ICS 35.040
L 80

中华人民共和国国家标准

GB/T XXXXX—XXXX/ISO/IEC 27010:2012

信息技术 安全技术
行业间和组织间通信的信息安全管理

Information technology — Security techniques —

Information security management for inter-sector and

inter-organizational communications

(ISO/IEC 27010:2012, 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

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

1 范围

本标准给出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。

本标准特别为组织间和行业间通信给出了发起、实施、维护与改进信息安全的控制措施和指南。

本标准适用于行业间各种公共和私有的、国内的敏感信息交换和共享。特别是，本标准可适用于与组织或国家重要信息系统和基础信息网络[1)]的供给、维护和保护相关的信息交换与共享。

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 22080-2008 信息技术 安全技术 信息安全管理体系要求（ISO/IEC 27001:2005，IDT）

GB/T 22081-2008 信息技术 安全技术 信息安全管理实用规则（ISO/IEC 27002:2005，IDT）

GB/T 29246-2012 信息技术 安全技术 信息安全管理体系 概述和词汇（ISO/IEC 27000:2009，IDT）

3 术语、定义和缩略语

3.1 术语和定义

GB/T 29246-2012 中界定的以及下列术语和定义适用于本文件。

3.1.1

信息共享团体 information sharing community

商定共享信息的组织群。

注：组织可以是个体。

3.1.2

可信信息通信机构 trusted information communication entity

信息共享团体内支持信息交换的自治组织。

3.2 缩略语

下列缩略语适用于本标准：

TICE	可信信息通信机构	（Trusted Information Communication Entity）
WARP	预警、建议和报告中心	（Warning, Advice and Reporting Points）
ISMS	信息安全管理体系	（Information Security Management System）

1) 国际上叫做国家关键基础设施。

P2P	对等通信	（Peer to Peer）
IPR	知识产权	（Intellectual Property Right）
CVE	公共漏洞和暴露	（Common Vulnerabilities & Exposures）
ISIRT	信息安全事件响应组	（Information Security Incident Response Team）
TLP	交通信号灯协议	（Traffic Light Protocol）

4 概念和释义

4.1 介绍

本标准在第5至15章中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 22081-2008中定义了组织间双方交换信息的控制措施，以及用于公开可用信息的通用分发控制措施。然而，在某些情况下，需要在同一团体内的不同组织之间共享某种敏感信息，这种敏感信息仅限于对团体内成员公开可用。通常，这种信息只能对每个成员组织内特定的个人可用，或者有信息匿名化等其他安全要求。本标准定义附加的控制措施，并提供对GB/T 22080-2008和GB/T 22081-2008的补充指南和解释，以满足这些要求。

4.2 信息共享团体

为了使信息共享团体有效运行，必须依据某些共同利益或其他关系来定义共享敏感信息的范围。例如，团体可能是特定的行业，并因此将组织的成员资格限定在本行业中。当然，实际中还存在一些其他可以构成共同利益的基础，例如地理位置或共同所有权等。

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。因此，可能没有清晰或统一的适用于所有成员的组织结构和管理职能。为了有效的进行信息安全管理，管理责任和义务是必不可少的。因此，宜清晰定义适用于团体信息安全管理的组织结构和管理职能。

宜考虑同一信息共享团体中成员组织间的差异。这些差异可能包括：

——成员组织是否已经运行自己的ISMS；

——成员组织关于资产保护和信息披露的规则。

4.4 支撑机构

许多信息共享团体将会选择建立或者指定一个集中的支撑机构来组织和支撑信息共享。这种机构能够提供许多支持性的控制措施，这些控制措施比成员间直接通信更加容易和更加有效，比如源头和接收方的匿名化。

现实中有许多不同的组织模型可用于创建支撑机构，本标准中的附录D描述了两个通用模型，即可信信息通信机构（TICE）和预警、建议及报告中心（WARP）。

4.5 行业间通信

许多信息共享团体以行业为基础，因此无形中为共同利益提供了一个既定范围。然而，这种团体共享的信息很有可能对其他行业建立的信息共享团体有价值。在这种情况下，可能需要在原有信息共享团体的基础上再一次基于某种共同利益建立信息共享团体，诸如共享信息的自然属性。这称为行业间通信。

由于能在支撑机构之间而不是所有团体的所有成员之间建立必要的信息交换协议和控制措施，因此每一个信息共享团体中支撑机构的存在极大地方便了行业间通信。同时，通过支撑机构也可实现某些行业间通信所要求的源头或接收方组织匿名化。

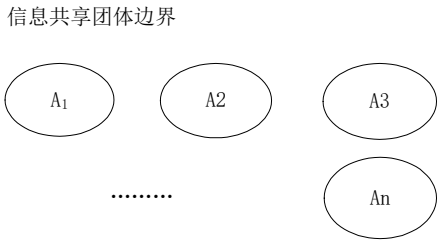
4.6 符合性

任何依据 GB/T 22080-2008 以及使用源于 GB/T 22081-2008、本标准和其他来源的控制措施所创建和运行的信息安全管理体系（ISMS）均能对照未加修改和补充的 GB/T 22080-2008 进行符合性评估。

但是，GB/T 22080-2008 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某个团体）时，有许多需要阐明的地方。

首先需要阐明的是本标准中所提及的组织的定义。

GB/T 22080-2008 要求 ISMS 由一个组织建立，并在组织整体业务活动和所面临风险的环境中运行（GB/T 22080-2008，4.1）。在此背景下，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。



图例

A_k：团体的成员组织 k（k=1…n），包括所有支撑机构。

图 1 团体与组织

其次，在许多信息共享团体中，并不是成员组织中的所有个人均被允许访问成员间共享的敏感信息。在此情况下，成员组织的一部分将被包含在团体 ISMS 范围内，一部分则在团体 ISMS 范围之外。团体 ISMS 范围外的成员组织将仅可访问被标记为广泛发布的团体信息，如图 2 所示。

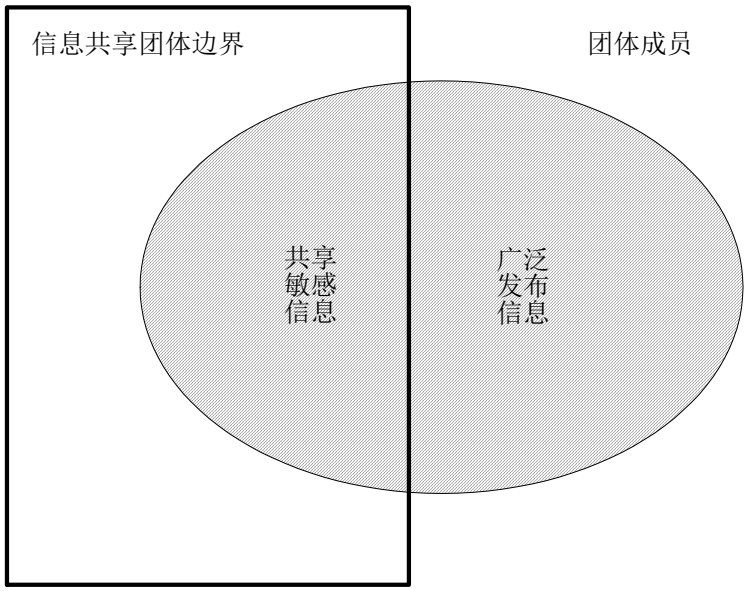


图 2　团体成员的一部分在范围内

信息共享团体的成员可能有自己的信息安全管理体系，因此某些流程可能同时属于团体和成员两者管理体系的范围之内。在这种情况下，对这些流程的要求至少在理论上可能存在冲突或不兼容，这时将其从成员的 ISMS 范围中排除或许更加合理——具体参见 GB/T 22080-2008，4.2.1 a）。

在确定信息共享团体风险评估方法时（GB/T 22080-2008，4.2.1 c)），需要认识到风险对不同的团体成员的影响可能不同。因此，团体需要选择一种风险评估方法来处理这种影响不一致的情况，对于风险评估准则的选择也是如此。

测量所选控制措施的有效性（GB/T 22080-2008，4.2.3 c)）需要信息共享团体全体成员的参与。关于自身环境中控制措施有效性情况，所有成员需要向信息提供者与信息共享团体这个整体提供定期反馈。

4.7　通信模型

选定的控制要求得到满足的条件下，本标准所涵盖的敏感信息通信可采用书面、口头或电子等任意形式。

本标准其余部分，通过如下参与者描述个体敏感通信：

——信息的源头是发起信息的个体或组织；该源头不需要是团体的成员。

——发起方是在信息共享团体内发起信息分发的团体成员。发起方可直接分发或通过支撑机构分发信息。发起方可以但不需要与信息源头相同；发起方可隐藏源头的身份。团体可提供使成员能隐藏其作为发起方的自身身份的工具。

——接收方是信息共享团体内分发信息的接收者。如果信息被标识为广泛分发，接收方不需要是团体成员。团体可提供使接收方对信息发起方隐藏其身份的工具。

5 安全方针

5.1 信息安全方针

5.1.1 信息安全方针文件

GB/T 22081-2008 中 5.1.1 的控制措施补充如下：

实施指南

信息安全方针文件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南。它宜对团体内参与信息共享的所有员工有效。信息安全方针可限制向团体成员中其他员工传播。

信息安全方针文件宜定义团体范围内使用的信息标记和分发策略。

5.1.2 信息安全方针的评审

GB/T 22081-2008 中 5.1.2 的控制措施补充如下:

实施指南

管理评审的输入宜包括信息共享团体成员的重大变化信息。

6 信息安全组织

6.1 内部组织

对行业间和组织间通信没有补充信息。

6.2 外部各方

6.2.1 与外部各方相关风险的识别

对行业间和组织间通信没有补充信息。

6.2.2 处理与顾客有关的安全问题

对行业间和组织间通信没有补充信息。

6.2.3 处理第三方协议中的安全问题

GB/T 22081-2008 中 6.2.3 的控制措施补充如下：

实施指南

为避免团体成员对参与处理参其所提供信息的特定第三方持有异议，所有团体成员宜了解参与提供团体服务的所有第三方的身份。

与供应商及服务提供方之间关于提供团体服务的协议中，宜规定对他们的服务定期实施安全评审和审核。

7 资产管理

7.1 对资产负责

7.1.1 资产清单

对行业间和组织间通信没有补充信息。

7.1.2 资产责任人

对行业间和组织间通信没有补充信息。

7.1.3 资产的可接受使用

GB/T 22081-2008 中 7.1.3 的控制措施补充如下：

实施指南

信息共享团体其他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全部规则进行保护和传播。

7.2 信息分类

7.2.1 分类指南

GB/T 22081-2008 中 7.2.1 的控制措施补充如下：

控制措施

信息宜按照它对组织的价值、法律要求、敏感性、可信度和关键性予以分类。

实施指南

除了 GB/T 22081-2008 给出的分类准则，信息宜按照它的可信度进行分类。宜依据信息源头的信誉、技术内容和描述质量进行评估。

同样的，敏感性取决于除维护信息保密性要求之外的很多方面，如信息泄露的影响、信息分发的紧迫性或破坏信息源头匿名性的可能性。

在解释信息共享团体中其他成员所分配的分类标记时宜加以注意。

例如，当收到敏感头字段被设置为“公司机密”（RFC 4021[参见参考文献 2]）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是指“公司机密”（如果是指“公司机密”，则该消息已被错误的发送）还是指“对收件人保密”，不明确。

7.2.2 信息的标记和处理

对行业间和组织间通信没有补充信息。

7.3 信息交换保护

GB/T 22081-2008 第 7 章，资产管理部分，补充的控制目标如下：

目标：确保信息共享团体中信息交换受到充分保护。

即使成员是采用不同方式标记、分发、保护自身信息的独立机构或机构的一部分，仍宜采取一致的方式保护信息共享团体成员间交换的信息。

当有匿名要求时，宜删除可识别信息交换源头的所有信息。同样的，接收方宜在不暴露身份的情况下接收共享信息。

团体之外发布共享信息宜收到控制。

7.3.1 信息传播

控制措施

基于团体规定的预定义传播标记，宜限制接收成员内的信息传播。

实施指南

对于未分配传播标记的信息，宜给出信息共享团体定义的默认传播标记。如果有疑问，或者没有可普遍接受的默认传播协议，宜谨慎处理信息。如果可能的话，接收方宜请求发起方重新发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、阻止打印与输出等使用限制。

其他信息

共享信息的不同属性或组成部分可能具有不同的敏感性。特别的，已有消息或其他共享信息包含的知识可能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。如果是这样，需要一个清晰的用户权限策略或模型以使用户理解体系允许他们做什么，以及限制他们做什么。

7.3.2 信息声明

控制措施

每一次信息交换宜从声明开始，除正常信息标记外，声明中列出接收方需要遵从的所有特殊要求。

实施指南

如果不能充分理解声明或无法履行声明中的内容，接收方宜要求发起方解释清楚。

7.3.3 信息可信度

控制措施

每一次信息交换宜标明发起方在所传送信息的可信度和准确性方面的置信度。

实施指南

鉴于紧迫性、潜在结果和技术限制，也许不可能在信息传送前验证所有信息。对于存在限制的地方，宜作为消息的一部分给出这些限制。

信息源头匿名或未知的情况下，指出所保留的信息可信度特别重要。标明发起方已能验证直接给出的信息与保证其可靠性的情况也很重要。

7.3.4 信息敏感性消减

控制措施

信息交换的发起方宜标明经过一些外部事件或一段时间后，所提供信息的敏感性是否消减。

实施指南

即使所提供信息的敏感性随时间消减，信息可能仍需要保护。分类指南（见 7.2.1）可能需要包含针对敏感性消减的默认控制措施。

7.3.5 匿名源头保护

控制措施

当要求匿名时，团体成员在发起或接收的所有通信中，宜删除所有源头标识信息。

实施指南

向信息共享团体其他成员传递信息前，信息发起方负责从源头（如果源头与发起方不同）获取许可。同时，发起方宜询问源头，是否可以将其标识为信息的原始提供者。

由于内容分析可暴露源头身份，因此源头保护过程考虑消息源头和消息内容同等重要。在可能的情况下，消息的发起方在消息分发前，宜要求源头对匿名信息和目标接收方名单进行审查。

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，那么这条消息就可能暴露事件源头。

具有能够在不破坏匿名性的情况下保证数据可靠性的技术机制。例如，不暴露发起方真实身份的情况下，共享密钥加密可能被用于确认通信发起于团体成员。

7.3.6 匿名接收方保护

控制措施

经发起方许可，团体成员宜在不暴露自己身份的情况下接收通信。

实施指南

匿名接收可通过技术方法（如加密）和程序手段（如通过支撑机构进行路由）实现。必须注意确保匿名不违反法律约束或降低团体的整体信任度。

其他信息

行业团体希望保持成员详细信息的私密性。因此对于有效的行业间通信，匿名接收通常是必要的。

7.3.7 进一步发布授权

控制措施

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

实施指南

信息进一步分发前，每个接收方宜负责从发起方获得广泛发布的所有必要授权。

在行业间通信中，发起方无法确认将要接收信息的所有组织。在此情况下，需要授予通用发布许可或特定行业发布许可。

其他信息

交通信号灯协议（参见附录C）通常用于标明不寻求附加许可情况下信息如何进一步分发。

8 人力资源安全

8.1 任用之前

8.1.1 角色和职责

对行业间和组织间通信没有补充信息。

8.1.2 审查

对行业间和组织间通信没有补充信息。

8.1.3 任用条款和条件

GB/T 22081-2008 中 8.1.3 的控制措施补充如下：

实施指南

审查准则对于一个信息共享团体中的全部成员不可能保持一致。对于可获取共享团体信息的成员组织中的所有员工或承包商，团体宜考虑定义适用于他们的验证核查的最低级别。

8.2 任用中

对行业间和组织间通信没有补充信息。

8.3 任用的终止或变化

对行业间和组织间通信没有补充信息。

9 物理和环境安全

对行业间和组织间通信没有补充信息。

10 通信和操作管理

10.1 操作规程和职责

对行业间和组织间通信没有补充信息。

10.2 第三方服务交付管理

对行业间和组织间通信没有补充信息。

10.3 系统规划和验收

对行业间和组织间通信没有补充信息。

10.4 防范恶意和移动代码

10.4.1 控制恶意代码

GB/T 22081-2008 中 10.4.1 的控制措施补充如下：

实施指南

无论团体成员间的通信服务是否提供抗病毒信息扫描，从一个信息共享团体其他成员处接收到的信息宜进行恶意代码扫描。

10.4.2 控制移动代码

对行业间和组织间通信没有补充信息。

10.5 备份

对行业间和组织间通信没有补充信息。

10.6 网络安全管理

对行业间和组织间通信没有补充信息。

10.7 介质处置

对行业间和组织间通信没有补充信息。

10.8 信息的交换

10.8.1 信息交换策略和规程

对行业间和组织间通信没有补充信息。

10.8.2 交换协议

GB/T 22081-2008 中 10.8.2 的控制措施补充如下：

实施指南

所有信息共享团体宜定义信息交换协议，同时宜仅允许签署和接受协议的成员加入团体。

10.8.3 运输中的物理介质

对行业间和组织间通信没有补充信息。

10.8.4 电子消息发送

GB/T 22081-2008 中 10.8.4 的控制措施补充如下：

实施指南

所有信息共享团体宜定义规则保护传输中的信息，同时宜仅允许接受和实施这些规则的准成员加入团体。任何支撑机构内部宜实施这些规则。

信息共享团体宜考虑实施不依赖于电子消息发送的信息共享替代机制，且使成员能够明确说明特定信息是由这些替代路径分发。

10.8.5 业务信息系统

对行业间和组织间通信没有补充信息。

10.9 电子商务服务

对行业间和组织间通信没有补充信息。

10.10 监视

10.10.1 审计记录

GB/T 22081-2008 中 10.10.1 的控制措施补充如下：

实施指南

若信息共享团体要求，成员宜记录共享信息在内部的传播。

10.10.2 监视系统的使用

对行业间和组织间通信没有补充信息。

10.10.3 日志信息的保护

对行业间和组织间通信没有补充信息。

10.10.4 管理员和操作员日志

对行业间和组织间通信没有补充信息。

10.10.5 故障日志

对行业间和组织间通信没有补充信息。

10.10.6 时钟同步

对行业间和组织间通信没有补充信息。

11 访问控制

对行业间和组织间通信没有补充信息。

12 信息系统获取、开发和维护

12.1 信息系统的安全要求

对行业间和组织间通信没有补充信息。

12.2 应用中的正确处理

对行业间和组织间通信没有补充信息。

12.3 密码控制

12.3.1 使用密码控制的策略

GB/T 22081-2008 中 12.3.1 的控制措施补充如下：

实施指南

密码技术也可用于实现信息共享的传播规则，如通过信息权限管理实现。

12.3.2 密钥管理

对行业间和组织间通信没有补充信息。

12.4 系统文件的安全

对行业间和组织间通信没有补充信息。

12.5 开发和支持过程中的安全

对行业间和组织间通信没有补充信息。

12.6 技术脆弱性管理

对行业间和组织间通信没有补充信息。

13 信息安全事件管理

13.1 报告信息安全事态和弱点

13.1.1 报告信息安全事态

GB/T 22081-2008 中 13.1.1 的控制措施补充如下：

实施指南

信息共享团体的成员宜考虑是否宜向其他成员报告检测到的事态。团体宜协商一致并公布对其他成员有价值的事件类型指南。团体成员宜进行判断，以确保只报告对其他成员有潜在价值的事态。

为了保护发起方的信誉，保持事件机密性且不允许团体成员泄露事件信息具有较强的趋势。然而，将事件信息传递给其他成员将促进未来在事件预防与事件及时快速响应方面的合作与协调，并将改善团体整体安全性。因此，在无需暴露事态和事件所有结果情况下，可以将其报告给其他成员。

同样，成员宜及时检查所有报告的事态，以查看它们是否将会对自己的操作产生影响。例如，提供计划维护操作共享服务的成员的常规公告中，可能需要其他成员在维护活动启动之前审查替代提供者的可靠性。

13.1.2 报告安全弱点

对行业间和组织间通信没有补充信息。

13.1.3 风险提示系统

GB/T 22081-2008 中 13.1，报告信息安全事态和弱点部分，补充的控制措施如下：

控制措施

风险提示系统宜在信息共享团体内部署以及时有效地传递可用的优先信息。

实施指南

优先信息是可使其他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。

13.2 信息安全事件和改进的管理

13.2.1 职责和规程

对行业间和组织间通信没有补充信息。

13.2.2 对信息安全事件的总结

GB/T 22081-2008 中 13.2.2 的控制措施补充如下：

实施指南

宜基于信息共享团体分发的信息执行调查，以减少类似事件的风险，并且更好的理解面向团体和所有相关重要信息基础设施的风险。此调查可能由相关团体成员或通过已有的支撑机构执行。

即使成员未受到发生事件的影响，信息共享团体成员在报告事件后仍宜进行事后评审，以触发对安全事件响应计划、相关程序和业务风险的更新。每个成员宜确保所报告的事件响应经过了评估，每个成员也宜确保识别了针对成员自身响应过程的所有经验或可能的改进，并且这些经验或改进对持续改进其响应流程是起作用的。

13.2.3 证据的收集

对行业间和组织间通信没有补充信息。

14 业务连续性管理

14.1 业务连续性管理的信息安全方面

14.1.1 在业务连续性管理过程中包含信息安全

对行业间和组织间通信没有补充信息。

14.1.2 业务连续性和风险评估

GB/T 22081-2008 中 14.1.2 的控制措施补充如下：

实施指南

信息共享团体成员实施的业务连续性风险评估宜考虑对其他成员敏感信息供给的依赖。

14.1.3 制定和实施包含信息安全的连续性计划

GB/T 22081-2008 中 14.1.3 的控制措施补充如下：

实施指南

信息共享团体成员制定的业务连续性计划宜解决与其他成员交换敏感信息的需求，并将其作为恢复流程的一部分。

14.1.4 业务连续性计划框架

对行业间和组织间通信没有补充信息。

14.1.5 测试、维护和再评估业务连续性计划

对行业间和组织间通信没有补充信息。

15 符合性

15.1 符合法律要求

15.1.1 可用法律的识别

GB/T 22081-2008 中 15.1.1 的控制措施补充如下：

实施指南

信息共享团体宜适当考虑所有相关的协议、与信息共享相关的法律和法规如反垄断法律或法规。这样可能阻止特定组织加入团体或对它们的代表加以限制。

15.1.2 知识产权（IPR）

对行业间和组织间通信没有补充信息。

15.1.3 保护组织的记录

对行业间和组织间通信没有补充信息。

15.1.4 数据保护和个人信息的隐私

对行业间和组织间通信没有补充信息。

15.1.5 防止滥用信息处理设施

对行业间和组织间通信没有补充信息。

15.1.6 密码控制措施的规则

对行业间和组织间通信没有补充信息。

15.1.7 信息共享团体的责任

GB/T 22081-2008 中 15.1，符合法律要求部分，补充的控制措施如下：

控制措施

信息共享团体所有成员宜阐明、理解及认可责任问题和补救措施，以处理信息被有意或无意泄露的情况。

实施指南

补救措施宜至少包含向发起方反馈的关于所有未授权泄露的通知，其中具有足够的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源头，如有可能，仍宜将通知反馈给源头。这可能通过诸如 TICE 的可信第三方的媒介来实现。

未授权泄露可能直接影响责任方，为重建团体信任，在一段时间内可能会涉及排除或限制某些成员的访问。

15.2 符合安全策略和标准以及技术符合性

对行业间和组织间通信没有补充信息。

15.3 信息系统审计考虑

15.3.1 信息系统审计控制措施

对行业间和组织间通信没有补充信息。

15.3.2 信息系统审计工具的保护

对行业间和组织间通信没有补充信息。

15.3.3 团体职能的审计

GB/T 22081-2008 中 15.3，信息系统审计考虑部分，补充的控制措施如下：

控制措施

每一个信息共享团体宜明确说明成员审计其他成员的系统及所有可信服务提供方的系统的权利。

实施指南

审计成员系统的权威机构可能限定在可信第三方，如 TICE 或 WARP。