ICS 35.030
CCS L80

中华人民共和国国家标准

GB/T 32920—XXXX/ISO/IEC 27010:2015
代替 GB/T 32920—2016

信息安全技术 行业间和组织间通信的信息安全管理

Information security technology - Information security management for inter-sector and inter-organizational communications

(ISO/IEC 27010:2015,IDT)

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

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

本文件代替GB/T 32920—2016《信息技术 安全技术 行业间和组织间通信的信息安全管理》，与GB/T 32920—2016相比，依据ISO/IEC 27010的结构变化和技术变化，本文件结构变化见附录NA，主要技术变化如下：

a) 更改标准名称为《信息安全技术 行业间和组织间通信的信息安全管理》；
b) 删除了术语“信息共享团体”、“可信信息通信机构”，直接引用GB/T 29246术语和定义（见第3章，2016年版的第3章）；
c) 增加了关于附录内容引用的说明（见4.1）；
d) 删除了业务连续性和风险管理中信息共享团体成员实施业务连续性风险评估的实现指南（见2016年版的4.1）；
e) 增加了信息共享团体信任的说明（见4.2）；
f) 信息共享团体管理中，考虑成员组织间差异时，增加了不同的法律或法规环境（见4.3）；
g) 删除了符合性评估的说明（见2016年版的4.6）；
h) 增加了按优先级分级说明（见8.2.1）；
i) “信息分类”更改为“信息分级”（见8.2.1）。

本文件等同采用ISO/IEC 27010:2015《信息技术　安全技术　行业间和组织间通信的信息安全管理》（英文版）。根据GB/T 1.1—2020和GB/T 20000.2—2009的规定，做了如下一些编辑性修改：

a) 增加了“本文件中“针对行业间和组织间通信没有附加特定的控制”，指的是GB/T 22081—2016中对应条款没有附加特定的控制”（见引言）；
b) ISO/IEC 27000:2014更改为与GB/T 29246—2017对应的ISO/IEC 27000:2016(见2和3.1）；
c) 增加了3.2缩略语（见3）；
d) 增加了对附录NA直接引用的引语“附录NA给出GB/T 32920—XXXX与GB/T 32920—2016结构变化对比表。”（见4.1）；
e) 增加了对附录NA直接引用的引语“附录NB给出了GB/T 22081—2016/ISO/IEC 27002:2013与ISO/IEC 27002:2022控制的对应关系”（见4.1）；
f) 增加了资料性附录NA（见附录NA）；
g) 增加了资料性附录NB（见附录NB）；
h) 参考文献增加ISO/IEC 27002:2022。

本文件由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：山东省标准化研究院、中国网络安全审查技术与认证中心、国家计算机网络应急技术处理协调中心、日照市标准化研究院、陕西省网络与信息安全测评中心、西安邮电大学、华为技术有限公司、杭州安恒信息技术股份有限公司、长扬科技（北京）有限公司、北京三快在线科技有限公司、阿里云计算有限公司、山东正中信息技术股份有限公司、成都秦川物联网科技股份有限公司、青岛中盛信息技术有限公司、OPPO广东移动通信有限公司、济宁市质量技术监督信息所、莒县政务服务中心、众安信息技术服务有限公司。

本文件主要起草人：王曙光、公伟、朱丰雪、魏军、王文磊、李丹、张勇、邵萌、梁伟、赵华、祖岩岩、秦扬、许志国、胡鑫磊、王媛、郑伟、张磊、苏志卫、李腾、李永发、常立丽、刘金琳、刘晓宇、张明状、戴洪刚、秦峰、万谊平。

本文件及其所代替的历次版本发布情况为：

——2016年首次发布为GB/T 32920—2016；

——本次为第一次修订。

引　言

本文件是对 GB/T 22080—2016 和 GB/T 22081—2016 在信息共享团体中使用的补充。本文件中的指南是对信息安全管理体系（ISMS）标准族其他标准中通用指南的补充。

GB/T 22080—2016 和 GB/T 22081—2016 采用一种通用的方式处理组织间的信息交换。当组织间进行敏感信息[1)]交换时，可通过建立信息共享团体来确保接收方安全的使用敏感信息。尽管信息共享团体成员间存在竞争，但成员之间相互信任，他们相信对方会对已共享敏感信息采取安全保护措施。

信息共享团体成员间相互信任是团体有效运行的前提。一方面信息发起方需要信任接收方不会泄露或不当的使用数据；另一方面信息接收方基于发起方的资质，信任发起方提供信息的准确性。以上两方面需要信息共享团体明确有效的安全策略和实践的支持。为达到上述目标，信息共享团体成员需要建立一个涵盖共享信息的通用安全管理体系即信息共享团体的信息安全管理体系（ISMS）。

针对行业间不同团体之间敏感信息的共享，由于信息发起方无法了解所有接收方，此时可通过在团体及其信息共享协议之间建立信任来进行信息共享。

本文件中“针对行业间和组织间通信没有附加特定的控制”，指的是GB/T 22081—2016中对应条款没有附加特定的控制。

1） 行业或组织认为可能造成利益损失但又不能成为国家秘密的信息为敏感信息。

信息安全技术 行业间和组织间通信的信息安全管理

1 范围

本文件提供了信息安全管理体系（ISMS）标准族的补充指南，用于在信息共享团体中实现信息安全管理。

本文件为行业间和组织间通信提供了有关发起、实现、维护与改进信息安全的控制和指南。它为如何使用已建立的消息传递和其他技术方法满足规定要求提供了指南和通用原则。

本文件适用于行业间和组织间各种形式的敏感信息交换与共享。特别的，本文件可适用于与组织或国家关键基础设施的供给、维护和保护相关的信息交换与共享[2)]。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 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）

GB/T 22081—2016 信息技术 安全技术 信息安全管理实践指南（ISO/IEC 27002:2013,IDT）

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）

3 术语、定义和缩略语

3.1 术语和定义

GB/T 29246—2017 界定的术语和定义适用于本文件。

3.2 缩略语

下列缩略语适用于本文件：

CVE：公共漏洞和披露（Common Vulnerabilities & Exposures）

IPR：知识产权（Intellectual Property Right）

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

ISMS：信息安全管理体系（Information Security Management System）

P2P：对等通信（Peer to Peer）

TICE：可信信息通信机构（Trusted Information Communication Entity）

TLP：交通信号灯协议（Traffic Light Protocol）

WARP：预警、建议及报告点（Warning, Advice and Reporting Points）

4 概念和释义

2) 本文件旨在支持在敏感信息交换与共享时建立信任，从而促进信息共享团体的国际化发展。

4.1 简介

本文件第 5 至 18 章给出了针对行业间和组织间通信的信息安全管理体系（ISMS）指南。

GB/T 22081—2016 定义的控制涵盖了组织间信息交换的控制，以及公开可用信息的通用分发控制。当在组织的团体内共享敏感的且仅限于团体成员公开可用的信息时，通常要求信息仅对团体内特定个人可用或信息匿名。为满足上述要求，本文件定义了附加的控制，并提供了对 GB/T 22080—2016 和 GB/T 22081—2016 的附加指南和解释。

本文件包含五个附录，附录 A 给出了组织之间共享敏感信息的潜在好处；附录 B 提供了一份指南，该指南给出了信息共享团体成员如何评估其他成员提供信息的信任程度；附录 C 给出了交通灯协议，这是一种在信息共享团体中广泛使用的机制，用于表示允许的信息分发；附录 D 给出了一些用于组织信息共享团体的模型的示例；附录 NA 给出了 GB/T 32920—XXXX 与 GB/T 32920—2016 控制的对应关系；附录 NB 给出了 GB/T 22081—2016/ISO/IEC 27002:2013 与 ISO/IEC 27002:2022 控制的对应关系。

4.2 信息共享团体

信息共享团体成员需具有共同利益或其他关系（诸如团体的成员都属于特定行业，或者团体成员具有相同的地理位置或所属关系），明确共享敏感信息的范围，才可有效运行。

团体成员之间应相互信任，并共同遵守信息共享协议（协议内容见附录 A 中 A.6）的约定。

4.3 团体管理

信息共享团体可创建于独立组织或组织的一部分。团体需对信息安全管理做出承诺，宜明确定义团体信息安全管理的组织架构和管理职能。

宜考虑信息共享团体中成员之间的差异，主要包括：

——不同的法律法规环境；

——成员是否已经运行 ISMS；

——成员关于资产保护和信息披露的规则。

4.4 支持性机构

信息共享团体可选择建立或者指定集中的支持性机构来进行信息共享。支持性机构可为信息共享提供信息安全控制（如来源方和接收方匿名）。通过支持性机构进行信息共享比成员间直接通信更方便有效。

目前存在许多不同的、可用于建立支持性机构的组织模型。附录 D 描述了两个通用模型，即可信信息通信机构（TICE）和预警、建议及报告点（WARP）。

4.5 行业间通信

当在已有信息共享团体基础上，再一次基于共同利益(如共享信息的自然属性)建立信息共享团体，即为行业间通信。

支持性机构为行业间通信提供了有效支撑，一方面通过支持性机构建立了信息交换协议和控制，另一方面满足了某些行业间通信所要求的来源方或接收方匿名。

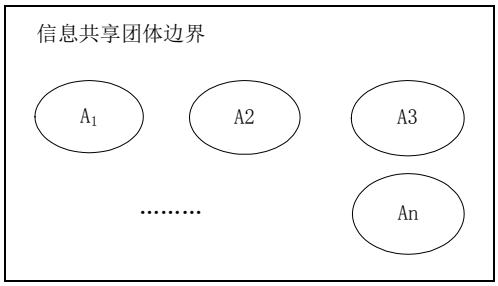
4.6 符合性

GB/T 22080—2016 在应用于信息共享团体（或行业间通信，即基于不同团体而建立的团体）时，有许多需要解释的地方。

首先需要解释的是本文件中所涉及组织的定义。

GB/T 22080—2016 要求 ISMS 由组织建立、实现、维护和持续改进（GB/T 22080—2016，4.4）。在

此环境中，相关组织就是信息共享团体。同时，信息共享团体的成员自身也是组织，如图 1 所示。



说明：

A_k：团体的成员 k（k=1…n），包括所有支持性机构。

图 1　团体与组织

其次，在信息共享团体中，并不是团体成员中的所有人员均可访问成员间共享的敏感信息。在此情况下，成员的一部分包含在团体 ISMS 范围内，一部分则在团体 ISMS 范围之外。团体 ISMS 范围外的成员仅可访问被标记为广泛发布的团体信息，如图 2 所示。

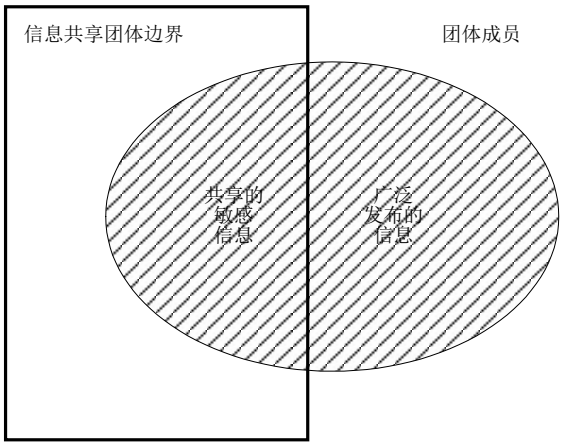


图 2　团体成员的一部分在范围内

当信息共享团体的成员有自己的信息安全管理体系时，其中某些过程将同时属于团体和成员两者管理体系的范围之内，此时这些过程可能存在冲突和不兼容，需将这些过程从成员的 ISMS 范围中排除——具体见 GB/T 22080—2016，4.3。

在定义信息共享团体的风险评估过程时（GB/T 22080—2016，6.1.2），需要认识到风险对不同的团体成员影响不同。因此，团体需要选择一种可处理不一致影响的风险评估方法。对于风险评估准则的选择也是如此。

4.7　通信模型

本文件中敏感信息通信可采用书面、口头或电子等各种形式。

本文件中敏感信息通信涉及的参与方主要包括：

——来源方：信息产生的人员或组织。

注：来源方不需要是团体成员。

——发起方：在信息共享团体内启动信息分发的团体成员。发起方可直接分发或通过支持性机构分发信息。信息发起方可以与来源方相同，也可不同。发起方需隐藏来源方的身份。团体需提供便利，以使成员能隐藏其作为发起方的身份。

——接收方：信息共享团体内分发信息的接收者。对标记为广泛分发的信息，接收方不需要是团体成员。团体需提供便利，以使接收方对信息发起方隐藏其身份。

5 信息安全策略

5.1 信息安全管理指导

5.1.1 信息安全策略

GB/T 22081—2016 中 5.1.1 的控制增加如下：

实现指南

信息共享方针宜定义团体成员如何共同制定信息共享团体的安全管理策略和指导。它宜对团体内参与信息共享的所有人员可用。该方针可限制向团体成员中未参与信息共享的人员传播。

信息共享方针宜定义团体范围内使用的信息标记和分发规则。

5.1.2 信息安全策略的评审

GB/T 22081—2016 中 5.1.2 的控制增加如下:

实现指南

评审宜包括信息共享团体成员重大变化的信息。

6 信息安全组织

针对行业间和组织间通信没有附加特定的控制。

7 人力资源安全

7.1 任用前

7.1.1 审查

GB/T 22081—2016 中 7.1.1 的控制增加如下：

实现指南

审查规则对于信息共享团体全部成员不完全一致。对于可访问共享团体信息人员或承包商，团体宜考虑界定适用于他们的验证核查的最低级别。

7.1.2 任用条款和条件

针对行业间和组织间通信没有附加特定的控制。

7.2 任用中

针对行业间和组织间通信没有附加特定的控制。

7.3 任用的终止和变更

针对行业间和组织间通信没有附加特定的控制。

8 资产管理

8.1 有关资产的责任

8.1.1 资产清单

针对行业间和组织间通信没有附加特定的控制。

8.1.2 资产的所属关系

针对行业间和组织间通信没有附加特定的控制。

8.1.3 资产的可接受使用

GB/T 22081—2016 中 8.1.3 的控制增加如下：

实现指南

信息共享团体成员提供的信息是一项资产，宜按照信息共享团体或信息发起方制定的规则进行保护、使用和传播。

8.1.4 资产归还

针对行业间和组织间通信没有附加特定的控制。

8.2 信息分级

8.2.1 信息的分级

GB/T 22081—2016 中 8.2.1 的控制修改如下：

控制

信息宜按照法律要求、价值、可信性、优先级、重要性和其对未授权泄露或修改的敏感性进行分级。

实现指南

除了 GB/T 22081—2016 给出的分级准则，信息宜按照它的可信性和优先级进行分级。可信性宜按照信息来源的信誉、技术内容和描述质量来评估。优先级宜表明紧急或立即采取行动（例如进一步分发）的必要性。

同样的，敏感性取决于除维护信息保密性之外的很多方面，如信息泄露的影响或损害信息来源方匿名的可能性。

在解读信息共享团体成员的分级标记时宜注意其含义[3)]。

8.2.2 信息的标记

针对行业间和组织间通信没有附加特定的控制。

8.2.3 资产的处理

针对行业间和组织间通信没有附加特定的控制。

8.3 介质处理

针对行业间和组织间通信没有附加特定的控制。

8.4 信息交换保护

GB/T 22081—2016 第 8 章，资产管理，附加的控制目标为：

目标：确保信息共享团体信息交换得到充分保护。

即使成员是采用不同方式标记、分发、保护自身信息的独立组织或组织的一部分，仍宜采取一致的

3) 例如当收到敏感头字段被设置为“公司保密”（RFC 4021[1]）的电子邮件时，常见的电子邮件客户端将会显示消息“请按保密信息处理”。在这种情况下，发起方的本意究竟是指“公司保密”（如果是指“公司保密”，则该消息已被错误的发送）还是指“对收件人保密”，指代不明确。

方式保护信息共享团体成员间交换的信息。

当要求匿名时，宜移除可识别信息交换来源方的相关信息。同样的，宜在不泄露接收方身份的情况下接收共享的信息。

宜控制团体之外共享信息的发布。

8.4.1 信息传播

控制

基于团体确定的预设传播标记，宜限制接收成员间的信息传播。

实现指南

对于未分配传播标记的信息，宜给予团体确定的默认传播标记。如果有疑问，或者没有可普遍接受的默认传播协议，信息宜谨慎处理。必要时，接收方宜请求发起方重新传送具有明确传播标记的信息。

传播限制可包括诸如控制电子复制与粘贴、防止截屏截图、阻止打印与输出等。

其他信息

共享信息因信息属性及组成部分的不同而具有不同的敏感性。特别的，消息中包含的知识和共享信息因内容不同而有不同的敏感性。

信息权限管理功能通常用于强制执行使用中的限制。此时需要一个清晰的用户权限策略或模型以使用户理解什么是体系允许他们做的，什么是体系限制他们做的。

8.4.2 信息免责声明

控制

每次信息交换宜从免责声明开始，除正常信息标记外，声明中宜列出接收方需要遵从的特殊要求。

实现指南

如果接收方不能充分理解免责声明，则宜要求发起方作出澄清，否则该声明无法实施。

8.4.3 信息可信性

控制

每次信息交换宜指出发起方对所传送信息的可信性和准确性方面的可信程度。

实现指南

基于紧迫性、潜在后果和技术限制，无法在信息传送前验证所有信息的可信性，宜在信息中阐明此局限性。

信息来源方匿名或未知的情况下，对信息可信性（见附录 B）可持保留意见，并需要指出发起方在何处能够验证直接提供的信息并保证其真实性。

8.4.4 信息敏感性降低

控制

信息交换的发起方宜指出，经过一些外部事态或一段时间后，提供信息的敏感性是否降低。

实现指南

即使提供信息的敏感性随时间降低，信息仍需保护。分级指南（见 8.2.1）需包含针对敏感性降低的默认控制措施。

8.4.5 来源方匿名保护

控制

团体成员在发起或接收的有匿名要求的通信中，宜移除来源方的相关标识信息。

实现指南

向信息共享团体成员传递信息前，信息发起方负责从来源方（当来源方与发起方不同时）获得批准。发起方还宜询问来源方，是否可以将其标识为信息的原始提供方。

由于对消息内容进行分析可能泄露来源方身份，因此来源方保护既要关注消息的来源，也要关注消息的内容。如果有可能，消息发起方在消息分发前，宜请求消息来源方对匿名信息和目标接收方名单进行审查[4)]。

可采取不破坏匿名性的情况下保证数据真实性的技术机制，如采用共享的加密秘钥，在不泄露发起方真实身份情况下，用于确认发起于团体成员的通信。

8.4.6 接收方匿名保护

控制

征得发起方同意，团体成员宜在不泄露自己身份的情况下接收通信。

实现指南

匿名接收可通过技术手段（如加密）和规程手段（如通过支持性机构进行路由）实现。必须注意确保匿名不违反法律规定或降低团体的整体信任级别。

其他信息

行业团体需要保持成员关系详细信息的私密性，因此行业间通信需要对接收方匿名保护。

8.4.7 进一步发布授权

控制

除非信息被标记为广泛发布，否则未经发起方正式批准，信息分发不宜超出信息共享团体。

实现指南

信息进一步分发前，接收方宜负责从发起方获得信息广泛发布的必要授权。

在行业间通信中，发起方无法确认将要接收信息的所有接收方时，需要授予通用的或特定行业发布的批准。

其他信息

交通灯协议（见附录 C）通常用于指示如何在不寻求附加批准的情况下，进一步分发信息。

9 访问控制

针对行业间和组织间通信没有附加特定的控制。

10 密码

10.1 密码控制

10.1.1 密码控制的使用策略

GB/T 22081—2016 中 10.1.1 的控制增加如下：

实现指南

密码技术可通过诸如信息权限管理用于实现信息共享的传播规则。

10.1.2 密钥管理

4) 例如，对于消息“一种防火墙未检测到但被策略服务器检测到的新病毒导致自助提款机今天不能正常工作”，如果当天只有一家银行遭遇了公共服务中断问题，那么这条消息就可能泄露来源方。

针对行业间和组织间通信没有附加特定的控制。

11 物理和环境安全

针对行业间和组织间通信没有附加特定的控制。

12 运行安全

12.1 运行规程和责任

针对行业间和组织间通信没有附加特定的控制。

12.2 恶意代码防范

12.2.1 恶意软件的控制

GB/T 22081—2016 中 12.2.1 的控制增加如下：

实现指南

无论团体成员间的通信服务是否进行信息扫描，从其他团体成员接收的信息宜进行扫描以确定是否存在恶意软件。

12.3 备份

针对行业间和组织间通信没有附加特定的控制。

12.4 日志和监视

12.4.1 事态日志

GB/T 22081—2016 中 12.4.1 的控制增加如下：

实现指南

当信息共享团体要求时，成员宜记录共享信息的内部传播情况。

12.4.2 日志信息的保护

针对行业间和组织间通信没有附加特定的控制。

12.4.3 管理员和操作员日志

针对行业间和组织间通信没有附加特定的控制。

12.4.4 时钟同步

针对行业间和组织间通信没有附加特定的控制。

12.5 运行软件控制

针对行业间和组织间通信没有附加特定的控制。

12.6 技术方面的脆弱性管理

针对行业间和组织间通信没有附加特定的控制。

12.7 信息系统审计的考虑

12.7.1 信息系统审计的控制

针对行业间和组织间通信没有附加特定的控制。

12.7.2 团体审计权

GB/T 22081—2016 中 12.7，信息系统审计的考虑，附加的控制为：

控制

信息共享团体宜规定其成员审计其他成员的系统和可信服务提供商系统的权利。

实现指南

对成员系统审计的授权可仅限于可信第三方，如 TICE 或 WARP。

13 通信安全

13.1 网络安全管理

针对行业间和组织间通信没有附加特定的控制。

13.2 信息传输

13.2.1 信息传输策略和规程

针对行业间和组织间通信没有附加特定的控制。

13.2.2 信息传输协议

GB/T 22081—2016 中 13.2.2 的控制增加如下：

实现指南

信息共享团体宜定义信息传输协议，同时宜仅允许签署和接受协议的成员加入团体。

13.2.3 电子消息发送

GB/T 22081—2016 中 13.2.3 的控制增加如下：

实现指南

信息共享团体宜定义用以保护传输信息的规则，同时宜仅允许接受和实现这些规则的准成员加入团体。所有支持性机构宜内部实施这些规则。

信息共享团体宜实现不依赖于电子消息发送的信息共享替代机制，且推动成员规定特定消息由这些替代路径分发。

13.2.4 保密或不泄露协议

针对行业间和组织间通信没有附加特定的控制。

14 系统获取、开发和维护

针对行业间和组织间通信没有附加特定的控制。

15 供应商关系

15.1 供应商关系中的信息安全

15.1.1 供应商关系的信息安全策略

针对行业间和组织间通信没有附加特定的控制。

15.1.2 在供应商协议中强调安全

GB/T 22081—2016 中 15.1.2 的控制增加如下：

实现指南

为避免团体成员对参与处理其所提供信息的特定第三方有异议，团体成员宜了解参与提供团体服务的第三方身份。

团体与供应商及服务提供方之间的协议，宜明确对他们的服务定期实施安全评审和审计。

15.1.3 信息与通信技术供应链

针对行业间和组织间通信没有附加特定的控制。

15.2 供应商服务交付管理

针对行业间和组织间通信没有附加特定的控制。

16 信息安全事件管理

16.1 信息安全事件的管理和改进

16.1.1 责任和规程

针对行业间和组织间通信没有附加特定的控制。

16.1.2 报告信息安全事态

GB/T 22081—2016 中 16.1.2 的控制增加如下：

实现指南

信息共享团体成员宜考虑是否向其他成员报告检测到的事态。团体宜协商一致并发布对其他成员有价值的事件类型指南。团体成员宜只报告对其他成员有价值的潜在事态。

为了保护发起方的信誉，需保持事件保密性且不允许团体成员泄露事件信息。然而将事件信息传递给其他成员将促进未来在事件预防和事件及时快速响应方面的合作与协调，并将改进团体整体安全性。因此，在无需透漏事态和事件的后果前提下，可以将其报告给其他成员。

同样，成员宜及时检查报告的事态，以查看它们是否将会对自己的操作产生影响。

注：例如提供维护操作的共享服务的成员例行公告中，可要求其他成员在维护活动开始之前评审替代供应商的可靠性。

16.1.3 报告安全弱点

针对行业间和组织间通信没有附加特定的控制。

16.1.4 信息安全事态的评估和决策

针对行业间和组织间通信没有附加特定的控制。

16.1.5 信息安全事件的响应

针对行业间和组织间通信没有附加特定的控制。

16.1.6 从信息安全事件中学习

GB/T 22081—2016 中 16.1.6 的控制增加如下：

实现指南

宜基于信息共享团体分发信息，由相关团体成员或支持性机构（如果存在）对信息安全事件进行调查，以降低类似事件的风险，并且更好的了解面向团体和所有相关重要信息基础设施的风险。

即使成员未受到有问题事件的影响，信息共享团体成员在报告事件后仍宜实施事后评审，以制定安全事件响应规划、相关规程，并对业务风险配置进行更新。每个成员宜确保对所报告的事件响应进行了评估，也宜确保识别了针对成员自身响应过程的经验或可能的改进，以不断完善其响应过程。

16.1.7 证据的收集

针对行业间和组织间通信没有附加特定的控制。

16.1.8 预警系统

GB/T 22081—2016 中 16.1，信息安全事件的管理和改进，附加的控制为：

控制

宜在信息共享团体内部署预警系统，以及时有效地传递可用的优先信息。

实现指南

优先信息是可使团体成员避免或最小化类似不良事态的信息。重要的是，即使没有经过充分的分析和确认，这类信息也急需共享。

17 业务连续性管理的信息安全方面

17.1 信息安全的连续性

17.1.1 规划信息安全连续性

GB/T 22081—2016 中 17.1.1 的控制增加如下：

实现指南

信息共享团体成员制定的业务连续性和灾难恢复计划宜满足与其他成员以安全方式交换敏感信息的需求，并将其作为恢复过程的一部分。

17.1.2 实现信息安全连续性

针对行业间和组织间通信没有附加特定的控制。

17.1.3 验证、评审和评价信息安全连续性

针对行业间和组织间通信没有附加特定的控制。

17.2 冗余

针对行业间和组织间通信没有附加特定的控制。

18 符合性

18.1 符合法律和合同要求

18.1.1 适用的法律和合同要求的识别

GB/T 22081—2016 中 18.1.1 的控制增加如下：

实现指南

信息共享团体宜考虑所有与信息共享有关的协议、法律和法规（如反垄断相关法律或法规）。这可阻止特定组织加入团体或对它们的代表加以限制。

18.1.2 知识产权

针对行业间和组织间通信没有附加特定的控制。

18.1.3 记录的保护

针对行业间和组织间通信没有附加特定的控制。

18.1.4 隐私和个人可识别信息保护

针对行业间和组织间通信没有附加特定的控制。

18.1.5 密码控制规则

针对行业间和组织间通信没有附加特定的控制。

18.1.6 信息共享团体的责任

GB/T 22081—2008 中 18.1，符合法律和合同要求，附加的控制为：

控制

信息共享团体成员宜阐明、理解及批准责任问题及补救措施，以处理信息被有意或无意泄露的情况。

实现指南

补救措施至少宜包括向发起方反馈未授权的泄露，并提供细节来识别泄露的信息。

即使信息已经得到清理且不会泄露其来源方，仍宜将其反馈给来源方。这可通过可信第三方作为中介（如 TICE）来实现。

未授权泄露的后果可能直接影响责任方，为重建团体信任，在一段时间内可排除或限制某些成员的访问。

18.2 信息安全评审

针对行业间和组织间通信没有附加特定的控制。

附 录 A
（资料性）
共享敏感信息

A.1 概述

敏感信息作为一种有重要价值的资产，在组织间共享时需对其加强安全管理。当业务需要或敏感信息对组织非常关键时，应及时传递敏感信息，以更好的解决业务问题并作出决策。

信息共享团体可代表多种类型的组织或者个人。团体成员多种多样，可来自于各种行业，其与特定行业的业务活动密切相关。团体成员的共同期望是，在团体内共享敏感信息，并通过协商好的控制和过程加强敏感信息使用的治理。

为在信息共享团体内安全的交换敏感信息，有必要设计、实现和监视过程以及时提供安全的信息流动。这些过程宜确保信息传递给合适的人，不会被用于恶意目的，不会被任意再分发而变成实质上公开的信息。

分发的有效性取决于信息共享团体成员间信任程度。同时，宜采取相关安全控制防止信息分发给如下个人或组织：

——使用或积累数据实施恶意行为的；

——未经信息发起方允许而公开传播信息的；

——提供未经充分分析的信息，因此导致可能浪费或误导资源的不当行为，并对组织产生影响的。

为了使信息共享团体有效运行，团体成员需授权信息接收方可根据接收到的信息进行相关处置，且信息接收方不得滥用这些信息（如用于获得商业利益）。

A.2 挑战

为了应对以下挑战，需加强行业间和组织间通信的信息安全管理，防止影响正常的业务状况并在事件发生时导致业务中断：

——新的安全威胁和漏洞；

——对系统与网络日益增长的依赖性；

——合同、法律法规和业务的发展与限制；

——恰当的通信模型的建立；

——攻击和响应过程之间的协调；

——持续的治理。

团体成员间安全的和适应力强的通信宜包括下列要素：

——风险知识和风险管理；

——传播和通信；

——监视。

这三项要素各有其特定的价值，它们之间紧密联系、相辅相成。

团体成员代表之间良好的个人关系有助于团体成员间更好地建立信任。面对面的交流有助于建立个人关系，有助于增强对彼此可信性和判断力的信心，而仅使用远程通信技术很难建立信任。然而既要求信息来源方匿名，又要求信任信息来源方，二者无法兼顾。通常，只有在确信自己的身份信息不会泄露前提下，才能更好的进行交流。

信息共享团体并非所有成员间都进行信息共享，信息分发可仅限于团体特定成员或限于某一主题。

最后，当团体间共享信息时（如行业间通信），团体间的信息传递者面临着如下特殊困难[5)]：

5) 与行业间通信相比，这些问题通常在国际交流中显得更为突出。

1）信息来源方不了解其他团体的成员身份，必须依靠接口来保护匿名及达到其他发布条件；

2）信息传递者由于缺乏专业知识而无法确认何时不宜再进一步进行团体通信。

A.3 潜在效益

虽然信息共享团体内成员共享敏感信息增加了信息不当泄漏的风险，但可通过有效管理风险使其对团体影响最小化。

共享敏感信息的潜在效益包括：

——风险环境中相关重大变化的风险预警，如新威胁、攻击更新的可能性、最新发现的漏洞等等；

——通过共享最佳实践提高安全性；

——访问从公开渠道不能得到的一些有用信息；

——通过消除重复工作节约成本；

——通过更好地了解威胁和脆弱性来更有效的进行风险评估；

——从其他组织类似活动涉及的信息中，更好的组织开展维护及干预活动；

——更好的防范安全事件；

——与类似组织进行安全措施的基准测试；

——企业社会责任；

——符合法律要求或企业方针策略。

团体宜监视和评审作为团体成员的具体效益（和缺点），以供成员评估他们是否继续成为团体成员时使用。

A.4 适用性

信息交换可在不同类型的组织间进行（如大型或小型的，政府或私人的，相似或不同的）。敏感信息共享尤其适用于在同一行业或具有共同目标的组织间，在分担特定行业的信息安全风险同时，可获得较好的效益。GB/T 25067[2]确定了一些这样的行业。

信息共享还适用于行业之间、通过基于其他特征（如地理位置）确定的团体之间、分层结构的团体中基于行业的团体之间，此时也可获得较好的效益。

A.5 定义和运行一个信息共享团体

信息共享团体宜定义治理其运行的规则和条件，这些规则和条件宜包括：

——治理信息共享团体的成员关系及其内部组织的规则和条件；

——信息共享团体的目标和给成员的预期效益；

——成员加入或退出信息共享团体的程序；

——治理集中式团体过程或机构（如 TICE 或 WARP）的规则和条件；

——有关团体成员义务、纪律处分和开除的过程与准则的规则和条件；

——针对成员如何使用和传递共享信息的清晰规则；

——团体成员的其他法律及财务方面的义务和条件。

信息共享团体的这些规则和条件还宜：

——确保以高效和安全的方式（这种方式确保目标受众恰当及时的接收数据）传递信息；

——针对已识别的信息类型，根据传输其数据时信道的优先级，确定通信信道及其优先级；

——规定允许将信息传递给团体成员的情况；

——规定与团体通信相关的数据保护及分发属性（包括可选的和必选的）；

——对于与信息传递有关的数据保护及分发属性，制定明确的解释规则；

——要求成员提供关于已接收信息相关性、及时性和准确性方面的反馈；

——必要时，规定或调整现有的消息交换标准。

通信规则宜定义通信的频次、接收确认的要求以及优先级或升级准则。通信过程中，信息共享团体不同成员间的信任级别不同，并随时间和情况的变化而变化。

宜基于诸如目标受众、传递信息的属性、信道的覆盖面和频次、成本等准则，通过评估优缺点为团体信息传递选择合适的通信信道（例如电子消息发送、公共网站或会员网站、会议或双向通话、公共邮政服务发送的信件或面对面会议等）。通信对目标受众的影响取决于信道覆盖受众的有效性、通信对受众的可信性、通信对问题或信息主题的适宜性等。

信息共享过程中，有些信息需要实时传递，有些信息可通过日常结果进行共享。

何时将信息传输给团体成员的情况示例包括：立即报告检测到的符合预设配置文件的事件、定期报告或响应来自其他成员的信息请求。数据保护和分发属性的示例包括：隐藏信息来源方的要求、信息的敏感性或发起方对信息可信度评估。解释数据保护和分发属性规则的示例是交通灯协议（TLP），见附录C。相关属性因通信信道不同而不同（例如邮政分发的必选属性与互联网邮件的必选属性不同）。

无论选择和实施何种技术解决方案，它们宜与团体内共享信息类型相符合，并与定义的团体目标相一致。面对面的接触交流可以更好的建立信任，并通过邀请新成员加入团体使团体规模不断扩大。团体本身可信平台及其他共享基础设施的存在也可促进团体的快速发展。

A.6 信息交换协议

信息共享团体宜在信息交换协议中定义治理团体通信的机制和过程。信息可通过信件、面对面会议口头交流及电子形式进行交换，可使用预定义的格式和协议进行正式交换，或以非结构化的方式进行非正式交换，可进行例行或特定的交换，也可通过点对点通信、分层结构或通过集中式的支持性机构（如TICE或WARP）进行交换。

信息交换协议可仅允许信息与选定的团体成员共享，也可仅允许信息在成员间直接传递（即使存在集中式报告设施），或者仅可匿名共享。

信息交换协议宜规定可在团体成员间交换的信息类型，以确保团体成员就交换的信息达成共识，并确保成员根据共享信息的敏感性级别设计和实施适合的安全措施。

信息类型的示例包括：

——“公告”，对应于告知性的解释事态；

——“警报和预警”，对应于无法解释的物理事态或IT相关事态、拒绝服务攻击、扫描或欺骗；

——“事件处理”，对应于与实际事件相关的分析、响应支持和响应协调；

——“信息请求”，对应于团体成员之间发出的信息请求；

——“服务质量预测”，提供团体通信信道有效性和可靠性预测的信息。

需要采用一种合适的数据过滤方法，否则信息共享过犹不及。当采用能够区别高优先级和低优先级信息的方法时，构建趋势信息将是信息共享的一大效益。

A.7 成功因素

信息共享团体成功因素包括：

1）信息共享团体成员具有共同利益（例如固网电信公司和移动公司都对识别骗局电话感兴趣）；

2）团体成员可借助授权代表使事情发生在内部；

3）团体可限制成员资格，例如确保决策中的公平代表权。

A.8 信息共享团体的ISMS范围

信息共享团体的ISMS范围宜包括：

——用于团体成员（包括中介机构）信息通信的所有过程；

——通信过程相关的信息存储；

——由相关成员实现的发送和接收共享信息的过程；

——由团体成员实现的销毁共享信息的过程。

除了附加在共享信息的自然属性和信息共享系统接口上的限制外，ISMS范围不宜包括相关团体成员管理自身信息安全所实现的信息安全管理过程，以及可能被其他信息安全管理体系所覆盖的信息安全管理过程。ISMS可由支持性机构（如TICE或WARP）进行集中管理，也可由团体成员协作管理。

附 录 B
（资料性）
信息交换中建立信任

B.1 信任声明

接收方对收到声明的信任程度，主要取决于信息接收方对来源方的信任程度和信息来源方对声明的信任程度。

用于执法机关和情报机构的“5*5”模型是对此最好的概括：

——｛A--E｝信息接收方对来源方信任程度的递减；

——｛1--5｝信息来源方对信息信任程度的递减。

因此，“A-1”信息是绝对可信的，而“E-5”信息通常将被废弃。

显而易见，在现实世界中，“A-1”信息非常少。虽然期望来源方和信息都是绝对可信的，但现实中总是存在偶然性误差[6)]。

关于信任声明的另一个问题是华而不实的增强信任所带来的风险。目前存在一种可证实的内在趋势或潜在假设，即同一信息（看似具有不同来源）的多个实例是确定的。

信任不能仅从字面上去理解，特别是，这种信任的数学模型不宜为附加的实例分配线性权重。

B.2 技术支持

B.2.1 概述

目前已开发出多种技术，以支持对未知的或不熟悉的机构以电子方式提供信息的信任。这些技术同Web 2.0[3]的概念密切相关。

注：Web 2.0不是一组技术，它是一个与社交媒体有关的理论或概念，它融合了一些理念，将Web用作一个平台，利用集体智慧，共同创造（用户生成）内容、Web的社交用途等。

Web 2.0 中以下两个方面与本文件密切关联：

——伪匿名；

——信誉系统。

B.2.2 匿名和伪匿名

由于各种各样的原因，信息来源方和接收方都要求匿名。匿名实际能达到的强度取决于对背景的认知即对整个消息传递系统的了解。在大型、分散式的系统中，参与者无法完全了解整个消息传递系统，同时，消息的背景会随着时间而变化。

匿名的概念与**不可链接性**的概念紧密联系在一起，即观察后得到的感兴趣项目之间的关联与从先验知识中得到的感兴趣项目之间的关联是一样的。

关系匿名意味着通信双方一定程度上的不可追溯性，因此，不可能将发起方与其接收方关联起来。

不可观察性是指当发起方发送和接收方接收时，不能进行观察。

关系不可观察性意味着不能观察发起方和接收方之间的通信。

伪匿名或笔名涉及用标签代替个人姓名和其他身份特征，以阻止识别数据主体。**假名化**是使用伪匿名或笔名作为标识标签的一种状态。

有关可链接程度，各种类型的笔名可以是：

a）个人笔名：个人笔名被看作姓名（代表持有人公民身份）的替代品。它可用于各种环境中，例

6) 最著名的例子就是在基于卫星导航系统的全球定位系统（GPS）的使用中，地图定位或路线规划系统误差的偶然失灵，导致大型交通工具被误导开到了小型车道上，由此经常成为新闻中“轻松幽默”栏目的材料。

如身份证号码、DNA、昵称、演员的艺名或移动电话号码等。

b）角色笔名：角色笔名的使用限于特定的角色，例如客户的笔名或同一“因特网用户”的多个Internet 账户角色笔名。相同的角色笔名可用于不同的通信合作者。

c）关系笔名：针对不同的通信合作者，使用不同的笔名。这意味着不同的通信合作者不能分辨他们是否在与同一用户通信。

d）角色关系笔名：对于不同的角色和不同的通信合作者，使用不同的角色关系笔名。这意味着通信合作者无法确认用于不同角色的两个笔名是否属于同一持有者；另一方面，与同一用户相同角色交互的两个不同通信合作者，仅从笔名不知道相同角色的用户是否是同一用户[7]。

e）事务笔名：对每一项事务，使用与所有其他事务笔名不可链接的事务笔名（且至少在开始时与所有其他事务笔名不可链接），例如，随机生成的网上银行事务号码。因此，可使用事务笔名实现强匿名要求。

总的来说，角色笔名和关系笔名的匿名性强于个人笔名。匿名的强度随着角色关系笔名应用的增强而增强，但角色关系笔名的使用仅限于相同角色和相同关系。

笔名持有者与笔名有关的个人数据越少，匿名性越强。

B.2.3 信誉系统

信誉系统是构成 Web 上许多社交媒体和社交网络的基础，其用于筛选与之关联度最高的信息，且随着信息数量和信息种类的不断增加，信息的关联度变得越来越高。

信誉系统是一组策略和规程，用于根据个体过去的活动计算信誉分数。在网络世界中，信誉系统与数字足迹（即数字环境中追溯某人活动的痕迹）的概念紧密联系在一起。

信用报告提供了一种量化信誉的方法，相比传统信用报告，Web 信誉机制（如 Internet 拍卖评级）更令人关注。当在 Web 上交易（买、卖、借、还）时，产生了数字数据。

注：尽管此数据属于个人，但它由信用评级机构所拥有（事实上，个人为了获取它们需要支付费用）。

现在已经有越来越多形式完善的信誉系统。例如 eBay 信誉系统，由于它是透明的，因此它不同于信用分数。每一个反馈(包括负反馈)都会反馈给评论的当事人，因此这也提供了一个申诉的机会。

信誉系统可通过确认新的信息来源方、确认内容来源方、实时告警（诸如 Twitter 搜索和 Google 告警）、增强未知来源方的信任、通过外部见解补充搜索、为可信共享域引入新的或外部思想、预测来自外部来源方的机会与威胁等任务，融合更广泛团体来源方的见解来增加信任。然而，目前 Web 2.0 的许多技术（如 wikis）由于内部没有一个强健的信任模型，因此在建立信任时存在限制。

B.3 评估信息的可信度

支撑信任的概念本质上是主观而非客观的，就这点而论，它未必符合其机械的表述。虽然如此，一种Pareto方法[4]可用于解决上述问题:这种方法只需要付出相对少的努力就可获得大部分的期望结果，而要解决全部问题，完善整个模型需要付出与收获不成比例的努力。

这种方法的组成部分包括：

a）信息的发起方宜在他们发布的信息中赋予信任等级[8]。

b）理想情况下，宜使用结构化数据格式标识信息来源方。

c）宜支持匿名报告（因为安全领域的经验表明，提供匿名服务可有效推进信息共享）。

d）边界对象：用于封装信息交换的内容。边界对象是信息的结构化组合，在团体内是成员相互认可的，可推动跨语言和域边界的通信（例如 Mitre 的公共漏洞和暴露（CVE）标记的成功，在一

7） 例如，假设信息源在非公共领域与张三进行信息通信时经常使用“甲”这个名字，而与李四进行相同的信息通信时使用“乙”。后张三和李四各自分别从“丙”和“丁”接收了关于某个新课题的信息。张三和李四不知道“丙”和“丁”是否是同一人，也不知道“丙”是否与“甲”或“乙”是同一个人，或与后两者都是同一个人。

8） 该方法的有效性已得到英国国家基础设施保护中心确认，并用于自动配置和分发预警信息给各类信息共享团体。

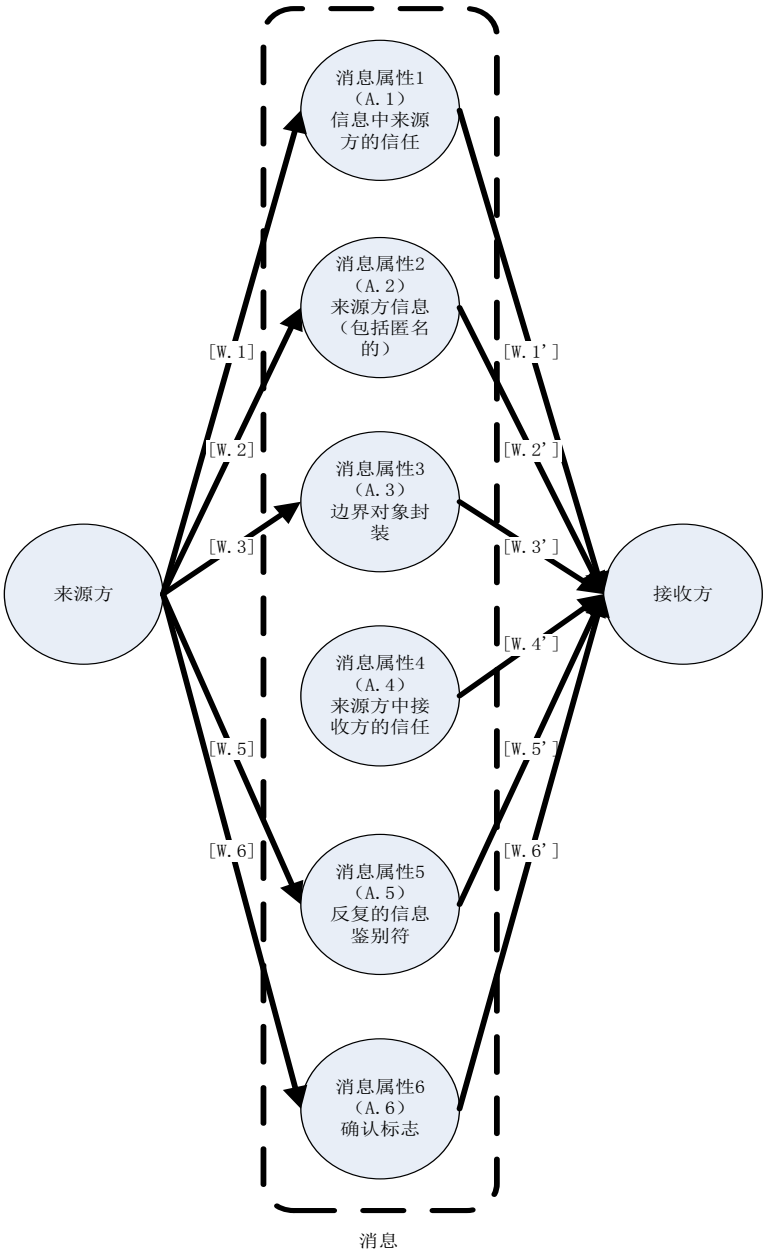
定程度上要归功于其实际采用了这种边界对象）。

e）可信信息交换的发起方和接收方都宜提供一份关于信息是否支持以前所接收的内容以及支持次数的评估：在当前最新技术下为此目的进行的自动信息分析是不可靠的。为了最小化似是而非的增强信任所带来的风险，需要将回报递减的累积分布函数用于以前实例的计数，这意味着附加信息的加权值随着计数值的增大而减小。

f）来源方或接收方就信息是否已独立经过确认的问题为信息赋予一个标志。

g）信息接收方宜基于 5*5 模型（见 B.1）对信息来源方进行主观评价。

信息共享团体成员可以将这些准则经过适当的加权后量化信任，得到的信任量化值宜加入从团体其他成员处收到的信息中，如图 B.1 所示。



说明

W.n:发起方对消息中信息可信性的判断

W.n′:接收方对消息中信息可信性的判断

图 B.1 消息内容可信性的评估

附 录 C
（资料性）
交通灯协议

此附录描述了交通灯协议（TLP），其广泛用于信息共享团体用以指示允许的信息分发。尽管交通灯协议的基本概念众所周知，但在协议使用中存在许多细微的不同变化[9)]。

TLP 的创建是为了鼓励不同组织间更多的共享敏感信息。发起方需表明除了直接接收方外希望信息传播范围的大小。

TLP 基于如下概念：信息发起方使用四种颜色中的一种对信息进行标记，以在需要时指出信息接收方可以进行何种传播。当需要更广泛的传播时，接收方必须询问发起方。

四种颜色及其含义如下：

——“红色”-仅限于指定的接收方个人。例如在会议中，“红色”信息仅限于到会人员。在大多数情况下，“红色”信息将口头传递或面对面传递；

——“琥珀色”-受限的分发。仅在“按需所知”基础上，接收方可与组织中其他人共享“琥珀色”信息。发起方可规定此共享的预期限制；

——“绿色”-整个团体。此类信息可在一个特定的团体内广泛传播，但这些信息不得公布或发布到 Internet 上，也不得在团体外发布；

——“白色”-无限制的。根据标准版权规则，“白色”信息可自由分发而不受任何限制。

发起方提供的敏感信息在披露时宜按照 TLP 进行标记。在没有其他说明或规定的情况下，所有的敏感信息都将视为“琥珀色”。同时默认情况下，除非在信息披露时另有特别说明，否则敏感信息来源方的身份将始终为“红色”。

TLP也可仅在组织内使用，例如只授予部分个人可以完全访问所有共享信息，见图2。

9) 此描述是从欧洲网络和信息安全局（ENISA）发布的网络安全信息交换的良好实践指南[5]中获得的，概念最初是由英国的国家基础设施保护中心（CPNI）制定的。

附 录 D
（资料性）
组织信息共享团体的模型

D.1 概述

组织一个信息共享团体有很多方式，从同等合作者的自由协会到高度结构化与集中式控制的正式法律机构。此附录描述了常见的、有效支撑信息安全管理的两种团体组织形式。

D.2 可信信息通信机构

D.2.1 概述

作为集中的协调和沟通门户，可信信息通信机构（TICE）是支持信息共享团体成员间信息交换的自治组织。它已成为行业间和组织间通信的信息安全管理体系的核心要素。TICE 可确保信息共享团体成员间有效和安全信息交换，并帮助成员监视、分析、管理对事件及风险的响应。

可信信息通信机构（TICE）由一组行业专家组成，他们的主要工作是：

——确保 TICE 和团体成员间进行适当的信息交换；

——分析和响应信息安全事件；

——处理事件并支持团体成员从违规中恢复；

——通过以下方法提升团体成员的信息安全意识：

——发布当前使用组件的漏洞公告；

——通知团体成员代表关于利用这些漏洞的病毒和攻击，这样得到授权的成员就可对组件进行高效的修补和更新。

TICE 可作为信息来源方或接收方匿名的可信中介，从而使得成员信任可信来源方，而又不必暴露自己的身份或信任其他隐藏身份的成员。

TICE 可基于或发展自某个已存在的组织，如已经服务于相关团体的信息安全事件响应组（ISIRT）并对其进行扩展，在常规被动服务基础上，增加主动式 TICE 服务。

D.2.2 TICE 组织上的考虑

D.2.2.1 行业专家

为确保具有恰当技能的人员参与其中，并确保专家能够确定交互通信及相关信息基础设施环境中信息的相关性，TICE 组织架构中宜包含具有公共知识的专家或行业知识的专家。

宜通过专家分析，特别是对以下领域（但不限于）进行分析：

——业务管理；

——IT 安全和基础设施；

——运行；

——内部监管机构；

——法律部门。

专家可以是兼职的或全职的，并且可在控制中心或运行现场。

D.2.2.2 组织架构

一个典型的 TICE 宜至少包含以下职能部门：

——执行委员会（必选，负责 TICE 战略管理和团体成员关系）；

——运行技术组（必选，负责分析业务和技术风险问题，确定应用补丁或变更的适用性）；

——运行技术联络员（可选，推荐他们负责提高TICE对组件集成层面（本地站点）涉及的运行环境或资源的认识）；

——法律专家（可选，推荐他们在TICE起始阶段处理法律问题）；

——通信专家（可选，推荐他们负责关注与技术问题有关的翻译难题，从而为团体成员准备更易于理解的消息）。通信专家可提供从团体成员向运行技术组的反馈，因此可作为两个群体之间的促进者。

D.2.2.3 团体成员管理

为确保团体成员间的信任，TICE宜为鉴别、评估、持续了解和管理团体成员或其代表提供支持。

D.2.2.4 组织模式

TICE组织模式主要取决于TICE组织架构、团体成员的性质、能否扩展通过扩展TICE完成相关服务、永久聘用的或是根据需要临时聘用的行业专家。

TICE至少存在三种可能的模式：

——独立模式：作为一个独立组织，有自己的管理层和员工。

——嵌入模式：建立在组织内部并利用其资源提供服务。TICE所分配资源的数量因支持活动不同而不同。

——自愿模式：在自愿基础上由提供建议和支持的专家组成，此模式高度依赖与参与专家的积极性。

D.2.3 TICE核心和可选服务

选择TICE提供的服务时宜基于以下事项：

——信息共享团体成员间通信的范围和风险；

——TICE范围、信息共享团体的组织和性质；

——团体环境中TICE担任的角色（作为成员间信息共享的推动者或发起者）。

TICE核心服务包括：

——响应式服务。响应式服务旨在检测对信息基础设施组件的所有潜在攻击，分析和报告攻击与威胁的影响，响应帮助请求，向团体成员报告事件。

——主动式服务。一些主动式服务旨在事件或事态发生或被检测到之前，通过改进信息共享团体的安全流程和相关信息基础设施，有效推动信息交换。另外一些主动式服务旨在通过增强团体成员的意识提高事件预防，以降低事件发生时的影响和范围。

TICE可选服务包括：

——恶意代码调查服务。恶意代码调查服务旨在：

——分析可能涉及恶意行为的组件上发现的所有文件或对象。

——处理并传递结果给团体成员、供应商和其他相关方，以阻止恶意软件的进一步传播并减轻风险。

——安全和质量管理服务。安全和质量管理服务旨在风险分析、业务持续性管理和安全意识等方面帮助团体成员。

——匿名服务。匿名服务旨在确保团体成员不泄漏自身身份的情况下发送或接收信息。

D.2.4 结论

TICE模型为组织间信息共享提供了一个全面、可控和结构化的模型。它适用于需要及时、快速进行信息共享和分析、成员或政府可支持所需中心基础设施成本的关键环境中。

D.3 预警、建议及报告点

D.3.1 概述

预警、建议及报告点（WARP）模型[6]自2003年起一直在用，该模型为各行业的组织间敏感信息共享提供了一种行之有效的机制。

WARP通常在具有共同利益的人或组织间共享信息，其主要基于信息共享团体成员代表的个人关系。WARP成员数一般在20到100个之间（成员之间具有强共同利益，如小型企业、当地政府、服务提供商、利益群体等），其中包含一个擅长与成员沟通的操作员。

WARP可作为信息共享团体的一部分协同工作，并通过共享信息降低信息系统遭受破坏的风险，从而降低对所在组织的风险。

注：此信息共享团体可基于产业、行业、地理位置、技术标准、利益群体或风险群体等共同利益。

通常，WARPs是小型的、私人的和不以盈利为目的的。

D.3.2 WARP职能

WARP操作员可使用网页、电子邮件、电话、短信和会面向团体成员发送网络安全预警和IT安全建议，也可使用公告板、会议及通用通信技能，利用成员自身的知识去帮助其他团体成员。WARP通过增强成员间的信任鼓励成员匿名谈论自己的事件和问题。

D.3.3 WARP服务

D.3.3.1 概述

WARP通常提供三种核心服务：

——预警过滤服务-成员从在线列表中选择，只接收他们需要的安全信息；

——建议中介服务-成员通过其他成员的布告栏学习他们的举措和经验；

——可信共享服务-成员通过查看报告（报告是匿名的，可以避免遭受尴尬或指责）借鉴彼此的攻击和事件。

D.3.3.2 预警过滤

此服务允许WARP成员接收根据他们感兴趣的领域过滤出来的预警及建议。预警过滤应用软件使用一个允许WARP成员可修改和维护他们选择的订阅树‘标记列表’，帮助WARP操作员及时分类和分发预警及建议。此服务实现了WARP的预警部分。

D.3.3.3 建议中介

此服务允许WARP成员在安全环境中讨论良好实践和信息安全问题。此服务可使成员以交易方式向他人提供经验和技能。此服务实现了WARP的建议部分。

D.3.3.4 可信共享

此服务提供了一个可信的环境，在该环境中WARP成员可在明确共享敏感信息不会对他们造成伤害或尴尬的情况下，共享诸如事件或威胁数据等敏感信息。在相应的安全保障下，共享可通过电话、电子邮件或面对面等方式进行。此外，敏感信息进行匿名处理后也可共享给与其存在信任关系的WARPs及政府部门（用以核对和监测国家总体发展趋势）。此服务实现了WARP的报告部分。

D.3.3.5 其他服务

WARP还可提供对团体成员有益的其他服务。通常为了使WARP操作员满足成员要求的时间和资源最小化，这些服务通常非常简单直接。

D.3.4 效益

WARPs通过提供如下内容为成员增强信息安全：

——可信环境；

——安全信息过滤；

——获取专家建议；

——威胁预警；

——战略决策支持；

——提高安全意识。

建立 WARP 的效益包括但不限于：

——工作效率：WARP 通过促进信息共享和任务协调，减少了重复工作，提升了工作效率，从而使企业或政府供应商受益。

——避免信誉受损：组织逐步开始通过在线途经如网站与公众互动，网站服务的可用性对组织的信誉至关重要。成为 WARP 成员可以保障组织网站的可用性，从而避免组织信誉受损。

——预警：在 WARP 团体内共享成员遇到的问题及解决方案，将为其他团体成员提供预警等个性化服务（即使大型商业供应商提供的服务也无法比拟）。

——政府和其他 WARPs 的支持：共享和分发来自可信来源方的有用建议，可通过建立 WARP 操作员论坛获得其他WARPs操作上的支持,也可通过过滤预警应用的点对点合作分发其他WARPs的预警和建议。

——低成本：WARP 模型旨在通过最少的人员配备（或虚拟团队）实现低成本。

——免费的工具箱：WARP 提供者可使用 WARP 工具箱（从现有 WARPs 经验中创建），包括背景信息、如何启动、创建与运行 WARP 以及下载列表（内容广泛，从媒体文章到营销资料）。

——可持续性：WARPs 的可持续性已在实践中得到广泛验证。

——软件：WARP 供应商可访问专为支持 WARP 核心服务而开发的专业软件。

——增强的可信性：特别是在公益活动中。WARP 非盈利特点及已有的最佳实践，有助于获得团体的信任并增强组织的可信性（尤其适用于公益活动）。

——符合性： WARP 成员关系将帮助成员满足 GB/T 22081-2016 中有关联系的控制。

——发展潜力：越来越多行业（他们具有较低成本和较好的可持续性的基础设施及专业知识）开始构建 WARPs，未来发展潜力巨大。

——企业社会责任：成为 WARP 的成员可增强团体成员的企业社会责任，获得团体成员的信任，并有效支持操作员和成员的业务策略。

D.3.5 结论

WARP 模型为组织间信息共享提供了一个简单的协作模式。它特别适合于资金有限、必须提供集中式基础设施、自愿运行的情况。

附 录NA
（资料性）
GB/T 32920—XXXX 与 GB/T 32920—2016 控制的对应关系

GB/T 32920—XXXX 与 GB/T 32920—2016 控制的对应关系见表 NA.1。

表 NA.1 GB/T 32920—XXXX 与 GB/T 32920—2016 控制对应关系表

GB/T 32920—XXXX	GB/T 32920—2016
5 信息安全策略	
5.1 信息安全管理指导	
5.1.1 信息安全策略	5.1.1 信息安全方针文件
5.1.2 信息安全策略的评审	5.1.2 信息安全方针的评审
6 信息安全组织	6 信息安全组织
7 人力资源安全	
7.1 任用前	
7.1.1 审查	8.1.2 审查
7.1.2 任用条款及条件	8.1.3 任用条款和条件
7.2 任用中	8.2 任用中
7.3 任用的终止和变更	8.3 任用的终止或变化
8 资产管理	
8.1 有关资产的责任	
8.1.1 资产清单	7.1.1 资产清单
8.1.2 资产的所属关系	7.1.2 资产责任人
8.1.3 资产的可接受使用	7.1.3 资产的可接受使用
8.1.4 资产归还	8.3.2 资产的归还
8.2 信息分级	
8.2.1 信息的分级	7.2.1 分类指南
8.2.2 信息的标记	7.2.2 信息的标记和处理
8.2.3 资产的处理	7.2.2 信息的标记和处理 10.7.3 信息处理规程
8.3 介质处理	10.7 介质处置

表NA.1 （续）

GB/T 32920—XXXX	GB/T 32920—2016
8.4 信息交换保护	7.3 信息交换保护
8.4.1 信息分发	7.3.1 信息传播
8.4.2 信息免责声明	7.3.2 信息免责声明
8.4.3 信息可靠性	7.3.3 信息可信性
8.4.4 信息敏感性消减	7.3.4 信息敏感性降低
8.4.5 匿名来源保护	7.3.5 匿名来源方保护
8.4.6 匿名接收方保护	7.3.6 匿名接收方保护
8.4.7 进一步发布授权	7.3.7 进一步发布授权
9 访问控制	11 访问控制
10 密码	
10.1 密码控制	
10.1.1 密码控制的使用策略	12.3.1 使用密码控制的策略
10.1.2 密钥管理	12.3.2 密钥管理
11 物理和环境安全	9 物理和环境安全
12 运行安全	
12.1 运行规程和职责	10.1 操作规程和职责
12.2 恶意软件防范	
12.2.1 恶意软件的控制	10.4.1 控制恶意代码 10.4.2 控制移动代码
12.3 备份	10.5 备份
12.4 日志和监视	10.10 监视
12.4.1 事态日志	10.10.1 审计记录
12.4.2 日志信息的保护	10.10.3 日志信息的保护
12.4.3 管理员和操作员日志	10.10.4 管理员和操作员日志
12.4.4 时钟同步	10.10.6 时钟同步
12.5 运行软件控制	12.4 系统文件的安全
12.6 技术方面的脆弱性管理	12.6 技术脆弱性管理

表NA.1 （续）

GB/T 32920—XXXX	GB/T 32920—2016
12.7 信息系统审计的考虑	
12.7.1 信息系统审计控制	15.3.1 信息系统审计控制措施
13 通信安全	
13.1 网络安全管理	10.6 网络安全管理
13.2 信息传输	
13.2.1 信息传输策略和规程	10.8.1 信息交换策略和规程
13.2.2 信息传输协议	10.8.2 交换协议
13.2.3 电子消息发送	10.8.4 电子消息发送
13.2.4 保密或不泄露协议	6.1.5 保密性协议
14 系统获取、开发和维护	12 信息系统获取、开发和维护
15 供应商关系	
15.1 供应商关系中的信息安全	
15.1.1 供应商关系的信息安全策略	新的控制
15.1.2 在供应商协议中强调安全	6.2.3 处理第三方协议中的安全问题
15.1.3 信息与通信技术供应链	新的控制
15.2 供应商服务交付管理	10.2 第三方服务交付管理
16 信息安全事件管理	
16.1 信息安全事件的管理和改进	
16.1.1 责任和规程	13.2.1 职责和规程
16.1.2 报告信息安全事态	13.1.1 报告信息安全事态
16.1.3 报告信息安全弱点	13.1.2 报告安全弱点
16.1.4 信息安全事态的评估和决策	新的控制
16.1.5 信息安全事件的响应	新的控制
16.1.6 从信息安全事件中学习	13.2.2 对信息安全事件的总结
16.1.7 证据的收集	13.2.3 证据的收集
16.1.8 早期预警系统	新的控制

表NA.1 （续）

GB/T 32920—XXXX	GB/T 32920—2016
17 业务连续性管理的信息安全方面	
17.1 信息安全的连续性	
17.1.1 规划信息安全连续性	14.1.1 在业务连续性管理过程中包含信息安全 14.1.3 制定和实施包含信息安全的连续性计划
17.1.2 实现信息安全连续性	14.1.3 制定和实施包含信息安全的连续性计划
17.1.3 验证、评审和评价信息安全连续性	14.1.5 测试、维护和再评估业务连续性计划
17.2 冗余	新的控制
18 符合性	
18.1 符合法律和合同要求	
18.1.1 适用的法律和合同要求的识别	15.1.1 可用法律的识别
18.1.2 知识产权	15.1.2 知识产权（IPR）
18.1.3 记录的保护	15.1.3 保护组织的记录
18.1.4 隐私和个人可识别信息保护	15.1.4 数据保护和个人信息的隐私
18.1.5 密码控制规则	15.1.6 密码控制措施的规则
18.2 信息安全评审	15.2 符合安全策略和标准以及技术符合性

附 录NB
（资料性）
GB/T 22081—2016/ISO/IEC 27002:2013 与 ISO/IEC 27002:2022 控制的对应关系

GB/T 22081—2016/ISO/IEC 27002:2013 与 ISO/IEC 27002:2022 控制的对应关系见表 NB.1。

表 NB.1 GB/T 22081—2016/ISO/IEC 27002:2013 与 ISO/IEC 27002:2022 控制的对应关系表

GB/T 22081—2016/ISO/IEC 27001:2013	ISO/IEC 27002:2022
5 信息安全策略	
5.1 信息安全管理指导	
5.1.1 信息安全策略	5.1 信息安全策略
5.1.2 信息安全策略的评审	5.1 信息安全策略
6 信息安全组织	
6.1 内部组织	
6.1.1 信息安全的角色和责任	5.2 信息安全的角色和责任
6.1.2 职责分离	5.3 职责分离
6.1.3 与职能机构的联系	5.5 与职能机构的联系
6.1.4 与特定相关方的联系	5.6 与特定相关方的联系
6.1.5 项目管理中的信息安全	5.8 项目管理中的信息安全
6.2 移动设备和远程工作	
6.2.1 移动设备策略	8.1 用户终端设备
6.2.2 远程工作	6.7 远程工作
7 人力资源安全	
7.1 任用前	
7.1.1 审查	6.1 审查
7.1.2 任用条款及条件	6.2 任用条款及条件
7.2 任用中	
7.2.1 管理责任	5.4 管理责任
7.2.2 信息安全意识、教育和培训	6.3 信息安全意识、教育和培训
7.2.3 违规处理过程	6.4 违规处理过程
7.3 任用的终止和变更	
7.3.1 任用终止或变更的责任	6.5 任用终止或变更的责任

表NB.1 （续）

GB/T 22081—2016/ISO/IEC 27001:2013	ISO/IEC 27002:2022
8 资产管理	
8.1 有关资产的责任	
8.1.1 资产清单	5.9 信息和其他相关资产的清单
8.1.2 资产的所属关系	5.9 信息和其他相关资产的清单
8.1.3 资产的可接受使用	5.10 信息和其他相关资产的可接受使用
8.1.4 资产归还	5.11 资产归还
8.2 信息分级	
8.2.1 信息的分级	5.12 信息的分级
8.2.2 信息的标记	5.13 信息的标记
8.2.3 资产的处理	5.10 信息和其他相关资产的可接受使用
8.3 介质处理	
8.3.1 移动介质的管理	7.10 存储媒体
8.3.2 介质的处置	7.10 存储媒体
8.3.3 物理介质的转移	7.10 存储媒体
9 访问控制	
9.1 访问控制的业务要求	
9.1.1 访问控制策略	5.15 访问控制
9.1.2 网络和网络服务的访问	5.15 访问控制
9.2 用户访问管理	
9.2.1 用户注册和注销	5.16 身份管理
9.2.2 用户访问供给	5.18 访问权
9.2.3 特定访问权管理	8.2 特定访问权
9.2.4 用户的秘密鉴别信息管理	5.17 鉴别信息
9.2.5 用户访问权的评审	5.18 访问权
9.2.6 访问权的移除或调整	5.18 访问权
9.3 用户责任	
9.3.1 秘密鉴别信息的使用	5.17 鉴别信息

表NB.1 （续）

GB/T 22081—2016/ISO/IEC 27001:2013	ISO/IEC 27002:2022
9.4 系统和应用访问控制	
9.4.1 信息访问限制	8.3 信息访问限制
9.4.2 安全登录规程	8.5 安全鉴别
9.4.3 口令管理系统	5.17 鉴别信息
9.4.4 特权实用程序的使用	8.18 特权实用程序的使用
9.4.5 程序源代码的访问控制	8.4 访问源代码
10 密码	
10.1 密码控制	
10.1.1 密码控制的使用策略	8.24 密码的使用
10.1.2 密钥管理	8.24 密码的使用
11 物理和环境安全	
11.1 安全区域	
11.1.1 物理安全边界	7.1 物理安全边界
11.1.2 物理入口控制	7.2 物理入口
11.1.3 办公室、房间和设施的安全保护	7.3 办公室、房间和设施的安全保护
11.1.4 外部和环境威胁的安全防护	7.5 物理和环境威胁的安全防护
11.1.5 在安全区域工作	7.6 在安全区域工作
11.1.6 交接区	7.2 物理入口
11.2 设备	
11.2.1 设备安置和保护	7.8 设备安置和保护
11.2.2 支持性设施	7.11 支持性设施
11.2.3 布缆安全	7.12 布缆安全
11.2.4 设备维护	7.13 设备维护
11.2.5 资产的移动	7.10 存储媒体
11.2.6 组织场所外的设备与资产安全	7.9 组织场所外资产安全
11.2.7 设备的安全处置或再利用	7.14 设备的安全处置或再利用
11.2.8 无人值守的用户设备	8.1 用户终端设备

表NB.1 （续）

GB/T 22081—2016/ISO/IEC 27001:2013	ISO/IEC 27002:2022
11.2.9 清理桌面和屏幕策略	7.7 清理桌面和屏幕
12 运行安全	
12.1 运行规程和职责	
12.1.1 文件化的操作规程	5.37 文件化的操作规程
12.1.2 变更管理	8.32 变更管理
12.1.3 容量管理	8.6 容量管理
12.1.4 开发、测试和运行环境的分离	8.31 开发、测试和运行环境的分离
12.2 恶意软件防范	
12.2.1 恶意软件的控制	8.7 恶意软件防范
12.3 备份	
12.3.1 信息备份	8.13 信息备份
12.4 日志和监视	
12.4.1 事态日志	8.15 日志
12.4.2 日志信息的保护	8.15 日志
12.4.3 管理员和操作员日志	8.15 日志
12.4.4 时钟同步	8.17 时钟同步
12.5 运行软件控制	
12.5.1 运行系统的软件安装	8.19 运行系统的软件安装
12.6 技术方面的脆弱性管理	
12.6.1 技术方面脆弱性的管理	8.8 技术方面脆弱性的管理
12.6.2 软件安装限制	8.19 运行系统的软件安装
12.7 信息系统审计的考虑	
12.7.1 信息系统审计的控制	8.34 审计测试期间信息系统防护
13 通信安全	
13.1 网络安全管理	
13.1.1 网络控制	8.20 网络安全
13.1.2 网络服务的安全	8.21 网络服务的安全

表NB.1 （续）

GB/T 22081—2016/ISO/IEC 27001:2013	ISO/IEC 27002:2022
13.1.3 网络中的隔离	8.22 网络隔离
13.2 信息传输	
13.2.1 信息传输策略和规程	5.14 信息传输
13.2.2 信息传输协议	5.14 信息传输
13.2.3 电子消息发送	5.14 信息传输
13.2.4 保密或不泄露协议	6.6 保密或不泄露协议
14 系统获取、开发和维护	
14.1 信息系统的安全要求	
14.1.1 信息安全要求分析和说明	5.8 项目管理中的信息安全
14.1.2 公共网络上应用服务的安全保护	8.26 应用安全要求
14.1.3 应用服务事务的保护	8.26 应用安全要求
14.2 开发和支持过程中的安全	
14.2.1 安全的开发策略	8.25 安全开发生命周期
14.2.2 系统变更控制规程	8.32 变更管理
14.2.3 运行平台变更后对应用的技术评审	8.32 变更管理
14.2.4 软件包变更的限制	8.32 变更管理
14.2.5 系统安全工程原则	8.27 安全系统架构和工程原则
14.2.6 安全的开发环境	8.31 开发、测试和运行环境的分离
14.2.7 外包开发	8.30 外包开发
14.2.8 系统安全测试	8.29 开发和验收中安全测试
14.2.9 系统验收测试	8.29 开发和验收中安全测试
14.3 测试数据	
14.3.1 测试数据的保护	8.33 测试信息
15 供应商关系	
15.1 供应商关系中的信息安全	
15.1.1 供应商关系的信息安全策略	5.19 供应商关系中的信息安全
15.1.2 在供应商协议中强调安全	5.20 在供应商协议中强调安全

表 NB.1 （续）

GB/T 22081—2016/ISO/IEC 27001:2013	ISO/IEC 27002:2022
15.1.3 信息与通信技术供应链	5.21 管理 ICT 供应链中信息安全
15.2 供应商服务交付管理	
15.2.1 供应商服务的监视和评审	5.22 供应商服务的监视、评审和变更管理
15.2.2 供应商服务的变更管理	5.22 供应商服务的监视、评审和变更管理
16 信息安全事件管理	
16.1 信息安全事件的管理和改进	
16.1.1 责任和规程	5.24 信息安全事件管理的规划和准备
16.1.2 报告信息安全事态	6.8 信息安全事态报告
16.1.3 报告信息安全弱点	6.8 信息安全事态报告
16.1.4 信息安全事态的评估和决策	5.25 信息安全事态的评估和决策
16.1.5 信息安全事件的响应	5.26 信息安全事件的响应
16.1.6 从信息安全事件中学习	5.27 从信息安全事件中学习
16.1.7 证据的收集	5.28 证据的收集
17 业务连续性管理的信息安全方面	
17.1 信息安全的连续性	
17.1.1 规划信息安全连续性	5.29 中断期间的信息安全
17.1.2 实现信息安全连续性	5.29 中断期间的信息安全
17.1.3 验证、评审和评价信息安全连续性	5.29 中断期间的信息安全
17.2 冗余	
17.2.1 信息处理设施的可用性	8.14 信息处理设施的冗余
18 符合性	
18.1 符合法律和合同要求	
18.1.1 适用的法律和合同要求的识别	5.31 法律、法规、监管和合同要求
18.1.2 知识产权	5.32 知识产权
18.1.3 记录的保护	5.33 记录的保护
18.1.4 隐私和个人可识别信息保护	5.34 隐私和个人可识别信息保护
18.1.5 密码控制规则	5.31 法律、法规、监管和合同要求

表 NB.1 （续）

GB/T 22081—2016/ISO/IEC 27001:2013	ISO/IEC 27002:2022
18.2 信息安全评审	
18.2.1 信息安全的独立评审	5.35 信息安全的独立评审
18.2.2 符合安全策略和标准	5.36 符合信息安全策略、规则和标准
18.2.3 技术符合性评审	5.36 符合信息安全策略、规则和标准 8.8 技术方面脆弱性的管理

参 考 文 献

[1] Internet Engineering Task Force. RFC 4021: Registration of Mail and MIME Header Fields [online]. March 2005 [viewed October 2014]. http://datatracker.ietf.org/doc/rfc4021/

[2] GB/T 25067 信息技术 安全技术 信息安全管理体系审核和认证机构要求

[3] O'REILLY. Tim. What Is Web 2.0 — Design Patterns and Business Models for the Next Generation of Software. O'Reilly Web Blog [online]. 30 September 2005 [viewed October 2014]. http://oreilly.com/web2/archive/what-is-web-20.html

[4] Wikipedia, The Free Encyclopedia. Pareto distribution [online]. 25 April 2011 [viewed October 2014]. http://en.wikipedia.org/wiki/Pareto_distribution

[5] European Agency for Network and Information Security. Good Practice Guide on Information Sharing. June 2009 [viewed October 2014]. http://www.enisa.europa.eu/activities/Resilienceand-CIIP/public-private-partnership/information-sharing-exchange/good-practice-guide

[6] Centre for the Protection of National Infrastructure (UK). WARP homepage. April 2010[viewed October 2014]. Available from: http://www.warp.gov.uk

[7] ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection-Information security controls