时费力，不是效率最佳的运行方式。

7)在规模较小的组织中，可指派一个人承担多个角色。

c)测试信息安全事件管理方案及其过程和规程的使用(参见 7.3.5)；

d)更新信息安全和风险分析及管理策略，以及具体系统、服务或网络的信息安全策略，包括对信息安全事件管理的引用，确保在信息安全事件管理方案输出的背景下定期评审这些策略(参见 7.4)；

e)建立 ISIRT，并为其成员设计、开发和提供合适的培训计划(参见 7.5)；

f)通过技术和其他手段支持信息安全事件管理方案(以及 ISIRT 的工作)(参见 7.6)；

g)设计和开发信息安全事件管理安全意识计划(参见 7.7)并将其分发给组织内所有员工(当有人员变更时重新执行一次)。

以下各节逐条描述了上述各项活动，其中包括所要求的每个文件的内容。

7.2 信息安全事件管理策略

7.2.1 目的

信息安全事件管理策略面向对组织信息系统和相关位置具有合法访问权的每一位人员。

7.2.2 读者

信息安全事件管理策略应经组织高级执行官的批准，并得到组织所有高级管理层确认的文件化的承诺。应对所有的组织成员及组织的合同商可用，还应在信息安全意识简报和培训中有所提及(参见 7.7)。

7.2.3 内容

信息安全事件管理策略的内容应涉及以下主题：

a)信息安全事件管理对于组织的重要性，以及高级管理层对信息安全事件管理及其相关方案作出的承诺；

b)对信息安全事态发现、报告和相关信息收集的概述，以及如何将这些信息用于确定信息安全事件。概述中应包含对信息安全事态的可能类型。以及如何报告、报告什么、向哪个部门以及向谁报告信息安全事态等内容的归纳，还包括如何处理全新类型的信息安全事态；

c)信息安全事件评估的概述，其中包括具体负责的人员、必须采取的行动以及通知和上报等；

d)确认一个信息安全事态为信息安全事件后所应采取的行动的概要，其中应该包括：

1)立即响应；

2)法律取证分析；

3)向所涉及人员和相关第三方传达；

4)考虑信息安全事件是否在可控制状态下；

5)后续响应；

6)“危机求助”发起；

7)上报标准；

8)具体负责的人员；

e)确保所有活动都得到恰当记录以备日后分析，以及为确保电子证据的安全保存而进行持续监控，以供法律起诉或内部处罚；

f)信息安全事件得到解决后的活动，包括事后总结经验教训和改进过程；

g)方案文件(包括规程)保存位置的详细信息；

h)ISIRT 的概述，围绕以下主题：

1)ISIRT 的组织结构和关键人员的身份，其中包括由谁负责以下工作：

——向高级管理层简单说明事件的情况；

——处理询问、发起后续工作等；

——对外联系(必要时)。

2)规定了 ISIRT 的具体工作以及 ISIRT 由谁授权的信息安全管理章程。章程至少应该包括 ISIRT 的任务声明、工作范围定义以及有关 ISIRT 董事会级发起人及其授权的详细情况；

3)着重描述 ISIRT 核心活动的任务声明。要想成为一个真正的 ISIRT，该小组应该支持对信息安全事件的评估、响应和管理工作，并最终得出成功的结论。该小组的目标和目的尤为重要，需要有清晰明确的定义；

4)定义 ISIRT 的工作范围。通常一个组织的 ISIRT 工作范围应包括组织所有的信息系统、服务和网络。有的组织可能会出于某种原因而将 ISIRT 工作范围规定得较小，如果是这种情况，应该在文件中清楚地阐述 ISIRT 工作范围之内和之外的对象；

5)作为发起者并授权 ISIRT 行动的高级执行官/董事会成员/高级管理人员的身份，以及 ISIRT 被授权的级别。了解这些有助于组织所有人员理解 ISIRT 的背景和设置情况，且对于建立对 ISIRT 的信任至关重要。应该注意的是，在这些详细信息公布之前，应该从法律角度对其进行审查。在有些情况下，泄漏一个小组的授权信息会使该小组的可靠性声明失效。

i)信息安全事件管理安全意识和培训计划的概述；

j)必须阐明的法律法规问题的总结(参见 5.2.3)。

7.3 信息安全事件管理方案

7.3.1 目的

信息安全事件管理方案的目的是提供一份文件，对事件处理和事件沟通的过程和规程作详细说明。一旦发现到信息安全事态，信息安全事件管理方案就开始起作用。该方案被用作以下活动的指南：

•对信息安全事态作出响应；

•确定信息安全事态是否为信息安全事件；

•对信息安全事件进行管理，并得出结论；

•总结经验教训，并确定方案和/或总体的安全需要改进的地方；

•执行已确定的改进工作。

7.3.2 读者

应将信息安全事件管理方案告示给组织全体员工，因此，包括负责以下工作的员工：

•发现和报告信息安全事态，可以是组织内任何员工，无论是正式工还是合同工；

•评估和响应信息安全事态和信息安全事件，以及事件解决后必要的经验教训总结、改进信息安全和修订信息安全事件管理方案的工作。其中包括运行支持组(或类似的工作组)成员、ISIRT、管理层、公关部人员和法律代表。

还应该考虑任何第三方用户，以及报告信息安全事件及相关脆弱性的第三方组织、政府和商业信息安全事件和脆弱性信息提供组织。

7.3.3 内容

信息安全事件管理方案文件的内容应包括：

a)信息安全事件管理策略的概述；

b)整个信息安全事件管理方案的概述；

c)与以下内容相关的详细过程和规程[8)]以及相关工具和衡量尺度的信息：

8)组织可自己决定是将所有规程放入到方案文件中，还是通过附加文件详细阐明全部或部分规程

1)规划和准备

——发现和报告发生的信息安全事态(通过人工或自动方式)；

——收集有关信息安全事态的信息；

——使用组织内认可的事态/事件严重性衡量尺度进行信息安全事态评估，确定是否可将它们重新划分为信息安全事件；

2)使用(当确认发生了信息安全事件时)

——将发生的信息安全事件或任何相关细节传达给其他内部和外部人员或组织；

——根据分析结果和已确认的严重性级别，启动立即响应，其中可能包括启动恢复规程和/或向相关人员传达；

——按要求和相关的信息安全事件的严重性级别，进行法律取证分析，必要时更改事件级别；

——确定信息安全事件是否处于可控制状态；

——做出任何必要的进一步响应，包括在后续时间可能需要做出的响应(例如，在实施一次灾难的完全恢复工作中)；

——如果信息安全事件不在控制下，发起“危机求助”行动(如呼叫消防队/部门或者启动业务连续性计划)；

——按要求上报，便于进一步评估和/或决策；

——确保所有活动被恰当记录，以便于日后分析；

——更新信息安全事态/事件数据库；

(信息安全事件管理方案文件应考虑对信息安全事件的立即响应和长期响应。所有的信息安全事件都需要提早评估其潜在负面影响，包括短期和长期影响(例如，在最初的信息安全事件发生一段时间后，可能会出现重大灾难)。此外，对完全不可预见的信息安全事件作出某些响应是必要的，且它们同时需要专门的防护措施。即使在这种情况下，方案文件应该对必要的步骤提供一般性指南。)

3)评审

——按要求进行进一步法律取证分析；

——总结信息安全事件的经验教训并形成文件；

——根据所得的经验教训，评审和确定信息安全的改进；

——评审相关过程和规程在响应、评估和恢复每个信息安全事件时的效率，根据所总结的经验教训，确定信息安全事件管理方案在总体上需要改进的地方；

——更新信息安全事态/事件数据库。

4)改进——根据经验教训，进行如下改进：

——信息安全风险分析和管理结果；

——信息安全事件管理方案(例如过程和规程、报告单和/或组织结构)；

——整体的安全，实施新的和/或经过改进的防护措施。

d)事态/事件严重性衡量尺度的细节(如严重或轻微，或重大、紧急、轻微、不要紧)以及相关指南；

e)在每个相关过程中决定是否需要上报和向谁报告的指南，及其相关规程。任何负责信息安全事态或事件评估工作的人员都应从信息安全事件管理方案文件提供的指南中知晓，在正常情况下，什么时候需要向上报告以及向谁报告。此外，还会有一些不可预见的情况可能也需要向上报告。例如。一个轻微的信息安全事件如果处理不当或在一周之内没有处理完毕，可能会发展成重大事件或“危机”情况。指南应定义信息安全事态和事件的类型、上报类型和由谁负责上报。

f)确保所有活动被记录在相应表单中，以及日志分析由指定人员完成所遵守的规程；

g)确保所维护的变更控制制度包括了信息安全事态和事件追踪、信息安全事件报告更新以及方案本身更新的规程和机制；

h)法律取证分析的规程；

i)有关使用入侵检测系统(IDS)的规程和指南，确保相关法律法规问题都得到阐述(参见5.2.3)。这些指南中应包含对攻击者采取监视行动利弊问题的讨论。有关 IDS 的进一步信息，可参见 ISO/IEC TR 15947《IT 入侵检测框架》和 ISO/IEC TR 180431(选择、配置和操作 IDS 指南》；

j)方案的组织结构；

k)整个 ISIRT 及个人成员的授权范围和责任；

1)重要的合同信息。

7.3.4 规程

在信息安全事件管理方案开始运行之前，必须有形成正式文件并经过检查的规程可供使用，这一点十分重要。每个规程文件应指明其使用和管理的负责人员，适当时来自运行支持组和/或 ISIRT。这样的规程应包含确保电子证据的收集和安全保存，以及将电子证据在不间断监控下妥善保管以备法律起诉或内部处罚之需等内容。而且，应有形成文件的规程不仅包括运行支持组和 ISIRT 的活动，同时还涉及法律取证分析和“危机求助”活动——如果其他文件(如业务连续性计划)不包括这些内容的话。显然，形成文件的规程应该完全符合信息安全事件管理策略和其他信息安全事件管理方案文件。

需要重点理解的是，并非所有规程都必须对外公开。例如，并非组织内所有员工都需要了解了 ISIRT 的内部操作规程之后才能与之进行协作。ISIRT 应该确保可“对外公开”的指南，其中包括从信息安全事件分析中得出的信息，以易于使用的方式存在，如将其置于组织的内部网上。此外，将信息安全事件管理方案的某些细节仅限于少数相关人员掌握可以防范“内贼”篡改调查过程。例如，如果一个盗用公款的银行职员对方案的细节很清楚，他或她就能更好地隐藏自身的行为，或妨碍信息安全事件的发现和调查及事件恢复工作的进行。

操作规程的内容取决于许多准则，尤其是那些与已知的潜在信息安全事态和事件的性质

以及可能涉及到的信息系统资产类型及其环境相关的准则。因此，一个操作规程可能与某一特定事件类型或实际上与某一类型产品(如防火墙、数据库、操作系统、应用程序)乃至具体产品相关联。每个操作规程都应清楚注明需要采取哪些步骤以及由谁执行。它应该是外部人员(如政府部门和商业 CERT 或类似组织，以及供应商等)和内部人员的经验的反映。

应有操作规程来处理已知类型的信息安全事态和事件。但还应有针对未知类型信息安全事态或事件的操作规程。用于针对此种情况的操作规程需阐明以下要求：

•处理这类“例外”的报告过程；

•及时得到管理层批准以免响应延迟的相关指南；

•在没有正式批准过程的情况下预授权的决策代表。

7.3.5 方案测试

应安排信息安全事件管理过程和规程的定期检查和测试，以突现可能会在管理信息安全事态和事件过程中出现的潜在缺陷和问题。在前一次响应评审产生的任何变更生效之前，应对其进行彻底检查和测试。

7.4 信息安全和风险管理策略

7.4.1 目的

在总体信息安全和风险管理策略中，以及具体系统，服务和网络的信息安全策略中包括信息安全事件管理方面的内容可达到以下目的：

•描述信息安全事件管理——尤其是信息安全事件报告和处理方案——的重要性；

•表明高级管理层针对适当准备和响应信息安全事件的需要，对信息安全事件管理方案作出的承诺；

•确保各项策略的一致性；

•确保对信息安全事件作出有计划的、系统的和冷静的响应，从而将事件的负面影响降至最低。

7.4.2 内容

应对总体的信息安全和风险管理策略，以及具体系统、服务或网络信息安全策略进行更新，以便它们清晰阐明总体的信息安全事件管理策略及相关方案。应有相关章节阐述高级管理层的承诺并概述以下内容：

•策路；

•方案的过程，和相关基础设施；

•检查、报告、评估和管理事件的要求。

并明确指定负责授权和/或执行某些关键行动的人员(如切断信息系统与网络的连接或甚至将其关闭)。

此外，策略应要求建立适当的评审机制，以确保从信息安全事件发现、监视和解决过程中得出的任何信息可被用于保证总体信息安全和风险管理以及具体系统、服务或网络的信息安全策略的持续有效。

7.5 ISIRT 的建立

7.5.1 目的

建立 ISIRT 的目的是为评估和响应信息安全事件并从中总结经验教训等工作提供具备合格人员的组织结构，并提供这方面工作所必要的协调、管理，反馈和沟通。ISIRT 不仅可以降低信息安全事件带来的物理和经济损失，还能降低可能因信息安全事件而造成的组织声誉损害。

7.5.2 成员和结构

ISIRT 的规模、结构和组成应该与组织的规模和结构相适应。尽管 ISIRT 可以组成一个独立的小组或部门，但其成员还可以兼任其他职务，因此鼓励从组织内各个部门中挑选成员组成 ISIRT。如第 4.2.1 和 7.1 节所述，许多情况下，ISIRT 是由一名高级管理人员所领导的一个虚拟小组。该高级管理人员可以得到各特定主题的专业人员(如擅长处理恶意代码攻击的专业人员)支持，ISIRT 可根据所发生信息安全事件的类型召唤相关人员前来处理紧急情况。在规模较小的组织中，一名成员还可以承担多种 ISIRT 角色。ISIRT 还可由来自组织不同部门(如业务运行部、IT/电信部门、审计部、人力资源部、市场营销部等)的人员组成。

IsIRT 成员应该便于联系，因此，每个成员及其备用人员的姓名和联系方式都应该在组织内进行登记。例如，一些必要的细节应清晰记入信息安全事件管理方案的文件中，包括规程文件和报告单，但可以不在策略声明文件中有所记载。

ISIRT 管理者应：

•指派授权代表以对如何处理事件做出立即决策；

•通常有一条独立于正常业务运行的专线用于向高级管理层报告情况；

•确保 ISIRT 全体成员具有必需的知识和技能水平，并确保他们的知识和技能水平可以得到长期保持；

•指派小组中最适合的成员负责每次事件的调查工作。

7.5.3 与组织其他部门的关系

ISIRT 管理者及成员必须具有某种等级授权，以便采取必要措施响应信息安全事件。但是，对于那些可能给整个组织造成经济上或声誉上的负面影响的措施，则应得到高级管理层的批准。为此，在信息安全事件管理策略和方案中必须详细说明授予 ISIRT 组长适当权限，使其报告严重的信息安全事件。

应对媒体的规程和责任也应得到高级管理层批准并形成文件。这些规程应规定：

•由组织中哪个部门负责接待媒体；

•该部门如何就这一问题与 ISIRT 相互交换信息。

7.5.4 与外部方的关系

ISIRT 应与外部方建立适当关系。外部方可能包括：

•签订合同的外部支持人员，如来自 CERT；

•外部组织的 ISIRT 或计算机事件响应组，或 CERT；

•执法机关；

•其他应急机构(如消防队/部门等)；

•相关的政府部门；

•司法人员；

•公共关系官员和/或媒体记者；

•业务伙伴；

•顾客；

•普通公众。

7.6 技术和其他支持

在已经取得、准备并测试了所有必要的技术和其他支持方式后，要对信息安全事件作出快速、有效的响应会变得更加容易。这包括：

•访问组织资产(最好使用最新的资产登记簿)的详细情况，并了解它们与业务功能之间关联方面的信息；

•查阅业务连续性战略及相关计划文件；

•文件记录和发布的沟通过程；

•使用电子信息安全事态/事件数据库和技术手段快速建立和更新数据库，分析其中的信息，以便于对事件作出响应(不过应该认识到，组织偶尔会有要求或使用手工记录的情况)；

•为信息安全事态/事件数据库做好充分的业务连续性安排。用来快速建立和更新数据库、分析其信息以便于对信息安全事件作出响应的技术手段应该支持：

•快速获得信息安全事态和事件报告；

•通过适当方式(如电子邮件、传真、电话等)通知已事先选定的人员(以及相关外部人员)，因而要求对可靠的联系信息数据库(它应该是易于访问的，同时还应包括纸质文件和其他备份)，以及适当时以安全方式将信息发送给相关人员的设施进行维护；

•对已评估的风险采取适当的预防措施，以确保电子通信(无论是通过互联网的还是不通过互联网的)，不会在系统、服务和网络遭受攻击时被窃听；

•对已评估的风险采取适当的预防措施，以确保电子通信(无论是通过互联网的还是不通过互联网的)在系统、服务和网络遭受攻击时仍然可用；

•确保收集到有关信息系统、服务和/或网络的所有数据以及经过处理的所有数据；

•如果根据已得到评估的风险采取措施，利用通过加密的完整性控制措施可帮助确定系统、服务和/或网络以及数据是否发生了变动以及它们的哪些部分发生了变动；

•便于对已收集信息的归档和安全保存(例如在日志和其他证据离线保存在 CD 或 DVD ROM 等只读介质中之前对其使用数字签名)；

•准备将数据(如日志)打印输出，其中包括显示事件过程、解决过程和证据保管链的数据；

•根据相关业务连续性计划，通过以下方式将信息系统、服务和/或网络恢复正常运行：

——良好的备份规程；

——清晰可靠的备份；

——备份测试；

——恶意代码控制；

——系统和应用软件的原始介质；

——可启动介质；

——清晰、可靠和最新的系统和应用程序补丁。

一个受到攻击的信息系统、服务或网络可能无法正常运转。因此，只要可能，并考虑到已受评估的风险，响应信息安全事件必需的任何技术手段(软件和硬件)都不应依赖于组织的“主流”系统、服务或网络的运行。如果可能，它们应该完全独立。

所有技术手段都应认真挑选、正确实施和定期测试(包括对所做备份的测试)。

应指出的是，本节所描述的技术手段不包括那些用来直接检测信息安全事件和入侵并能自动通知相关人员的技术手段。有关这些技术内容的描述可参见 ISO/IEC TR 15947《信息技术 安全技术 IT 入侵检测框架》以及 ISO/IEC 13335《信息技术 安全技术 信息和通信技术安全管理》。

7.7 意识和培训

信息安全事件管理是一个过程，它不仅涉及技术而且涉及人，因此应该得到组织内有适当信息安全意识并经过培训的员工支持。

组织内所有人员的意识和参与，对于一个结构化的信息安全事件管理方法的成功来说，至关重要。鉴于此，必须积极宣传信息安全事件管理的作用，以作为总体信息安全意识和培训计划的一部分。安全意识计划及相关材料应该对所有人员可用，包括新员工，以及相关第

三方用户和合同商。应为运行支持组和 ISIRT 成员，以及如果必要的话，包括信息安全人员和特定的行政管理人员，制定一项特定的培训计划。应该指出的是，根据信息安全事件类型、频率及其与事件管理方案交互的重要程度的不同，直接参与事件管理的各组成员需要不同级别的培训。

安全意识简报应该包括下列内容：

•信息安全事件管理方案的基本工作机制，包括它的范围以及安全事态和事件管理“工作流程”；

•如何报告信息安全事态和事件；

•如果相关的话，有关来源保密的防护措施；

•方案服务级别协议；

•结果的通知——建议在什么情况下采用哪些来源；

•不泄露协议规定的任何约束；

•信息安全事件管理组织的授权及报告流程；

•由谁以及如何接受信息安全事件管理方案的报告。

在有些情况下，将有关信息安全事件管理的安全意识教育细节包括在其他培训计划(如面向员工的培训计划或一般性的总体安全意识计划)之中是可取的做法。这样的安全意识教育方法可以为特定人群提供极具价值的背景信息，从而改进培训计划的效果和效率。

在信息安全事件管理方案开始运行之前，所有相关人员必须熟悉发现和报告信息安全事态的规程，且被选人员必须十分了解随后的过程。还应该有后续的安全意识简报和培训课程。培训应该得到运行支持组和 ISIRT 成员、信息安全员和特定的行政管理员的具体练习和测试工作的支持。

8 使用

8.1 概述

运行中的信息安全事件管理由“使用”和“评审”这两个主要阶段组成，在这之后是“改进”阶段，即根据总结出来的经验教训改善安全状况。这些阶段及其相关过程在 5.2 中有简要介绍。“使用”阶段是本章描述的内容，随后的第 9 章和第 10 章将分别描述“评审”和“改进”阶段。

图 2 示出了这 3 个阶段及其相关过程。

8.2 关键过程的概述

使用阶段的关键过程有；

a)发现和报告发生的信息安全事态，无论是由组织人员/顾客引起的还是自动发生的(如，防火墙警报)；

b)收集有关信息安全事态的信息，由组织的运行支持组人员[9)]进行第一次评估，确定该事态是属于信息安全事件还是发生了误报；

9)一般来说，不要期望运行支持组人员就是安全专家

c)ISIRT 进行第二次评估，首先确认该事态是否属于信息安全事件，如果的确如此，则作出立即响应，同时启动必要的法律取证分析和沟通活动；

d)由 ISIRT 进行评审以确定该信息安全事件是否处于控制下：

1)如果处于控制下，则启动任何所需要的进一步的后续响应，以确保所有相关信息准备完毕，以供事件后评审所用；

2)如果不在控制下，则采取“危机求助”活动并召集相关人员，如组织中负责业务连续性的管理者和工作组；

e)在整个阶段按要求进行上报，以便进一步评估和/或决策；

f)确保所有相关人员，尤其是 ISIRT 成员，正确记录所有活动以备后面分析所用；

g)确保对电子证据进行收集和安全保存，同时确保电子证据的安全保存得到持续监视，以备法律起诉或内部处罚所需；

h)确保包括信息安全事件追踪和事件报告更新的变更控制制度得到维护，从而使得信息安全事态/事件数据库保持最新。

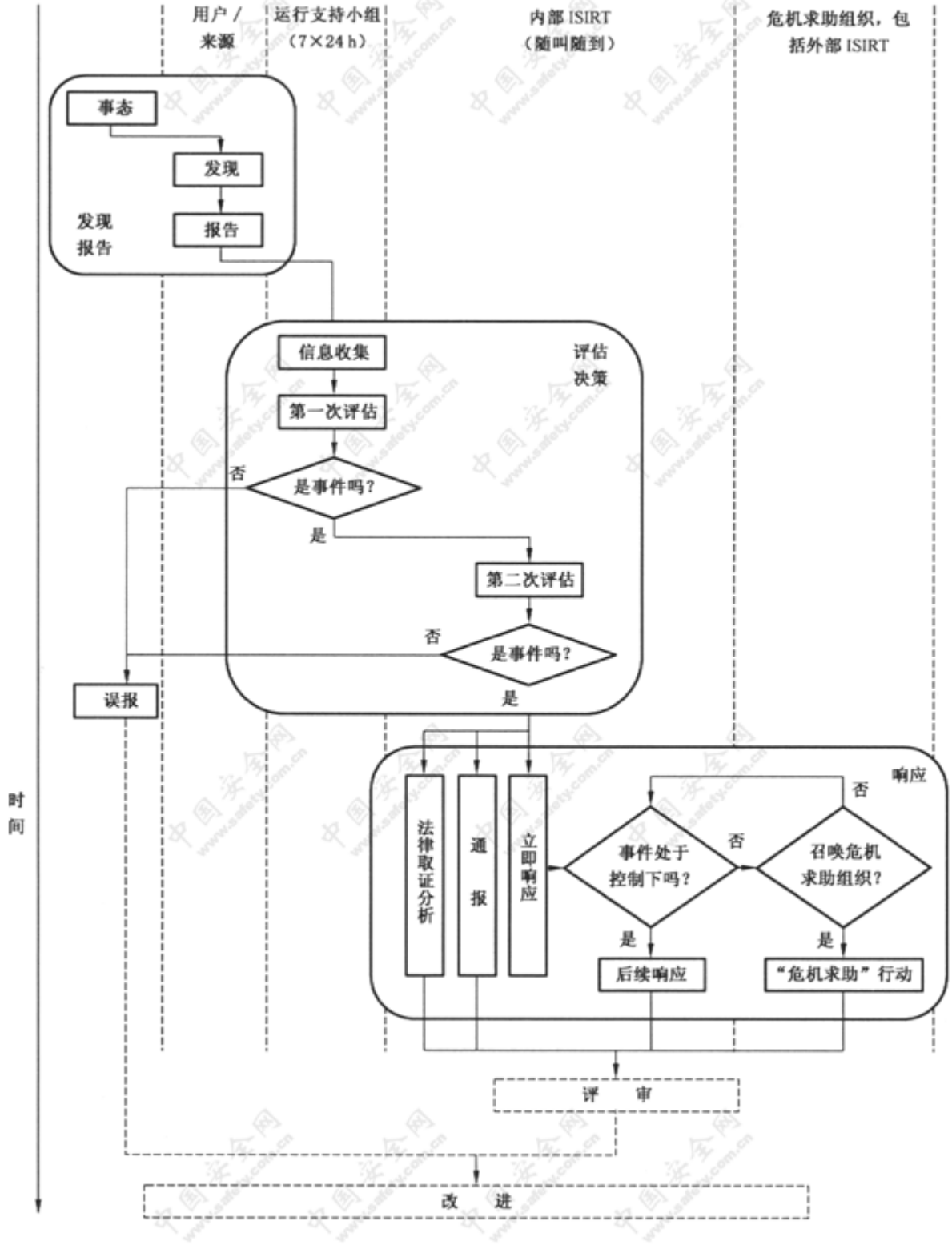

图 2 信息安全事态和事件处理流程图

所有收集到的、与信息安全事态或事件相关的信息应保存在由 ISIRT 管理的信息安全事态/事件数据库中。每个过程所报告的信息应按当时的情况尽可能保持完整，以确保为评估和决策以及其他相关措施提供可靠基础。

一旦发现和报告了信息安全事态，那么随后的过程应达到以下目的：

•以适当的人员级别分配事件管理活动的职责，包括专职安全人员和非专职安全人员的评估、决策和行动；

•制定每个被通知人员均需遵守的正式规程，包括评估和修改报告，评估损害，以及通知相关人员(至于每个人的具体行动由事件的类型和严重程度来决定)；

•使用指南来完整地将一个信息安全事态记入文件，如果该事态被归类为信息安全事件，那随后采取的行动也应记入文件，并更新信息安全事态/事件数据库。

指南涉及：

•8.3 讨论的信息安全事态发现和报告；

•8.4 讨论的评估和决策(确定是否应将信息安全事态归类为信息安全事件)；

•8.5 讨论的对信息安全事件的响应，包括：

——立即响应；

——评审以确定信息安全事件是否在控制之下；

——随后响应；

——“危机求助”行动；

——法律取证分析；

——沟通；

——上报问题；

——记录各项行动。

8.3 发现和报告

信息安全事态可以被由技术、物理或规程方面出现的某种情况引起注意的一人或多人发现。例如，发现可能来自火/烟探测器或者入侵(防盗)警报，并通知到预先指定位置以便有人采取行动。技术型的信息安全事态可通过自动方式发现，如由审计追踪分析设施、防火墙、入侵检测系统和防病毒工具在预设参数被激发的情况下发出的警报。

无论发现信息安全事态的源头是什么，得到自动方式通知或直接注意到某些异常的人员要负责启动发现和报告过程。该人员可以是组织内任何一名员工，无论是正式员工还是合同工。该员工应遵照相关规程，并使用信息安全事件管理方案规定的信息安全事态报告单在第一时间把信息安全事态报告给运行支持组和管理层。因此，所有员工要十分了解并且能够访问用于报告各种类型的可能的信息安全事态的指南——其中包括信息安全事态报告单的格式以及每次事态发生时应该通知的联系人的具体信息，这一点至关重要。(所有人员至少要知晓信息安全事件报告单的格式，这有助于他们理解信息安全事件管理方案。)

如何处理一个信息安全事态取决于该事态的性质以及它的意义和影响。对于许多人来说，这种决定超出了他们的能力。因此，报告信息安全事态的人员应尽量使用叙述性文字和当时可用的其他信息完成信息安全事态报告单，必要的话，与本部门管理者取得联系。报告单最好是电子格式的(例如以电子邮件或 web 表单的方式提交)，应该安全地发送给指定的运行支持组(它最好应提供 7×24h 服务)，并将一份拷贝交给 ISIRT 管理者。附录 A 给出了一份信息安全事态报告单的示例模板。

应该强调的是，在填写信息安全事态报告单的内容时，既要保证准确性，也要保证及时性。为了提高报告单内容的准确性而拖延提交报告单的时间，不是一种好做法。如果报告人对报告单上某些字段中的数据没有信心，在提交时应加上适当的标记，以便后来沟通时修改。还应该认识到，有些电子报告机制(如电子邮件)本身就是明显的攻击对象。

当默认的电子报告机制(如电子邮件)存在问题或被认为存在问题(包括认为可能出现系统受攻击且报告单可以被未授权人员读取的情况)时，应该使用备用的沟通方式。备用方式

可能包括通过人、电话或文本消息。当调查初期就明显表明，信息安全事态极有可能被确定为信息安全事件，特别是重大事件时，尤其应该使用上述备用方式。

应该指出的是，尽管在多数情况下，信息安全事态必须向上报告以便于运行支持组采取措施，但偶尔也会有在本部门管理者协助下直接在本地处理信息安全事态的情况。一个信息安全事态可能很快就被确定为误报，或者被解决达到满意的结果。在这种情况下，报告单应填写完毕后报告给本部门管理者以及运行支持组和 ISIRT，以便记录归档，如记人信息安全事态/事件数据库中。在这样的情况下，可以由报告信息安全事态结束的人员完成信息安全事件报告单所要求的一些信息——即使这种情况属实，那么信息安全事件报告单也应该填写完整并上报。

8.4 事态/事件评估和决策

8.4.1 第一次评估和初始决策

运行支持组中负责接收报告的人员应签收已填写完毕的信息安全事态报告单，将其输入到信息安全事态/事件数据库中，并进行评审。该人员应该从报告信息安全事态的人处得到详细说明，并从该报告人或其他地方进一步收集可用的任何必要和已知信息，随后，运行支持组的该人员应该进行评估，以确定这个信息安全事态是属于信息安全事件还是仅为一次误报。如果确定该信息安全事态属于误报，应将信息安全事态报告单填写完毕并发送给 ISIRT，供添加信息安全事态/事件数据库和评审所用，同时将拷贝发送给事态报告人及其部门管理者。

这一阶段收集到的信息和其他证据可能会在将来用于内部处罚或司法起诉过程。承担信息收集和评估任务的人员应接受证据收集和保存方面的专门培训。

除了记录行动的日期和时间外，全面记录下列内容也是必要的：

•看见了什么、做了什么(包括使用的工具)以及为什么要这么做；

•“证据”所处的位置；

•如何将证据归档(如果可行的话)；

•如何进行证据验证(如果可行的话)；

•证据材料的存储/安全保管以及随后对其进行访问的细节。

如果确定信息安全事态很可能是一个信息安全事件，而且运行支持组成员具有适当资质，则可以进行进一步评估。这可能引发必要的补救措施，例如确定应该增加哪些应急防护措施并指定适当人员执行。显然，当一个信息安全事态被确定为重大信息安全事件(根据组织内预先制定的事件严重性衡量尺度)时，应该直接通知 ISIRT 管理者。显而易见，如果出现“危机”情况，应该及时宣布，例如通知业务连续性管理者可能需要启动业务连续性计划，同时还应通知 ISIRT 管理者和高级管理层。但最可能的情况是，必须将信息安全事件直接指派给 ISIRT 进行进一步评估和采取措施。

无论决定下一步要采取什么行动。运行支持组成员都应尽可能地将信息安全事件报告单填写完整。附录 A 给出了一个信息安全事件报告单的示倒模板。信息安全事件报告单应使用叙述性文字，应尽可能确认和描述以下内容：

•该信息安全事件属于什么情况；

•事件是被如何引起的——由什么情况或由谁引起；

•事件带来的危害或可能带来的危害；

•事件对组织业务造成的影响或潜在影响；

•确定该信息安全事件是否属于重大事件(根据组织预前制定的事件严重性衡量尺度)；

•到目前为止是如何处理的。

当从以下几个方面考虑信息安全事件对组织业务的潜在或实际负面影响时：

•未授权泄露信息；

•未授权修改信息；

•抵赖信息；

•信息和/或服务不可用；

•信息和/或服务遭受破坏。

首先要考虑哪些后果与之相关，例如：

•对业务运行造成的财务损失/破坏；

•商业和经济利益；

•个人信息；

•法律法规义务；

•管理和业务运行；

•声誉损失。

对于那些被认为与信息安全事件相关的后果，应使用相关分类指南确定潜在或实际影响，并输入到信息安全事件报告单中。附录 B 给出了要点指南，该指南给出组织划分自身信息安全事件后果等级的要点示例。该后果等级可作为组织实施 GB/Z 20986-2007(信息安全技术 信息安全事件分类分级指南》的参考依据，有助于确定信息安全事件分级中“系统损失”这一参考要素的级别，结合“信息系统的重要程度”和“社会影响”，可明确信息安全事件的级别大小。

如果信息安全事件已被解决，报告中应该详细记录已经采取的防护措施和从事件中总结出的经验教训(例如，用来防止同样或类似事件再次发生的防护措施)。

一旦报告单填写完毕后，应将其送达 ISIRT 作为信息安全事态/事件数据库和评审的输入。

如果调查时间可能超过一周，应产生一份中间报告。

应该强调的是，根据信息安全事件管理方案文件提供的指南，负责评估信息安全事件的运行支持组人员应了解：

•何时必须将同题上报以及应该向谁报告；

•运行支持组进行的所有活动应遵循正式成文的变更控制规程。

当默认的电子报告机制(如电子邮件)存在问题或被认为存在问题(包括认为可能出现系统受攻击且报告单可以被未授权人员读取的情况)时，应该使用备用方式向 ISIRT 管理者报告。备用方式可能包括通过人、电话或文本消息传递。当信息安全事件属于重大事件时，尤其应该使用这种备用方式。

8.4.2 第二次评估和事件确认

进行第二次评估以及对是否将信息安全事态归类为信息安全事件的决定进行确认是 ISIRT 的职责。ISIRT 接收报告的人员应该：

•签收由运行支持组尽可能填写完成的信息安全事态报告单；

•将报告单输入信息安全事态/事件数据库；

•向运行支持组寻求任何必要的澄清说明；

•评审报告单内容；

•从运行支持组、信息安全事态报告单填写人或其他地方进一步收集可用的任何必要和已知信息。

如果信息安全事件的真实性或报告信息的完整性仍然存在某种程度不确定，ISIRT 成员

应该进行一次评估，以确定该信息安全事件是否属实还是仅为一次误报。如果信息安全事件被确定为误报，应完成填写信息安全事态报告、将其添加到信息安全事态/事件数据库中并送达 ISIRT 管理者。同时还应将报告的拷贝送达运行支持组、事态报告人及其部门管理者。

如果信息安全事件被确定是真实的，ISIRT 成员(包括必要的合作伙伴)应进行进一步的评估，以尽快确认：

•该信息安全事件是什么样的情形，是如何被引起的——由什么或由谁引起，带来或可能带来什么危害，对组织业务造成的影响或潜在影响，是否属于重大事件(根据组织预先制定的事件严重性衡量尺度而定)；

•对任何信息系统、服务和/或网络进行的故意的、人为的技术攻击，例如：

——系统，服务和/或网络被渗透的程度，以及攻击者的控制程度；

——攻击者访问——可能复制、篡改或毁坏了——哪些数据；

——攻击者复制、篡改或毁坏了哪些软件；

•对任何信息系统、服务和/或网络的硬件和/或物理位置进行的故意的、人为的物理攻击，例如：

——物理损害造成了什么直接和间接影响(是否设置了物理访问安全保护措施?)；

•并非直接由人为活动引起的信息安全事件，其直接和间接影响(例如，是因火灾而导致物理访问开放?是因某些软件或通信线路故障或人为错误而使信息系统变得脆弱?)；

•到目前为止信息安全事件是如何被处理的。

当从以下方面评审信息安全事件对组织业务的潜在或实际负面影响时：

•未授权泄露信息；

•未授权修改信息；

•抵赖信息；

•信息和/或服务不可用；

•信息和/或服务遭受破坏；

有必要确认哪些后果与之相关，如以下示例类别：

•对业务运行造成的财务损失/破坏；

•商业和经济利益；

•个人信息；

•法律法规义务；

•管理和业务运行；

•声誉损失。

对于那些被认为与信息安全事件相关的后果，应使用相关类别的指南确定潜在或实际影响，并输入到信息安全事件报告单中。附录 B 给出了要点指南，该指南给出组织划分自身信息安全事件后果等级的要点示例。该后果等级可作为组织实施 GB/Z Z0986-2007《信息安全技术 信息安全事件分类分级指南》的参考依据，有助于确定信息安全事件分级中“系统损失”这一参考要素的级别，结合“信息系统的重要程度”和“社会影响”，可明确信息安全事件的级别大小。

8.5 响应

8.5.1 立即响应

8.5.1.1 概述

在多数情况下，ISIRT 成员的下一步工作是确定立即响应措施，以处理信息安全事件、在信息安全事件单上记录细节并输入信息安全事态/事件数据库，以及向相关人员或工作组

通报必要的措施。这可能导致采取应急防护措施(例如在得到相关 IT 和/或业务管理者同意后切断、关闭受影响的信息系统、服务和/或网络)和/或增加已被确定的永久防护措施并将行动通报相关人员或工作组。如果尚不能这么做，则应根据组织预先确定的信息安全事件严重性衡量尺度确定信息安全事件的严重程度，如果事件足够严重，应直接上报组织相关高级管理人员。例如，如果事件明显是一种“危机”情况，应通知业务连续性管理者以备可能启动业务连续性计划，同时还要通知 ISIRT 管理者和高级管理层。

8.5.1.2 措施示例

这是一个在信息系统、服务和/或网络遭到放意攻击的情况下，采取相关的立即响应措施的例子。如果攻击者不知道自己已处于监视之下，可保留与互联网或其他网络的连接，以：

•允许业务关键应用程序正常运转；

•尽可能多地收集有关攻击者的信息。

但是在执行这一决策时，必须考虑以下因素：

•攻击者可能会意识到自己受到监视，很可能采取行动进一步毁坏受影响信息系统、服务和/或网络以及相关数据；

•攻击者可能会破坏对于追踪他/她本人有用的信息。

一旦作出中断/关闭受攻击的信息系统、服务和/或网络的决定，其迅速和可靠的执行必须在技术上可行。但同时应实施适当的鉴别手段，以使未授权人员无法进行这种活动。

需要进一步考虑的是如何预防事件重演，这通常是行动的重中之重；不难得出结论，攻击者暴露了应该矫正的弱点，仅仅追踪攻击者是不够的。特别是当攻击者是非恶意的且造成的危害小乃至没有危害时，这一点容易被忽视。

对于由非蓄意攻击导致的信息安全事件，应该确定其来源。在采取防护措施的同时，可能有必要关闭信息系统、服务和/或网络，或者隔离相关部分井将其关闭(在取得相关 IT 和/或业务管理者的预先同意下)。如果所发现的弱点对于信息系统、服务和/或网络设计来说是根本性的，或者说是一个关键弱点，处理起来可能需要更长时间。

另一个响应措施可能是启用监视技术(如“蜜罐”，参见 ISO/IEC TR 18043)。这样的行动应该依照正式成文的信息安全事件管理方案规定的规程进行。

ISIRT 成员应对照备份记录来检查因信息安全事件而出现讹误的信息，搞清是否存在篡改、删除或插入等情况。检查日志的完整性是必要的，因为故意行为的攻击者很可能为了掩盖自己的行踪而修改这些日志。

8.5.1.3 事件信息更新

无论确定下一步采取什么行动，ISIRT 成员都应尽最大能力更新信息安全事件报告，并将其添加到信息安全事态/事件数据库，同时按需要通知 ISIRT 管理者和其他必要人员。更新可能包括有关以下内容的更多信息：

•信息安全事件是什么样的情形；

•它是如何被引起的——由什么或由谁引起；

•它带来或可能带来什么危害；

•它对组织业务造成的影响或潜在影响；

•它是否属于重大事件(根据组织预先制定的事件严重性衡量尺度)；

•到目前为止它是如何被处理的。

如果信息安全事件已被解决，报告应包含已经采取的防护措施的详细情况和其他任何经验教训(例如用来预防相同或类似事件再次发生的进一步防护措施)。被更新的报告应该添加到信息安全事态/事件数据库中，并通报 ISIRT 管理者和其他必要人员。

应该强调的是，ISIRT 负责妥善保管与信息安全事件相关的所有信息，以备鉴别分析和可能在法庭上作证据之用。例如一个针对 IT 的信息安全事件，在最初发现事件后，应该在受影响的 IT 系统、服务和/或网络关闭之前收集所有只会短暂存在的数据，为完整的法律取证调查作好准备。需要收集的信息包括内存、缓冲区和注册表的内容以及任何过程运行的细节，以及：

•根据信息安全事件的性质，对受影响的系统、服务和/或网络进行一次完整复制，或对日志和重要文件进行一次低层备份，以备法律取证之用；

•对相邻系统、服务和网络的日志(例如包括路由器和防火墙的日志)进行收集和评审；

•将所有收集到的信息安全地保存在只读介质上；

•进行法律取证复制时应有两人以上在场，以表明和保证所有工作都是遵照相关法律法规执行的；

•用来进行法律取证复制的工具和命令的规范和说明书均应登记归档，并与原始介质一起保存。

在这一阶段如果可能的话，ISIRT 成员还要负责将受影响设施(IT 设施或其他设施)恢复到不易遭受相同攻击破坏的安全运行状态。

8.5.1.4 进一步的活动

如果 ISIRT 成员确定的确发生了信息安全事件，还应采取如下其他重要措施，如：

•开始法律取证分析；

•向负责对内对外沟通的人员通报情况，同时建议应该以什么形式向哪些人员报告什么内容。

一旦尽力完成信息安全事件报告后，应将其输入信息安全事态/事件数据库并送达 ISIRT 管理者。

如果组织内的调查工作超出了预定时间，应产生一份中间报告。

基于信息安全事件管理方案文件提供的指南，负责评估信息安全事件的 ISIRT 人员应该了解：

•何时必须将问题上报以及应该向谁报告；

•ISIRT 进行的所有活动均应遵循正式成文的变更控制规程。

当常规通信设施(如电子邮件)存在问题或者被认为存在问题(包括系统被认为可能处于攻击之下)，而且：

•得出信息安全事件属于严重事件的结论；

•确定出现了“危机”情况时，

应在第一时间将信息安全事件通过人、电话或文本方式报告给相关人员。

ISIRT 管理者在同组织的信息安全负责人及相关董事会成员/高级管理人员保持联络的同时，被认为有必要同所有相关方(组织内部的和外部的)也应保持联络(参见 7.5.3 和 7.5.4)。

为了确保这样的联络快速有效，有必要事先建立一条不完全依赖于受信息安全事件影响的系统、服务和/或网络的安全通讯渠道。包括指定联系人不在时的备用人选或代表。

8.5.2 事件是否处于控制下

在 ISIRT 成员作出立即响应，并进行了法律取证分析和通报相关人员后，必须迅速得出信息安全事件是否处于控制之下的结论。如果需要，ISIRT 成员可以就这一问题征求同事、ISIRT 管理者和/或其他人员或工作组的意见。

如果确定信息安全事件处于控制之下，ISIRT 成员应启动需要的后续响应，并进行法律

取证分析和向相关人员通报情况(参见 8.5.3、8.5.5 和 8.5.6)，直至结束信息安全事件的处理工作，使受影响的信息系统恢复正常运行。

如果确定信息安全事件不在控制之下，ISIRT 成员应启动“危机求助行动”(参见 8.5.4)。

8.5.3 后续响应

在确定信息安全事件处于控制之下、不必采取“危机求助”行动之后，ISIRT 成员应确定是否需要对信息安全事件作出进一步响应以及作出什么样的响应。其中可能包括将受影响的信息系统，服务和/或网络恢复到正常运行。然后，该人员应该将有关响应细节记录到信息安全事件报告单和信息安全事态/事件数据库中，并通知负责采取相关行动的人员。一旦这些行动成功完成后，应该将结果细节记录到信息安全事件报告单和信息安全事态/事件数据库中，然后结束信息安全事件处理工作，并通知相关人员。

有些响应旨在预防同样或类似信息安全事件再次发生。例如，如果确定信息安全事件的原因是 IT 硬件或软件故障，而且没有补丁可用，应该立即联系供应商。如果信息安全事件涉及到一个已知的 IT 脆弱性，则应装载相关的信息安全升级包。任何被信息安全事件突现出来的 IT 配置问题均应得到妥善处理。降低相同或类似 IT 信息安全事件再次发生可能性的其他措施还包括变更系统口令和关闭不用的服务。

响应行动的另一个方面涉及 IT 系统、服务和/或网络的监控。在对信息安全事件进行评估之后，应在适当的地方增加监视防护措施，以帮助发现具有信息安全事件症状的异常和可疑事态。这样的监视还可以更深刻地揭露信息安全事件，同时确定还有哪些其他 IT 系统受到危及。

启动相关业务连续性计划中特定的响应可能很必要。这一点既适用于 IT 信息安全事件，同时也适用于非 IT 的信息安全事件。这样的响应应涉及业务的所有方面，不仅包括那些与 IT 直接相关的方面，同时还应包括关键业务功能的维护和以后的恢复——其中包括(如果相关的话)语音通信、人员级别和物理设施。

响应行动的最后一个方面是恢复受影响系统、服务和/或网络。通过应用针对已知脆弱性的补丁或禁用易遭破坏的要素，可将受影响的系统、服务和/或网络恢复到安全运行状态。如果因为信息安全事件破坏了日志而无法全面了解信息安全事件的影响程度，可能要考虑对整个系统、服务和/或网络进行重建。这种情况下，启动相关的业务连续性计划十分必要。

如果信息安全事件是非 IT 相关的，例如由火灾、洪水或爆炸引起，就应该依照正式成文的相关业务连续性计划开展恢复工作。

8.5.4 “危机求助”行动

如 8.5.2 所述，ISIRT 确定一个信息安全事件是否处于控制下时，很可能会得出事件不在控制之下，必须按预先制定计划采取“危机求助”行动的结论。

有关如何处理可能会在一定程度上破坏信息系统可用性/完整性的各类信息安全事件的最佳选择，应该在组织的业务连续性战略中进行标识。这些选择应该与组织的业务优先顺序和相关恢复时间表直接相关，从而也与 IT 系统、语音通信、人员和食宿供应的最长可承受中断时间直接关联。业务连续性战略应该明确标明所要求的：

•预防、恢复和业务连续性支持措施；

•管理业务连续性规划的组织结构和职责；

•业务连续性计划的体系结构和概述。

业务连续性计划以及支持启动计划的现行防护措施，一旦经检验合格并得到批准后，便可构成开展“危机求助”行动的基础。

其他可能类型的“危机求助”行动包括(但不限于)启用：

•灭火设施和撤离规程；

•防洪设施和撤离规程；

•爆炸“处理”及相关撤离规程；

•专家级信息系统欺诈调查程序；

•专家级技术攻击调查程序。

8.5.5 法律取证分析

当前面的评估确定需要收集证据时——在发生重大信息安全事件的背景下，ISIRT 应进行法律取证分析。这项工作涉及按照正式文件规定的程序，利用基于 IT 的调查技术和工具，对指定的信息安全事件进行信息安全事件管理过程中迄今为止更周密的分析研究。它应该以结构化的方式进行，应该确定哪些内容可以用作证据，进而确定哪些证据可以用于内部处罚，哪些证据可以用于法律诉讼。

法律取证分析所需设备可分为技术(如审计工具、证据恢复设备)，规程、人员和安全办公场所 4 类。每项法律取证分析行动都应完全登记备案，其中包括相关照片、审计踪迹分析报告、数据恢复日志。进行法律取证分析人员的熟练程度连同熟练程度测试记录一起应登记备案。能够表明分析的客观性和逻辑性的任何其他信息也都应记录在案。有关信息安全事件本身、法律取证分析行动等的所有记录以及相关的存储介质，都应保存在一个安全的物理环境中并遵照相关规程严加控制，以使其不至被未授权人员接触，也不会被篡改或变得不可用。基于 IT 的法律取证分析工具应该符合标准，其准确性应能经得起司法推敲，而且要随着技术的发展升级到最新版本。ISIRT 工作的物理环境应提供可做验证的条件，以确保证据的处理过程不会受人质疑。显然，ISIRT 要有充足的人员配备才能做到在任何时候都能对信息安全事件作出响应，而且在需要时“随叫随到”。

随着时间的推移，难免会有人要求对信息安全事件(包括欺诈、盗窃和蓄意破坏)的证据重新审理。因此，要对 ISIRT 有所帮助，就必须有大量基于 IT 的手段和支持性规程供 ISIRT 在信息系统、服务或网络中揭开“隐藏”信息——其中包括看似像是已被删除、加密或破坏的信息。这些手段应能应付已知类型信息安全事件的所有已知方面(并且当然被记录在 ISIRT 规程中)。

当今，法律取证分析往往必须涉及错综复杂的联网环境，调查工作必将涵盖整个操作环境，其中包括各种服务器——文件、打印、通信、电子邮件服务器等，以及远程访问设施。有许多工具可供使用，其中包括文本搜索工具，镜像软件和法律取证组件。应该强调的是，法律取证分析规程的主要焦点是确保证据的完好无缺和核查无误，以保证其经得起法律的考验，同时还要保证法律取证分析在原始数据的准确拷贝上进行，以防分析工作损害原始介质的完整性。

法律取证分析的整个过程应包括以下相关恬动：

•确保目标系统、服务和/或网络在法律取证分析过程中受到保护，防止其变得不可用、被改变或受其他危害(包括病毒入侵)，同时确保对正常运行的影响没有或最小；

•对“证据”的“捕获”按优先顺序进行，也就是从最易变化的证据开始到最不易变化的证据结束(这在很大程度上取决于信息安全事件的性质)；

•识别主体系统、服务和/或网络中的所有相关文件，包括正常文件、看似(但并段有)被删除的文件、口令或其他受保护文件和加密文件；

•尽可能恢复已发现的被删除文件和其他数据；

•揭示 IP 地址、主机名、网络路由和 web 站点信息；

•提取应用软件和操作系统使用的隐藏、临时和交换文件的内容；

•访问受保护或被加密文件的内容(除非法律禁止)；

•分析在特别(通常是不可访问的)磁盘存储区中发现的所有可能的相关数据；

•分析文件访问、修改和创建的时间；

•分析系统/服务/网络和应用程序日志；

•确定系统/服务/网络中用户和/或应用程序的活动；

•分析电子邮件的来源信息和内容；

•进行文件完整性检查，检测系统特洛伊木马和原来系统中不存在的文件；

•如果可行，分析物理证据，如查看指纹、财产损害程度、监视录像、警报系统日志、通行卡访问日志以及会见目击证人等；

•确保所提取的潜在证据被妥善处理和保存，使之不会被损害或不可使用，并且敏感材料不会被未授权人员看到。应该强调的是，收集证据的行为要遵守相关法律的规定；

•总结信息安全事件的发生原因以及在怎样的时间框架内采取的必要行动，连同具有相关文件列表的证据一起附在主报告中；

•如果需要，为内部惩罚或法律诉讼行动提供专家支持。

所采用的方法应该记录在 ISIRT 规程中。

ISIRT 应该充分结合各种技能来提供广泛的技术知识(包括很可能被蓄意攻击者使用的工具和技术)、分析/调查经验(包括如何保存有用的证据)、相关法律法规知识以及事件的发展趋势。

8.5.6 通报

在许多情况下，当信息安全事件被 ISIRT 确定属实时，需要同时通知某些内部人员(不在 ISIRT/管理层的正常联系范围内)和外部人员(包括新闻界)。这种情况可能会发生在事件处理的各个阶段，例如，当信息安全事件被确认属实时，当事件被确认处于控制之下时，当事件被指定需要“危机求助”时，当事件的处理工作结束时以及当事件评审完成并得出结论时。

为协助必要时通报工作的顺利进行，明智的做法是提前准备一些材料，到时候根据特定信息安全事件的具体情况调整材料的部分内容，然后迅速通报给新闻界和/或其他媒体。任何有关信息安全事件的消息在发布给新闻界时，均应遵照组织的信息发布策略。需要发布的消息应由相关方审查，其中包括组织高级管理层、公共关系协调员和信息安全人员。

8.5.7 上报

有时会出现必须将事情上报给高级管理层、组织内其他部门或组织外人员/组织的情况。这可能是为了对处理信息安全事件的建议行动作出决定，也可能是为了对事件作出进一步评估以确定需要采取什么行动。这时应遵循 8.4 描述的评估过程，或者，如果严重问题早就凸现出来，或许已经处于这些过程之中了。在信息安全事件管理方案文件中应有指南可供那些可能会在某一时刻需要将问题上报的人员(即运行支持组和 ISIRT 成员)使用。

8.5.8 活动日志和变更控制

应该强调的是，所有参与信息安全事件报告和管理的人员应该完整地记录下所有的活动以供日后分析之用。这些内容应该包含在信息安全事件报告单和信息安全事态/事件数据库中，而且要在从第一次报告单到事件后评审完成的整个过程中不断更新。记录下来的信息应该妥善保存并留有完整备份。此外，在追踪信息安全事件以及更新信息安全事件报告单和信息安全事态/事件数据库的过程中所做的任何变更，均应遵照已得到正式批准的变更控制方案进行。

9 评审

9.1 概述

信息安全事件解决完毕并经各方同意结束处理过程后，还须进一步进行法律取证分析和评审，以确定有哪些经验教训需要汲取以及组织的整体安全和信息安全事件管理方案有哪些地方需要改进。

9.2 进一步的法律取证分析

在事件被解决后，可能依然需要进行法律取证分析以确定证据。此项工作应由 ISIRT 使用 8.5.5 建议的工具和规程进行。

9.3 经验教训

一旦信息安全事件的处理工作结束，应该迅速从信息安全事件中总结经验教训并立即付诸实施，这一点十分重要。经验教训可能反映在以下方面：

•新的或改变的信息安全防护措施需求。可能是技术或非技术(包括物理)的防护措施。根据总结出来的经验教训，可能需要迅速更新和发布安全意识简报(给用户和其他人员)，以及迅速修订和发布安全指南和/或标准；

•信息安全事件管理方案及其过程、报告单和信息安全事态/事件数据库的变更。

此外，这项工作应不仅限于某一次信息安全事件的范畴，还应分析事件的发展趋势和发生模式，这有助于确定防护措施或方法需要有哪些改变。根据一次 1T 信息安全事件的情况进行信息安全测试，尤其是脆弱性评估，也是十分明智的做法。

因此，应该定期分析研究保存在信息安全事态/事件数据库中的数据，以：

•确定事件的发展趋势和发生模式；

•确定需要关注的方面；

•分析在哪些部位采取预防措施可以降低将来事件发生的可能性。

在信息安全事件发生过程中所获得的相关信息应该用来进行事件发展趋势/发生模式的分析。这一点对于根据以往经验和文字资料尽早确定信息安全事件以及警告进一步会引发哪些信息安全事件来说，十分有效。

此外，还应充分利用政府部门，商业 CERT 和供应商提供的信息安全事件和相关脆弱性信息。

发生信息安全事件后。对信息系统、服务和/或网络进行的脆弱性评估和安全测试应不仅限于受信息安全事件影响的信息系统、服务和/或网络。应该把任何相关的信息系统、服务和/或网络全都包括进来。应通过全面的脆弱性评估来了解在此事件中所利用的其他信息系统、服务和/或网络的脆弱性，同时确保没有新的脆弱性被引入。

值得强调的是，脆弱性评估应定期进行，而且信息安全事件发生后对脆弱性的再次评估应是这一持续评估过程的一个组成部分(而并非替代)。

应该对信息安全事件作出分析总结，并呈递到组织管理层的信息安全管理协调小组和/或组织总体信息安全策略中定义的其他管理协调小组的每次会议上。

9.4 确定安全改进

在信息安全事件解决后的评审过程中，根据需要可能确定新的或改变的防护措施。改进建议和相关防护措施需求可能因财务或运作上的原因不能立即付诸实施，在这种情况下应该作为组织的长期目标逐步实行。例如，换用一种更安全更强固的防火墙短期内可能在财务上行不通，但是必须将其看作组织早晚要达到的长期信息安全目标(参见 10.3)。

9.5 确定方案改进

在事件解决之后，ISIRT 管理者或其代表应该评审所发生的一切以进行评估，从而“量

化”对信息安全事件整体响应的效果。这样的分析旨在确定信息安全事件管理方案的哪些方面成功地发挥了作用，有哪些方面需要改进。

响应后分析的一个重要方面是将信息和知识反馈到信息安全事件管理方案中。如果事件相当严重，应在事件解决后尽快安排所有相关方召开会议。这样的会议应该考虑以下因素：

-信息安全事件管理方案规定的规程是否发挥了预期作用?

•是否有对发现事件有帮助的规程或方法?

•是否确定过对响应过程有帮助的规程或工具?

•是否有在确定事件之后对恢复信息系统有帮助的规程?

•在事件发现、报告和响应的整个过程中向所有相关方的事件通报是否有效?

会议结果应记录归档，各方一致同意的任何行动都应适当地遵照行事(参见第 10.4 节)。

10 改进

10.1 概述

“改进”阶段的工作包括执行“评审”阶段提出的建议，即改进安全风险分析和管理结果、改善安全状况和改进信息安全事件管理方案。下面各条将逐一阐述这些主题。

10.2 安全风险分析和管理改进

根据信息安全事件的严重程度和影响，在评估信息安全风险分析和管理评审的结果时，必须考虑新的威胁和脆弱性。作为完成信息安全风险分析和管理评审更新的后续工作，引入更新的或全新的防护措施可能是必要的。

10.3 改善安全状况

遵照“评审”阶段(参见 9.4)提出的改进建议和对许多信息安全事件的分析，更新的和/或全新的防护措施需要启动。如 9.3 所述，这些措施可能是技术或非技术(包括物理)的防护措施，并可能需要迅速更新和发布安全意识简报(给用户和其他人员)，以及迅速修订和公布安全指南和标准。此外，对组织的信息系统、服务和网络应定期进行脆弱性评估，以帮助确定脆弱性和提供一个对系统/服务/网络持续加固的过程。

另外，在一次事件之后立即进行的信息安全规程和文件评审更有可能是以后会被要求的一种响应。在一次信息安全事件之后，相关的信息安全策略和规程应参考事件管理过程中收集的信息和识别的任何问题来进行更新。确保组织全体人员知悉信息安全策略和规程的更新是 ISIRT 以及组织信息安全管理者的一个长期持续目标。

10.4 改进方案

对信息安全事件管理方案中被确定需要改进的地方(参见 9.5)，需要认真评审和判断，然后据此修订更新方案文件。信息安全事件管理过程、规程和报告单的任何更改都应经过全面检查和测试后方可投入使用。

10.5 其他改进

“评审”阶段可能还会确定其他需要改进的方面，如信息安全策略、标准和规程的变更，IT 硬件和软件配置的变更等。

附录 A

(资料性附录)

信息安全事态和事件报告单示例

信息安全事态和事件报告

填写说明

信息安全事态和事件报告单的设计旨在向相关人员提供有关信息安全事态和事件(如果

事态被确定为信息安全事件)的信息。

如果你怀疑有信息安全事态正在发生或已经发生——尤其是可能会对组织的财产或声誉带来巨大损失或损害的事态,你应立即按照组织的信息安全事件管理方案规定的规程填写和提交一份信息安全事态报告单。

你提供的信息将被用来启动对事态的适当评估,从而确定是否要将该事态归类为信息安全事件,以及是否需要采取补救措施预防或限制损失或损害。如果时间紧迫,你可以不必在这时填写完本报告单的所有栏目。

如果你是评审已全部或部分填写的事态报告单的一名运行支持组成员,你将被要求审查是否需将该事态归类为信息安全事件。如果该事态被归为事件,你应尽可能将更多的信息填人信息安全事件报告单,且将信息安全事态和事件报告单一并转交给 ISIRT。无论该信息安全事态是否被归类为事件,都应及时更新信息安全事态/事件数据库。

如果你是评审由运行支持组转交的信息安全事态和事件报告单的一名 ISIRT 成员,你应随着调查的进展不断更新事件报告单的内容,同时对信息安全事态/事件数据库进行相应更新。

请遵照以下指南来完成报告单:

•如果可能,报告单应以电子方式[10)]填写和提交。(当默认的电子报告机制(如电子邮件)存在问题或被认为存在问题时(包括认为可能出现系统受攻击且报告单可以被未授权人员读取的情况时),应该使用备用的报告方式。备用方式可能包括通过人、电话或文本消息传递);

10) 只要可能,就应将这些报告制成电子表格(如在安全的 web 网页上),并且可与电子形式的信息安全事态/事件数据库链接。在当今世界上,运行基于纸质的方案会耗时费力,不是效率最佳的运行方式。

•只提供你本人了解的事实——不要为了完成报告单中的栏目凭推测填写。如果你不能肯定你提供的信息,请清楚地注明该信息没有被确认,以及使你认为它可能真实的依据;

•你应该提供你的全部详细联系信息。为了就你的报告进一步向你了解情况,就必须与体联系——不管是马上还是以后。

如果你后来发现自己提供的任何信息有不准确、不完整或误导性的地方,你应及时纠正并重新提交报告。

信息安全事态报告

事态日期:

事态编号[11)]:

11) 事态编号应由组织的 ISIRT 管理者分配。

相关事态和/或事件标识号(如果有的话)

报告人的详细情况

姓名: 地址:

单位: 部门:

电话: 电子信箱:

事态描述:

•发生了什么

•如何发生的

•为什么会发生

•受影响的部分

•对业务的负面影响
•任何已确定的脆弱性
信息安全事态细节
发生事态的日期和时间：
发现事态的日期和时间：
报告事态的日期和时间：
事态是否结束?(选择)是口 否口
如果是，具体说明事态持续了多长时间(天/小时/分钟)

信息安全事件报告
事件日期：
事件编号[12)]：
12) 事件编号应由组织的 ISIRT 管理者分配，并与相关的事态编号相对应。
相关事态和/或事件标识号(如果有的话)
运行支持成员的详细情况
姓名： 地址：
电话： 电子信箱：
ISIRT 成员的详细情况

姓名： 地址：
电话： 电子信箱：
信息安全事件描述
事件的进一步描述：
•发生了什么
•如何发生的
•为什么会发生
•受影响的部分
•对业务的负面影响
•任何已确定的脆弱性
信息安全事件细节
发生事件的日期和时间：
发现事件的日期和时间：
报告事件的日期和时间：
事件是否结束?(选择)是口 否口
如果是，具体说明事件持续了多长时间(天/小时/分钟)
如果否，具体说明到目前为止事件已经持续了多长时间

信息安全事件报告
信息安全事件的类型
(选择一项，然后填写相关栏目。)实际发生的口 未遂的口 可疑的口
(选择一项)
基本分类 有害程序事件(MI)口

子类 计算机病毒事件(CVI)口 蠕虫事件(WI)口
特洛伊木马事件(THI)口 僵尸网络事件(BI)口
混合攻击程序事件(BAD 口 网页内嵌恶意代码事件(WBPI)口
其他有害程序事件(OMI)口
起因 故意口 过失口 非人为口 未知口

基本分类 网络攻击事件(NAI)口
子类 拒绝服务攻击事件(DOSAI)口 后门攻击事件(BDAI)口
漏洞攻击事件(VAI)口 网络扫描窃听事件(NSEI)口
网络钓鱼事件(PI)口 干扰事件(ID)口
其他网络攻击事件(ONAI)口
起因 故意口 过失口 非人为口 未知口

基本分类 信息破坏事件(IDI)口
子类 信息篡改事件(IAI)口 信息假冒事件(IMI)口
信息泄漏事件(ILEI)口 信息窃取事件(III)口
信息丢失事件(ILOI)口
其他信息破坏事件(OIDI)口
起因 故意口 过失口 非人为口 未知口
基本分类 信息内容安全事件(ICSI)口
子类 违反宪法和法律、行政法规的信息安全事件口
针对社会事项进行讨论、评论形成网上敏感的舆论热点，出现一定规模炒作的信息安全事件口
组织串连、煽动集会游行的信息安全事件口
其他信息内容安全事件口
起因 故意口 过失口 非人为口 未知口

基本分类 设备设施故障(FF)口
子类 软硬件自身故障(SHF)口 外围保障设施故障(PSFF)口
人为破坏事故(MDA)口 其他设备设施故障(IF-OT)口
起因 故意口 过失口 非人为口 未知口

信息安全事件报告
基本分类 灾害性事件(DI)口
基本分类 其他事件(OI)口 (指不能归为以上 6 个基本分类的信息安全事件。)
受影响的资产
受影响的资产(如果有的话)
(提供受事件影响或与事件有关的资产的描述，包括相关序号、许可证和版本号。)
信息/数据：
硬件：
软件：
通信设施：

文档：

事件对业务的负面影响

对以下的每个选项指出是否相关，使用各类别(包括对业务运行造成的财务损失/破坏(FD)、商业和经济利益(CE)、个人信息(PI)、法律法规义务(LR)、管理和业务运行(MO)、声誉损失(LG))的指南(参见附录 B 的示例)，用“1～10”衡量尺度在“数值”项中记录事件对所涉及到的所有各方业务造成负面影响的程度。将所适用的指南的类别代号字母填写到“指南”项中，并且如果了解实际成本，可填写到“成本”项中。

数值 指南 成本

违背保密性口

(即未授权泄露)

违背完整性口

(即未授权篡改)

违背可用性口

(即不可用)

违背抗抵赖性口

遭受破坏口

事件的全部恢复成本

(如果可能，给出事件恢复的实际总成本， 数值 指南 成本

用“1～10”衡量尺度填写“数值”项，用实际成本

填写“成本”项)

信息安全事件报告

事件解决

事件调查开始日期：

事件调查员姓名：

事件结束日期：

影响结束日期：

事件调查完成日期：

调查报告的引用和位置

涉及的人员/作恶者

(选择一项) 人员(PE)口 合法建立的组织/部门(OI)口

有组织的团体(GR)口 事故(AC)口

无作恶者(NP)口

(例如，自然因素、设备故障、人为错误)

作恶者的描述

实际的或察觉的动机

(选择一项) 犯罪/经济收益(CG)口 消遣/黑客攻击(PH)口

政治/恐怖主义(PT)口 报复(RE)口

其他(OM)口

具体说明：

已采取的解决事件行动

(例如，“无行动”、“内部行动”、“内部调查”、“由……进行外部调查”)

计划采取的解决事件行动

(参见上例)

未完成的行动

(例如，调查仍在被其他人员要求)

信息安全事件报告

结论

(选择一项，指出事件后果级别，并用简短的叙述性文字来 特别严重口 严重口 较大口 较小口 论证这一结论)

(指出任何其他的结论)

被通知的个人/实体

(这一细节应由负责信息安全并声 信息安全管理者口
明所需行动的人员填写。如果需 站点管理者口
要，可以由机构的信息安全管理者 (说明哪一站点)
进行调整。) 报告发起人口 报告发起人的部门管理者口

警察口 其他口

(例如，帮助台、人力资源部、管理层、内部审计、执法机关、外部 CERT 等)具体说明：

涉及的个人

报告发起人 评审人 评审人

签字： 签字： 签字：

姓名： 姓名： 姓名：

角色： 角色： 角色：

日期： 日期： 日期：

报告发起人 评审人 评审人

签字： 签字： 签字：

姓名： 姓名： 姓名：

角色： 角色： 角色：

日期： 日期： 日期：

附录 B

(资料性附录)

信息安全事件评估要点指南示例

B.1 概述

本附录给出了信息安全事件负面后果评估和分类的要点指南示例，每项指南分使用 1(低级)~10(高级)衡量尺度。(实际上也可能使用其他衡量尺度，比如从 1 到 5，只要各组织采用最适合自身环境的衡量尺度。)

在阅读下列指南之前，应注意以下要点说明：

•在下面的有些指南示例中，有些条目被标明为“无输入”。这是因为指南统一了格式，从而本附录所示的所有六个类别的负面后果均可用 1~10 逐级上升的衡量尺度表达。然而某些类别中的某些等级(1～10)上，与相邻较低级别的后果条目相比没有足够的差异来形成一个条目，因此便将它们视为“无输入”。与此类似，在某些类别的高端由于与最高级别后果条目相比没有更严重的后果，因此便将其上的各高端后果条目视为“无输入”。(由此可见。

认为取消“无输入”项就可以压缩等级数量在逻辑上是不正确的。）

•对于下面使用了财务数字的指南，所示的范围看起来有些奇怪。在应用这些指南之前，必须用适于组织的货币单位填写它们的财务数字范围。

因此，要使用下面的指南示例。且当从以下方面考虑信息安全事件对组织业务造成的负面后果时：

•未授权泄露信息；

•未授权修改信息；

•抵赖信息；

•信息和/或服务不可用；

•信息和/或服务遭受破坏；

首先要考虑以下哪些后果类别与事件相关。对于被认为相关的后果，应该使用类别指南来确定其对组织业务运行的实际负面影响，并作为“数值”项条目填写到信息安全事件报告单中。

B.2 对业务运行造成的财务损失/破坏

信息未授权泄露和修改、抵赖以及不可用和遭受破坏的后果，可能是财务损失，如因行动迟缓或没有而造成股票下跌、合同欺诈或违反等。同样地，尤其是信息不可用或遭受破坏的后果会中断组织的业务运行。平息和/或从这样的事件中恢复过来需要耗费大量时间和精力。这在有些案例中表现得非常突出，应予以考虑。为了取得一个共同衡量尺度，恢复的时间应以人员的时间单位计算并转换成财务成本。这一成本应该参照组织内适当等级/级别的正常人月成本计算。应该使用以下指南。

a)导致财务损失/成本为 x_1 或更小；

b)导致财务损失/成本在 x_1+1 和 x_2 之间；

c)导致财务损失/成本在 x_2+1 和 x_3 之间；

d)导致财务损失/成本在 x_3+1 和 x_4 之间；

e)导致财务损失/成本在 x_4+1 和 x_5 之间；

f)导致财务损失/成本在 x_5+1 和 x_6 之间；

g)导致财务损失/成本在 x_6+1 和 x_7 之间；

h)导致财务损失/成本在 x_7+1 和 x_8 之间；

i)导致财务损失/成本大于 x_8；

j)组织停业。

B.3 商业和经济利益

商业和经济信息必须得到保护，并估算它们对于竞争者的价值以及它们的安全受到危及时可能会给组织的商业利益带来的影响。应该使用以下指南。

a)对竞争者有利益，但没有商业价值；

b)对竞争者有利益，其价值为 y_1 或更小(营业额)；

c)对竞争者有价值，其价值在 y_1+1 和 y_2(营业额)之间，或者导致财务损失或收入潜力损失，或者给个人或组织带来不当收入或优势，或者破坏对第三方信息的保密承诺；

d)对竞争者有价值，其价值在 y_2+1 和 y_3 之间(营业额)；

e)对竞争者有价值，其价值在 y_3+1 和 y_4 之间(营业额)；

f)对竞争者有价值，其价值大于 y_4+1(营业额)；

g)无输入”[13]；

13)“无输入”是指在这一影响等没没有相应条目可供输入。

h)无输入；

i)可能极大破坏组织的商业利益，或者极大破坏组织的财务生存能力；

j)无输入。

B.4 个人信息

根据我国个人信息保护相关法律法规的规定，组织应对持有和处理的个人信息施以保护，以防它们被未授权泄露，以免造成尴尬，甚至遭到法律诉讼。组织应按相关法律要求，保持个人信息的正确性，因为未授权修改导致错误信息会造成与未授权泄露信息类似的后果。同样重要的是，不得使个人信息不可用或遭受破坏，因为这会导致作出不正确决定或无法在所要求的时间内采取行动，最终造成与未授权泄露或修改信息类似的后果。应该使用以下指南。

a)给个人带来轻微痛苦(担忧)——气愤、沮丧、失望，但没有违背法律法规的要求；

b)给个人带来痛苦(担忧)——气愤、沮丧、失望，但没有违背法律法规的要求；

c)违背法律法规、道德规范或众所周知的有关保护信息的要求，给个人带来轻微尴尬；

d)违背法律法规、道德规范或众所周知的有关保护信息的要求，给个人带来严重尴尬或给群体带来轻微尴尬；

e)违背法律法规、道德规范或众所周知的有关保护信息的要求，给个人带来严重尴尬；

f)违背法律法规、道德规范或众所周知的有关保护信息的要求，给群体带来严重尴尬；

g)无输入；

h)无输入；

i)无输入；

j)无输入。

B.5 法律法规义务

组织持有和处理的数据应遵从国家相关法律法规规定的义务。不履行这些义务，无论有意还是无意，都有可能导致对相关组织或个人采取法律诉讼或行政处罚的行动。这些行动有可能导致罚款和/或判刑入狱。应该使用以下指南。

a)无输入；

b)无输入；

c)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；

d)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；

e)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/罚款或最高 2 年监禁；

f)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、10 年以下监禁；

g)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；

h)无输入；

i)无输入；

j)无输入。

B.6 管理和业务运行

有的信息十分重要，它的损害可能会危害组织的有效运行。例如，与策路变动相关的信息如果泄露的话，可能会引起公众反应-造成该策略无法实施。与财务或计算机软件相关信息的修改、抵赖或不可用也有可能对组织的运行带来严重后果。此外，对承诺的否认也可能会对组织的业务带来负面后果。应该使用以下指南。

a)组织的某个部分运行效率低；

b)无输入；

c)削弱组织及其运行的正常管理；

d)无输入；

e)阻碍组织策略的有效开发或执行；

f)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；

g)严重阻碍维织重要策略的开发或执行，或者中断或严重干扰组织的重要运行；

h)无输入；

i)无输入；

j)无输入。

B.7 声誉损失

信息的未授权泄露和修改、抵赖或不可用，可能会对组织的声誉造成损失，从而导致组织的声望损害、可信度损失以及其他负面后果。应该使用以下指南。

a)无输入；

b)导致组织内的局部尴尬境地；

c)负面地影响到与股东、客户、供应商、管理机关、政府部门、其他组织或公众之间的关系，导致当地/地区的负面曝光；

d)无输入；

e)负面地影响到与股东、客户、供应商、管理机关、政府部门、其他组织或公众之间的关系，导致国家范围内的负面曝光；

f)无输入；

g)负面地影响到与股东、客户、供应商、管理机关、政府部门、其他组织或公众之间的关系，导致广泛的负面曝光；

h)无输入；

i)无输入；

j)无输入。

附录 C

(资料性附录)

本指导性技术文件与 ISO/IEC TR 18044：2004 的技术性差异及其原因

表 C.1 给出了本指导性技术文件与 ISO/IEC TR 18044：2004 的技术性差异及其原因的一览表.。

表 C.1 本指导性技术文件与 ISO/IEC TR 18044：2004 技术性差异及其原因

本指导性技术文件的章条编号	技术性差异	原因
1 2	删除了 ISO/IEC TR 18044：2004 中第 1 章第 2 段中关于标准章节主要内容的简介。 归纳了 ISO/IEC TR 18044：2004 中第 11 章的内容，对其中的关键内容进行了概况，作为本指导性技术文件的第 1 章第 1 段。 引用了对应于国际标准 ISO/IEC 17799 的我国标准。 增加引用了 GB/Z 20986-2007《信息安全技术 信息安全事件分类分级指南》。	使本指导性技术文件第 1 章“范围”的内容更符合我国国家标准的描述要求。 符合 GB/T1.1
3	删除了 ISO/IEC TR 18044：2004 中第 3 章“术语和定义”的 3.5“其他”，将其改为参考文献。	根据 GB/T1.1 的要求，对一个术语集的引用改为参考文献。
4	增加了第 4 章“缩略语”	符合 GB/T1.1
—	删除了 ISO/IEC TR 18044：2004 的第 6 章“信息安全事件及其原因示例”。	该章内容仅是示例性说明，与 GB/Z 20986-2007 相关内容的描述存在差异，考虑到它对理解和使用整个标准的指导性作用不是很明显，故做了删除处理。
8.4.1	对原有内容，即“对于那些被认为与信息安全事件相关的后果，应使用相关分类指南确定潜在或实际影响，并输入到信息安全事件报告单中。附录 B 给出了要点指南。”进行了补充说明。 增加为“对于那些被认为与信息安全事件相关的后果，应使用相关分类指南确定潜在或实际影响，并输入到信息安全事件报告单中。附录 B 给出了要点指南。该指南给出组织划分自身信息安全事件后果等级的要点示例，该后果等级可作为组织实施 GB/Z 20989-2007《信息安全事件分类分级指南》的参考依据，有助于确定信息安全事件分级中“系统损失”这一参考要素的级别，结合“信息系统的重要程度”和“社会影响”，可明确信息安全事件的级别大小。”	对本指导性技术文件附录 B 的内容做了进一步的解释，另外，将本指导性技术文件与 GB/Z 20986-2007 的相互参考使用关系进行了详细的说明。
附录 A	参考 GB/Z 20989-2007 中对信息安全事件的分类和事件后果级别的内容进行了相应修改。	考虑到与 GB/Z 20986-2007 的协调性。

参考文献

[1]ISO/IEC TR 13335-3 Information technology—Guidelines for the management of IT Security—Part 3：Techniques for the management of IT Security

ISO/IECTR133353《信息技术 IT 安全管理指南 第 3 部分：IT 安全管理技巧》

[2]ISO/IEC TR 15947：2002 Information technology—Security techniques IT intrusion detection framework

ISO/IEC TR 15947：2002《信息技术 安全技术 IT 入侵检测框架》

[3]ISO/IEC 18028(all parts)IT security technique—IT network security

ISO/IEC 18028《信息技术 安全技术 IT 网络安全》(所有部分)

[4]ISO/IEC 18043 IT Security techniques—Selection，Deployment and Operations

of Intrusion Detection Systems(IDS)(document type subject to NP approval on SC27 N4029 by 2004-09-24)

ISO/IEC 18043《信息技术 安全技术 入侵检测系统(IDS)的选择、配置和操作》

[5]ISO/IEC Guide 73：2002 Risk management—Vocabulary—Guidelines for use in standards

ISO/IEC 指南 73：2002《风险管理 词汇 标准使用指南》

[6]Internet Engineering Task Force(IETF) Site Security Handbook，

http：//www.ietf.org/rfc/rfc2196. txt? number=2196

《互联网工程任务组(IETF)网站安全手册》，http：//www.ietf.org/rfc2196.txt? number=2196

[7]Expectations for Computer Security Incident Response—Best Practice，June 98，

ftp：//ftp.isi.edu/in-notes/rfc2350.txt

《对计算机安全事件响应的期望—最佳实践》，1998 年 6 月，ftp：//ftp.isi.edu/in-notes/rfc2350.txt

[8]NIST Special Publication 800-3 Nov’91，Establishing a Computer Incident Response Capability(CSIRC)，http：//csrc.nist.gov/publications/nlstpubs/800-3/800-3.pdf

NIST SP 800-3《建立计算机事件响应能力(CSIRC)》，1991 年 11 月，

http：//csrc.nist.gov/puhlieations/nistpubs/800-3/800-3.pdf

[9]ISO/IEC JTCl SC27 SD6，Glossary

ISO/IEC JTCI/SC27 SD6《术语集》

（校对：寒戈 责任编辑：竹勋）

发布单位： 国家质量监督检验检疫总局 2007-6-14 发布

提出单位： 全国信息安全标准化技术委员会

起草单位： 中国电子技术标准化研究所、北京同方信息安全股份有限公司、北京知识安全工程中心、北京邮电大学

批准单位： 国家标准化管理委员会