ICS 35.040
L 80

# 中华人民共和国国家标准

GB/T 32920—2016/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)

2016-08-29 发布　　2017-03-01 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

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准使用翻译法等同采用国际标准 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》(英文版)。根据 GB/T 1.1—2009 和 GB/T 20000.2—2009 的规定,做了如下一些编辑性修改:

——在本标准的引言中,添加“标准中‘针对行业间和组织间通信没有附加的信息’,指的是 GB/T 22081—2008中对应条款没有附加的信息”;

——在本标准的第 3 章中,添加 3.2 缩略语;

——在本标准附录 B.3 中,“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”放到脚注中;

——在本标准附录 C 中,“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”放到脚注中;

——在本标准 4.2 和 7.3.3 中,分别添加参见附录 A 和参见附录 B,以符合 GB/T 1.1—2009 中提到“每个附录均应在正文或前言的相关条文中明确提及”。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:山东省标准化研究院、厦门市美亚柏科信息股份有限公司、中国信息安全认证中心、江苏省电子信息产品质量监督检验研究院、贵州大学、泰安市技术监督情报所。

本标准主要起草人:王曙光、王庆升、公伟、隗玉凯、栾江霞、吴鸿伟、魏军、李旭、李智、赵倩倩、黄申、吴兰、潘平、杨平。

# 引　言

本标准是对 GB/T 22080—2008（ISO/IEC 27001：2005，IDT）和 GB/T 22081—2008（ISO/IEC 27002:2005,IDT)在信息共享团体中使用的补充。本标准包含的指南不包括信息安全管理体系(ISMS)标准族内其他标准中给出的通用指南,并与之互为补充。

GB/T 22080—2008 和 GB/T 22081—2008 采用一种通用的方式处理组织间的信息交换。当组织希望与多个其他组织进行敏感信息[1)]通信时,对敏感信息在其他组织中的使用将受到接收组织实现的充分安全控制的保护,发起方必须有信心。这可通过信息共享团体的建立来达到。信息共享团体中,虽然成员组织之间可能存在竞争,但每个成员仍信任其他成员会保护已共享信息。

只有建立了信任的信息共享团体才能有效运行。信息提供方必须能够信任接收方不会泄露或不当的使用数据。同时,基于发起方给出的所有资质,信息接收方必须能够信任信息是准确的。以上两个方面都很重要,它们必须得到明确有效的安全策略和良好实践应用的支持。为达到此目标,所有团体成员必须实现一个涵盖已共享信息安全的通用管理体系,即信息共享团体的信息安全管理体系(ISMS)。

此外,在并不是所有接收方都将为发起方所知的信息共享团体之间,也可进行信息共享。如果在这些团体及其信息共享协议之间建立起充分的信任,这种信息共享将可进行。特别相关的是在不同团体之间(如不同产业或市场行业)共享敏感信息。

本标准提供了使用已建立的通讯和其他技术方法如何满足规定要求的指南和通用原则。其目的是支持在交换和共享敏感信息时创建信任,从而促进信息共享团体的国际化发展。

标准中“针对行业间和组织间通信没有附加的信息”,指的是 GB/T 22081—2008 中对应条款没有附加的信息。

本标准题目中“通信”主要是指进行信息交换与共享,包括书面、口头、电子等所有形式信息交换与共享。

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。

# 信息技术　安全技术　行业间和组织间通信的信息安全管理

## 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有关发起、实现、维护与改进信息安全的控制和指南。

本标准适用于行业间各种公共和私有的、国内的和国际的所有形式的敏感信息交换与共享。特别是,本标准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　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 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文件:

| | | |
|---|---|---|
| CVE | 公共漏洞和暴露 | (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、建议和报告中心 | (Warning, Advice and Reporting Points) |

## 4 概念和释义

### 4.1 简介

本标准第5章至第15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—2008中定义了组织间双方涵盖信息交换的控制,以及用于公开可用信息的通用分发控制。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信息,这些信息在某些方面是敏感的且仅限于对团体内成员公开可用。通常,这些信息只能对每个成员组织内特定的个体可用,或者有诸如信息匿名化等其他安全要求。本标准定义附加的控制,并提供对GB/T 22080—2008和GB/T 22081—2008的附加指南和解释,以满足这些要求。

### 4.2 信息共享团体

为了有效运行,信息共享团体必须具有某些共同利益或其他关系来确定共享的敏感信息(参见附录A)的范围。例如,团体可能是特定的行业,且成员关系限制在本行业的组织内。当然,实际中还存在一些共同利益的其他基础,例如地理位置或通用所属关系等。

### 4.3 团体管理

信息共享团体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,管理承诺是必不可少的。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。

宜考虑一个信息共享团体中成员组织间的差异。这些差异可包括:

——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 支持性机构

许多信息共享团体将会选择建立或者指定一个集中的支持性机构来组织和支持信息共享。这样一个机构可提供许多支持性的控制,这些控制(如源头和接收方的匿名化)比成员间直接通信更加方便有效。

现实中存在许多不同的、可用于创建支持性机构的组织模型。本标准附录D描述了两个通用模型,即可信信息通信机构(TICE)及预警、建议和报告中心(WARP)。

### 4.5 行业间通信

许多信息共享团体将以行业为基础,这提供了共同利益的一个固有范围。然而,这种团体共享的信息很有可能对其他行业建立的其他信息共享团体有意义。在这种情况下,很可能要在原有信息共享团体的基础上再一次基于一些共同利益(如共享信息的自然属性)建立信息共享团体,这称为行业间通信。

由于可在支持性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,因此每一个信息共享团体中支持性机构的存在极大地支持了行业间通信。同时,通过支持性机构的使用也可达到某些行业间通信所要求的源头或接收方组织匿名化。

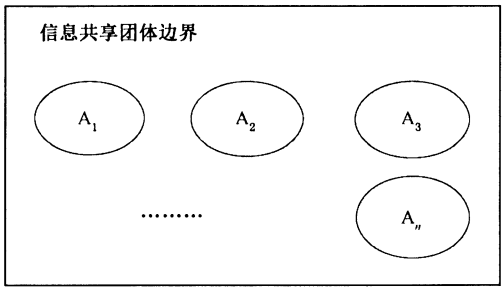
### 4.6 符合性

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所创建和运行的信息安全管理体系(ISMS)均可对照未加修改和增加的 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,将有许多需要解释的地方。

首先需要解释的是本标准中所涉及的组织的定义。

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将是组织,如图 1 所示。




说明:

$A_k$——团体的成员组织 $k$($k=1\cdots n$),包括所有支持性机构。

**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人员均将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。

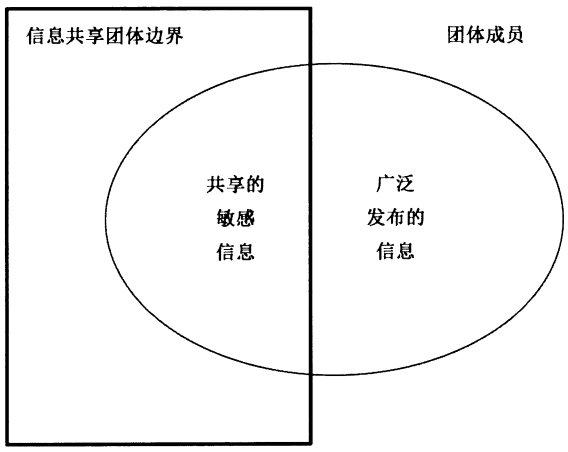



**图 2 团体成员的一部分在范围内**

信息共享团体的成员可能有自己的信息安全管理体系,因此某些过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,对这些过程的要求至少在理论上可能存在冲突和不兼容,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的风险评估方法时[GB/T 22080—2008,4.2.1 c)],其将需要认识到风险对不同的团体成员的影响可能不同。因此,团体将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。

测量所选控制的有效性[GB/T 22080—2008,4.2.3 c)]将需要信息共享团体全体成员的参与。关于自身环境中控制有效性情况,所有成员将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,通过如下参与方描述个体敏感通信:

——信息事项的源头是发起信息事项的人员或组织;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。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自身身份的设施。

——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设施。

## 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 中控制 5.1.1 补充如下:

**实施指南**

信息安全方针文件宜定义团体成员将如何共同制定信息共享团体的安全管理策略和指南。它宜使团体内参与信息共享的所有员工可用。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 中控制 5.1.2 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身份的重大变更信息。

## 6 信息安全组织

### 6.1 内部组织

针对行业间和组织间通信没有附加的信息。

### 6.2 外部各方

#### 6.2.1 与外部各方相关风险的识别

针对行业间和组织间通信没有附加的信息。

#### 6.2.2 处理与顾客有关的安全问题

针对行业间和组织间通信没有附加的信息。

#### 6.2.3 处理第三方协议中的安全问题

GB/T 22081—2008 中控制 6.2.3 补充如下：

**实施指南**

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团体服务供给的协议，宜确保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

针对行业间和组织间通信没有附加的信息。

#### 7.1.2 资产责任人

针对行业间和组织间通信没有附加的信息。

#### 7.1.3 资产的可接受使用

GB/T 22081—2008 中控制 7.1.3 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 中控制 7.2.1 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、可信性和关键性予以分类。

**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性进行分类。宜按照信息源头的信誉、技术内容和描述质量进行评估。

同样的，敏感性可取决于除维护信息保密性需要之外的很多方面，如信息泄露的影响、信息分发的紧迫性或危害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“公司保密”（RFC 4021[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”，不明确。

#### 7.2.2 信息的标记和处理

针对行业间和组织间通信没有附加的信息。

### 7.3 信息交换保护

GB/T 22081—2008 第 7 章，资产管理，增加的控制目标为：

| |
|---|
| 目标：确保信息共享团体中信息交换得到充分保护。<br>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。<br>当有匿名请求时，宜移除可标识信息交换源头的所有信息。同样的，宜在不泄露接收方身份的情况下接收共享的信息。<br>宜控制团体之外共享信息的发布。 |

#### 7.3.1 信息传播

**控制措施**

基于团体确定的预定义传播标记，宜限制接收成员间的信息传播。

**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，已有消息包含的知识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 信息免责声明

**控制措施**

每一次信息交换宜从一个免责声明开始，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实现声明中的内容，接收方宜要求发起方解释清楚。

#### 7.3.3 信息可信性

**控制措施**

每一次信息交换宜指出发起方在所传送信息的可信性和准确性方面的信任程度。

**实施指南**

鉴于紧迫性、潜在后果和技术限制，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，限制宜被指出作为消息的一部分。

信息源头匿名或未知的情况下，指出信息可信性（参见附录 B）的保留特别重要。指出发起方已能验证直接给出的信息与发起方保证信息真实性的情况也很重要。

#### 7.3.4 信息敏感性降低

**控制措施**

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，供应的信息的敏感性是否将降低。

**实施指南**

即使供应的信息的敏感性随时间降低，信息可能仍需保护。分类指南(见 7.2.1)可能需包含针对敏感性降低的默认控制。

### 7.3.5 匿名源头保护

**控制措施**

团体成员在发起或接收的有匿名请求的所有通信中，宜移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)获得批准。发起方还宜询问源头，是否可以将其标识为信息的原始提供方。

由于内容分析可能泄露源头身份，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，宜请求源头对匿名信息和目标接收方名单进行评审。

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漏事件源头。

存在能够在不危害匿名性的情况下保证数据真实性的技术机制。例如，共享的密码秘密可用于确认发起于团体成员的通信，而不泄漏发起者的真实身份。

### 7.3.6 匿名接收方保护

**控制措施**

经发起方批准，团体成员宜能在不泄漏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**

行业团体希望保持成员关系详细信息的私密性，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批准，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，需要授予通用发布的批准或特定行业发布的批准。

**其他信息**

交通信号灯协议(参见附录 C)通常用于指出不寻求附加批准情况下信息可如何进一步分发。

## 8 人力资源安全

### 8.1 任用之前

### 8.1.1 角色和职责

针对行业间和组织间通信没有附加的信息。

#### 8.1.2 审查

针对行业间和组织间通信没有附加的信息。

#### 8.1.3 任用条款和条件

GB/T 22081—2008 中控制 8.1.3 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太可能保持一致。对于将可访问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

针对行业间和组织间通信没有附加的信息。

### 8.3 任用的终止或变化

针对行业间和组织间通信没有附加的信息。

## 9 物理和环境安全

针对行业间和组织间通信没有附加的信息。

## 10 通信和操作管理

### 10.1 操作规程和职责

针对行业间和组织间通信没有附加的信息。

### 10.2 第三方服务交付管理

针对行业间和组织间通信没有附加的信息。

### 10.3 系统规划和验收

针对行业间和组织间通信没有附加的信息。

### 10.4 防范恶意和移动代码

#### 10.4.1 控制恶意代码

GB/T 22081—2008 中控制 10.4.1 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消息扫描，从信息共享团体其他成员处接收的信息宜针对已有恶意代码进行扫描。

#### 10.4.2 控制移动代码

针对行业间和组织间通信没有附加的信息。

### 10.5 备份

针对行业间和组织间通信没有附加的信息。

### 10.6 网络安全管理

针对行业间和组织间通信没有附加的信息。

### 10.7 介质处置

针对行业间和组织间通信没有附加的信息。

### 10.8 信息的交换

#### 10.8.1 信息交换策略和规程

针对行业间和组织间通信没有附加的信息。

#### 10.8.2 交换协议

GB/T 22081—2008 中控制 10.8.2 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

针对行业间和组织间通信没有附加的信息。

#### 10.8.4 电子消息发送

GB/T 22081—2008 中控制 10.8.4 补充如下：

**实施指南**

所有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。任何支持性机构宜内部实现这些规则。

信息共享团体宜考虑实现不依赖于电子消息发送的信息共享替代机制，且考虑使成员规定特定消息由这些替代路径分发。

#### 10.8.5 业务信息系统

针对行业间和组织间通信没有附加的信息。

### 10.9 电子商务服务

针对行业间和组织间通信没有附加的信息。

### 10.10 监视

#### 10.10.1 审计记录

GB/T 22081—2008 中控制 10.10.1 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的内部传播。

#### 10.10.2 监视系统的使用

针对行业间和组织间通信没有附加的信息。

#### 10.10.3 日志信息的保护

针对行业间和组织间通信没有附加的信息。

#### 10.10.4 管理员和操作员日志

针对行业间和组织间通信没有附加的信息。

#### 10.10.5 故障日志

针对行业间和组织间通信没有附加的信息。

#### 10.10.6 时钟同步

针对行业间和组织间通信没有附加的信息。

## 11 访问控制

针对行业间和组织间通信没有附加的信息。

## 12 信息系统获取、开发和维护

### 12.1 信息系统的安全要求

针对行业间和组织间通信没有附加的信息。

### 12.2 应用中的正确处理

针对行业间和组织间通信没有附加的信息。

### 12.3 密码控制

#### 12.3.1 使用密码控制的策略

GB/T 22081—2008 中控制 12.3.1 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，如通过信息权管理实现。

#### 12.3.2 密钥管理

针对行业间和组织间通信没有附加的信息。

### 12.4 系统文件的安全

针对行业间和组织间通信没有附加的信息。

### 12.5 开发和支持过程中的安全

针对行业间和组织间通信没有附加的信息。

### 12.6 技术脆弱性管理

针对行业间和组织间通信没有附加的信息。

## 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 中控制 13.1.1 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。团体宜协商一致并发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价值的潜在事态。

为了保护发起方的声誉，保持事件保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，在无需泄露事态和事件所有后果情况下，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，提供规划维护操作的共享服务的成员例行公告中，可能要求其他成员在维护活动开始之前评审替代提供者的可靠性。

#### 13.1.2 报告安全弱点

针对行业间和组织间通信没有附加的信息。

#### 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，增加的控制为：

**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

针对行业间和组织间通信没有附加的信息。

#### 13.2.2 对信息安全事件的总结

GB/T 22081—2008 中控制 13.2.2 补充如下：

**实施指南**

宜基于信息共享团体分发的信息实施调查，以降低类似事件的风险，并且更好地理解面向团体和所有相关重要信息基础设施的风险。此调查可由相关团体成员或已有的支持性机构实施。

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，以触发对安全事件响应规划、相关规程和业务风险配置的更新。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过程是起作用的。

#### 13.2.3 证据的收集

针对行业间和组织间通信没有附加的信息。

## 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

针对行业间和组织间通信没有附加的信息。

#### 14.1.2 业务连续性和风险评估

GB/T 22081—2008 中控制 14.1.2 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应的依赖。

#### 14.1.3 制定和实施包含信息安全的连续性计划

GB/T 22081—2008 中控制 14.1.3 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关注与其他成员交换敏感信息的需求，并将其作为恢复过程的一部分。

#### 14.1.4 业务连续性计划框架

针对行业间和组织间通信没有附加的信息。

#### 14.1.5 测试、维护和再评估业务连续性计划

针对行业间和组织间通信没有附加的信息。

## 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 中控制 15.1.1 补充如下：

**实施指南**

信息共享团体宜适当考虑所有与信息共享有关的相关协议、法律和法规如反垄断法律或法规。这样可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)

针对行业间和组织间通信没有附加的信息。

#### 15.1.3 保护组织的记录

针对行业间和组织间通信没有附加的信息。

#### 15.1.4 数据保护和个人信息的隐私

针对行业间和组织间通信没有附加的信息。

#### 15.1.5 防止滥用信息处理设施

针对行业间和组织间通信没有附加的信息。

#### 15.1.6 密码控制措施的规则

针对行业间和组织间通信没有附加的信息。

#### 15.1.7 信息共享团体的义务

GB/T 22081—2008 中 15.1，符合法律要求，增加的控制为：

**控制措施**

信息共享团体所有成员宜阐明、理解及批准义务问题和补救措施，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公告，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，仍宜将公告反馈给源头。这可通过可信第三方的媒介(如 TICE)来达到。

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

针对行业间和组织间通信没有附加的信息。

### 15.3 信息系统审计考虑

#### 15.3.1 信息系统审计控制措施

针对行业间和组织间通信没有附加的信息。

#### 15.3.2 信息系统审计工具的保护

针对行业间和组织间通信没有附加的信息。

#### 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，增加的控制为：

**控制措施**

每一个信息共享团体宜规定对其他成员的系统及所有可信服务提供方的系统，审计其成员权利。

**实施指南**

审计成员系统的机构可限定在可信第三方，如 TICE 或 WARP。

# 附 录 A
（资料性附录）
共享敏感信息

## A.1 引言

作为一种有重要价值的资产，敏感信息在组织间共享时必须得到安全的管理。为了解决业务问题并作出更好的决策，敏感信息必须及时交付，特别是它对于组织非常关键时更应如此。

信息共享团体可代表很多类型的组织甚至是个人。团体在成员关系方面可能有很大不同，团体也可能与诸如特定产业或市场行业等业务活动形式紧密匹配在一起。团体既可能处于公共行业又可能处于私有行业，或可能包含这两种行业的成员。共享某种类型的敏感信息，并接受协商好的关于治理这些敏感信息使用的控制和过程，实现上述要求是一个共同的期望。

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。这些过程宜确保将信息传播给合适的人，同时对信息不会被用于恶意目的提供合理保障，这些过程宜确保信息不会被任意再分发而变成实质上公开的信息。

分发的有效性将由成员在信息共享团体所建立的关系中持有的信任程度确定。同时，通信有关的安全机制宜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，因此导致不当行为而可能浪费或误导资源以及对组织产生影响的。

为了使信息共享团体有效运行，信息接收方必须获得其成员组织的授权，以对所接收信息进行操作。且信息接收方不能滥用这些信息，如用于获得商业利益。

## A.2 挑战

为了应对以下挑战，强烈推荐对行业间和组织间通信进行恰当的信息安全管理，否则可能影响正常的业务状况并可能导致事件发生过程中的业务中断：

——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事项：

——风险知识和管理。

——传播和通信。

——监视。

虽然宜根据这三项要素各自的特定价值采用它们，但它们之间密切联系、互为补充。

只有与其他成员代表们建立了个人关系，信息共享团体成员间才能更好地建立信任。人们需要通过面对面的交流建立关系，并创建在彼此可信性和判断力上的信心。只使用远程通信技术很难创建信任。同样，对信息源头的可信性给予信心而保持源头匿名的机制也很难建立。通常，如果人们对确信自

己的身份保密性有信心，他们将更好地畅所欲言。

即使不是所有成员都与其他成员共享所有的信息，信息共享团体仍是效的。分发机制必须足够灵活，以使分发能够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“看门人”面临着特殊困难：信息源头不一定了解其他团体的成员关系，必须依靠接口来保护匿名及其他发布情形；“看门人”可能由于缺乏专业知识而无法意识到何时不宜再进一步进行某些团体通信。与行业间通信相比，这些问题通常在国家间通信中显得更为突出。

## A.3 潜在益处

与其他成员共享敏感信息不可避免的增加了不当泄露的潜在风险。为使团体有效运行，必须管理这些风险并使其最小化，且益处必须超过可接受残余风险。

共享敏感信息的潜在益处包括：

——风险环境中任何重大变更的风险提示，如新威胁、攻击更新的可能性、最新发现的漏洞等等。

——通过共享最佳实践改进安全性。

——访问从任何公开源不能得到的一些有用信息。

——通过消除重复工作节约成本。

——通过更多的理解威胁和脆弱性更好地进行风险评估。

——从其他组织类似活动涉及的信息中，更好地组织维护及介入。

——为安全事件进行更充分的准备。

——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策略。

团体的监视和评审过程从团体成员关系中识别具体益处，以用于成员评估他们持续的团体成员关系，这是必要的。

## A.4 适用性

信息交换可在许多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。然而，在同一行业内运行的组织或具有共同目标的组织，它们共享特定行业类别的信息安全风险，通常可获得最大益处。GB/T 25067—2010（ISO/IEC 27006:2007，IDT）识别了部分这样的行业。

行业间或者通过基于其他特征（如地理位置）确定团体的方式共享信息，或者通过与分层结构团体中其他基于行业的信息共享团体共享信息，也可获得信息共享的极大益处。

## 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；

——信息共享团体的目的和给成员的预期益处；

——成员加入或退出信息共享团体的规程；

——治理所有集中式团体过程或机构（如 TICE 或 WARP）的规则和条款；

——有关团体成员义务、纪律处理和开除的过程与准则的规则和条件；

——针对成员可如何使用和传递共享信息的清晰规则；

——团体成员关系的其他法律和财务的义务及条件。

信息共享团体的规则和条件还宜：

——确保信息以一种高效和安全的方式通信，这种方式确保目标受众及时恰当的接收数据；

——针对每个已识别的信息类型，按照传输其数据时信道的优先使用权，规定和排列潜在的和选定的通信信道；

——规定允许将信息传递给团体成员的环境；

——规定与团体通信相关的强制与可选的数据保护及分发属性；

——规定清晰规则，以解释涉及到信息传播的数据保护及分发属性；

——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；

——若有可能，为信息交换规定或调整现有的消息传递标准。

通信规则应定义通信的频次、接收确认的所有要求以及所有优先级准则或升级准则。规则宜认识到信息共享团体成员在团体其他成员处的信任级别可能有所不同。随着时间和情形不同，信任程度可能不同。

当传递团体支持的已识别信息类型时，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、代价等准则，通过评估优缺点选择适合的通信信道。可能的通信信道的例子包括电子消息发送、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。

并非所有的信息都需要实时进行通信，有些信息最好通过例行接触进行共享。

对于何时将信息传输给团体成员的可能例子，包括：立即报告与预先确定配置相符的被检测事件，按时例行报告，或响应来自其他成员的信息请求。数据保护和分发属性的可能例子包括：隐藏信息源的要求、信息的敏感性或发起方对信息信赖性评估。解释数据保护和分发属性的一组规则的例子是交通信号灯协议(TLP)，参见附录C。基于所使用的通信信道，属性可能不同。例如，邮政分发的强制属性与互联网邮件的强制属性可能有很大不同。

无论选择和实现何种技术解决方案，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。面对面的交流能够建立信任，并且对于通过邀请新成员而扩大团体，这可能是一种必要方式。然而，可信平台及其他共享基础设施的存在本身就可促进成员关系。

### A.6 信息交换协议

信息交换协议中，信息共享团体宜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P2P通信、分层结构或集中式的支持性机构(如TICE或WARP)进行交换。

信息交换协议可允许信息只被选定的信息共享团体成员共享，或者仅可被匿名共享。同样的，即使存在集中式报告设施，也可允许在成员间直接传递信息。

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

可能的信息类型的例子包括：

——“公告”，对应于告知性的解释事态；

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

——“事件处理”，对应于实际事件有关的分析、响应支持和响应协调；

——“信息请求”，对应于从团体某个成员传送到所有或一些其他团体成员的信息的请求；

——“服务质量预测”，提供各种团体通信信道有效性和可靠性预测的信息。

除非包含适合的数据过滤方法，否则信息共享过犹不及。如果构建趋势信息被认为是共享的一大益处，那么必须存在一种能够区别高优先级的“立即行动”信息和低优先级的“列入记录”信息的方法。

## A.7 成功因素

尽管并不是所有成员可能对所有方面感兴趣，但有效的团体将有真正的共享利益。例如，固网电信公司对无线问题不感兴趣，但是同移动公司一样都将对识别骗局电话感兴趣。

有效团体的成员将利用获得授权的代表，这些代表可促成事情内部发生。

有效的团体可限制成员或以其他方式约束成员关系，例如在决策方面确保公平的代表。

## 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；

——由团体成员实现的破坏共享信息的过程。

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
（资料性附录）
信息交换中的建立信任

## B.1 陈述信任

在收到的陈述中，接收方的信任程度主要基于消息源头被信任的程度和陈述中源头自身信任。

用于执法机关和情报机构的“5 * 5”模型或许是对此最好的概括：

——{A--E}源头中信任程度的递减；

——{1--5}信息中源头赋予的信任程度的递减。

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。虽然源头和信息都被期望是绝对可信的，但现实中总是存在偶然性误差。可能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”项的材料。

陈述中关于信任的进一步问题是不明确的增强信任所带来的风险。存在一种内在倾向或潜在假设，即看似不同来源的相同信息的多个实例是确定的。

在一定程度上，这显然是准确的，但这种信任不能仅从字面上去理解，特别的，任何此类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 引言

目前已开发出多种技术，可为未知的或不常见机构产生的电子供应信息支持信任。这些技术同Web 2.0[4]的概念密切相关。Web 2.0不是一组技术，确切地说，它是一个有关社交媒体和融合思想的理论或概念，例如将Web用作一个平台，从而利用集体智慧。

Web 2.0中以下两个方面对本标准特别重要：

——伪匿名；

——信誉系统，也称作信誉引擎。

### B.2.2 匿名和伪匿名

由于各种各样的原因，信息源头和接收方可能希望保持匿名。匿名实际能达到的强度取决于背景知识即对整个消息传递系统的了解。在大型、分散式的系统中，所有参与者可能不能完全了解消息传递系统，且在很多情况下，消息的背景将是随着时间变化的。

匿名的概念与**不可链接性**的概念紧密联系在一起，即观察后得到的利益项之间的关联与从先验知识中得到的利益项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或多个接收方关联起来。

**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，以阻止识别数据对象，或至少使这样的识别本质上变得困难。**假名化**是使用伪匿名或笔名作为标识标签的一种状态。

有关链接性程度，各种类型的笔名可能是：

a) 个人笔名：个人笔名是被看作代表持有人公民身份的姓名的替代品。它可用于各种环境下，例如身份证号码、社会安全码、昵称、演员的艺名或移动电话号码。

b) 角色笔名：角色笔名的使用限于特定的角色，例如顾客笔名或用于相同角色“因特网用户”的许多实例化的 Internet 账户。相同的角色笔名可能与不同的通信合作者使用。

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未必知道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。

   例如，假设信息源在非公共领域与 Bernstein 进行信息通信时经常使用“Wool”这个名字，而与 Woodward 进行相同的信息通信时使用“Touched”。后 Bernstein 和 Woodward 各自分别从“Deep Throat”和“Watergate”接收了关于某个新课题的信息。Bernstein 和 Woodward 不知道“Deep Throat”和“Watergate”是否是同一人，也不知道“Deep Throat”是否与“Wool”或“Touched”是同一个人，或与后两者都是同一个人。

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，且至少在开始时与所有其他事务笔名不可链接的事务笔名，例如，随机生成的网上银行事务号码。因此，事务笔名可用于实现尽可能强健的匿名。

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 信誉引擎

信誉引擎的概念是构成 Web 上许多社交媒体和社交网络的基础。信誉引擎用于筛选与之相关度最高的信息，且随着信息数量和信息种类的显著增加，它们相关度变得越来越高。

信誉引擎是指正式的一组策略和规程，这些策略和规程主要用于计算基于个体过去活动的信誉分数。在网络世界中，信誉引擎与数字足迹的思想紧密联系在一起，而数字足迹即数字环境中追溯某人活动的痕迹。

信用报告和其他机制总是可以提供手段以量化信誉，但相比传统信用报告，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，就创建了数字数据。尽管此数据属于个人，但它会被信用评级机构之类的第三方获取并占有。（事实上，为了获取它们可能需要支付费用！）

现在已经有越来越多形式完善的信誉引擎，如 eBay 信誉引擎。由于是透明的，因此它不同于信用分数。且每一个反馈（包括负反馈）都返给评论的当事人，因此这也提供了一个申诉的机会。

信誉引擎可通过确认新的信息源头、确认内容源头、实时告警诸如 Twitter 搜索和 Google 告警、增强未知源头的信任、通过外部洞察力补充搜索、为可信共享域引入新的或外部思想、预测来自外部源头的机会与威胁等任务，融合更广泛团体源头的洞察力来增加信任。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，因此在用于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[5] 方法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。

这种方法的可能组成部分包括：

a) 信息的发起方宜在他们发布的信息中赋予信任等级[2)]。

b) 理想情况下，宜使用结构化数据格式清晰地识别所有信息的源头。

c) 除了源头标识的概念，还宜支持匿名报告，因为安全领域的经验表明，匿名措施极大的增加了信息共享。

d) 可用于封装任何信息交换实质内容的边界对象。边界对象是对团体利益有一定程度的相互承认的信息的结构化组合，这样就可跨越语言和域边界进行通信：例如 Mitre 的公共漏洞和暴露(CVE)标记的成功，在一定程度上要归功于其实际采用了这种边界对象。

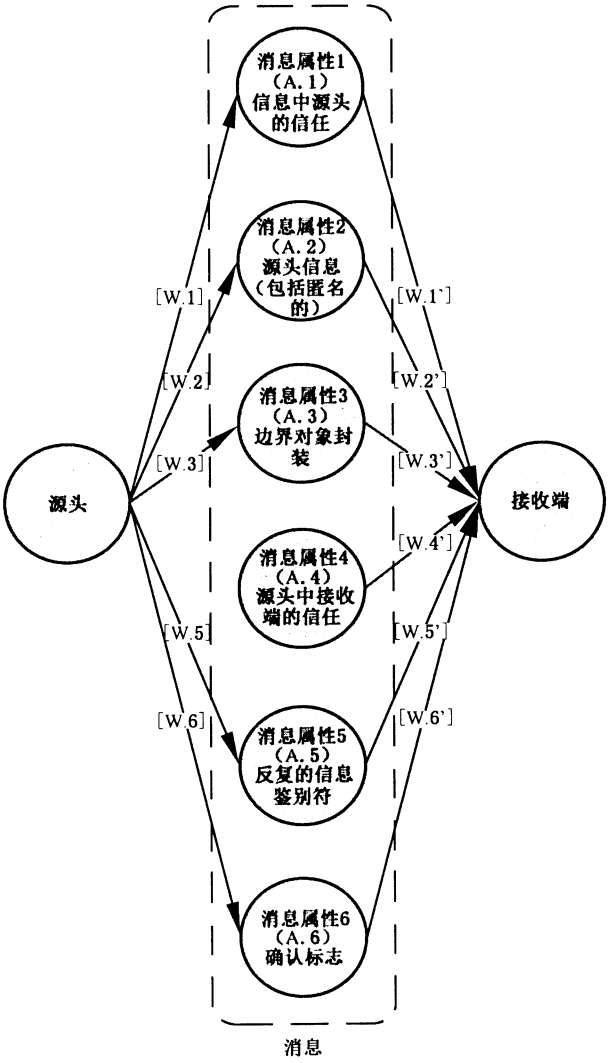
e) 可信信息交换的发起方和接收方都宜提供一份关于信息是否支持以前所接收的内容以及支持次数的评估：尽管在一些范围内存在为此目的进行的自动信息分析，但应该认识到，在当前最新技术下为此目的进行的自动信息分析是不可靠的。为了最小化似是而非的增强信任所带来的风险，需要将回报递减的累积分布函数用于以前实例的计数，这将意味着附加信息的加权值随着计数值的增大而减小。

f) 源头或接收方就信息是否已独立的经过确认的问题为信息赋予一个标志，以避免将所谓的都市传说当作有用信息。这样体现了对接收的信息保持进一步一定程度的关键性怀疑。

g) 信息接收方宜基于 5 * 5 模型为源头赋予一个主观评价(见 B.1)。

这些准则经过合适的加权可以使信息共享团体成员量化信任，信任量化值可以且宜加入从团体其他成员处收到的信息中，如图 B.1 所示。

2) 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。




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
## （资料性附录）
## 交通信号灯协议

此附录描述了交通信号灯协议，该机制广泛用于信息共享团体中以指出允许的信息分发。尽管基本概念已为众人所知，但在使用中存在许多细微的不同变化[3)]。

交通信号灯协议（TLP）的创建是为了鼓励不同组织间更多地共享敏感信息。如果共享敏感信息，发起方需示意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。当要求更广泛的传播时，接收方必须咨询发起方。

四种颜色和它们的含义如下：

——“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。发起方可能被期望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。然而信息可能既没有公布或发布到 Internet 上，也没有在团体外发布；

——“白色”无限制的。在标准版权规则约束下，“白色”信息可自由分发而不受任何限制。

无论如何，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被视为“琥珀色”。然而，默认情况下，敏感信息源头的身份将总是“红色”，在信息披露时作了特别说明的除外。

TLP 也适宜组织内使用，例如只授予某些个体可以完全访问所有共享信息的情况，见图 2。

3) 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
（资料性附录）
组织一个信息共享团体的模型

## D.1 引言

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。此附录描述了在实践中可见的、支持有效的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 引言

作为集中式的协调和沟通门户，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。它可成为行业间和组织间通信中有效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的和安全的信息交换，并帮助成员有效地监视、分析、管理对事件及风险的响应。

可信信息通信机构(TICE)由一组主题专家组成，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；

——为从破坏中恢复，处理事件并支持团体成员；

——通过以下方法向团体成员提供相关的信息安全意识：

——发布当前使用组件中的漏洞公告；

——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 可作为使共享信息的源头或接收方匿名的可信中介，从而使得成员对信息来自于可信源头有信心，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)。但是，ISIRT 需在提供一般的响应式服务基础上，扩展业务以提供主动式 TICE 服务。

### D.2.2 TICE 组织上的考虑

#### D.2.2.1 主题专家

为确保具有恰当技能的合适人选参与其中，并确保专家能够确定双向通信及相关信息基础设施环境中所有信息的相关性，TICE 组织结构应由公共专家或行业专家组成。

宜通过专家进行分析，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；

——法律部门。

专家要么是兼职或全职，且可能在控制中心或运行现场，要么是它们的结合。

#### D.2.2.2 组织结构

一个典型的 TICE 宜至少包含以下职能：

——执行委员会(必不可少，负责 TICE 战略管理和团体成员关系)；

——运行技术组(必不可少，负责分析业务和技术风险问题，确定应用补丁或变更时恰当的适用性)；

——运行技术通信人员(可选，推荐他们负责提高 TICE 对组件集成层面涉及的运行环境或资源的认识)；

——法律专家(可选，但是特别推荐他们在 TICE 起始阶段平息法律问题)；

——通信专家(可选，推荐他们负责关注有关技术问题的翻译困难，从而为成员准备更易于理解的消息)。作为团体成员和运行技术组之间的推动者，通信专家可提供从团体成员向运行技术组的反馈。

#### D.2.2.3 团体成员管理

为确保团体成员间关系恰当可信，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

对 TICE 而言，合适的组织模式很大程度上取决于当前结构的适当性、团体成员的性质、扩展此 TICE 能完成所述服务的潜能。同时，组织模式还取决于永久聘用的或是根据需要临时聘用的主题专家的可访问性。

TICE 至少存在三种可能的模式：

——独立式模式：作为一个独立组织，独立式 TICE 有自己的管理层和员工。

——嵌入式模式：嵌入式 TICE 建立在组织内部并利用其资源提供服务。正常情况和特定情况下，所分配资源的数量可能因支持活动而有所变化。

——自愿式模式：自愿式 TICE 由自愿基础上相互提供建议和支持的专家组成。它宜被视作一个高度依赖于参与者动机的专家团体。

### D.2.3 TICE 核心和可选服务

对于 TICE 提供给团体成员的服务，选择服务是一个关键阶段，宜基于以下事项：

——信息共享团体成员间所提议通信相关的范围和风险；

——TICE 范围、信息共享团体的组织和性质。

此外，它很大程度上取决于团体环境中 TICE 担任的角色(作为成员间信息共享的推动者或发起者)。

潜在的 TICE 核心服务为：

——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，向团体成员响应帮助请求、响应事件的报告。

——主动式服务。主动式服务旨在所有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，确保和促进充分的信息交换。此外，一些主动式服务旨在通过成员的意识降低事发时的影响和范围，以改进事件的预防。

潜在的 TICE 可选服务为：

——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某个组件上发现的所有文件或对象。

——处理并传播结果给团体成员、供应商和其他相关方，以阻止恶意软件的进一步传播和减轻

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长期目标方面帮助团体成员。

——匿名化服务。匿名化服务旨在确保团体成员不向其他成员泄漏自身身份的情况下能发送或接收信息。

#### 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。它特别适合于及时和优先信息共享、分析非常重要的关键环境，以及支持所需中心基础设施成本的成员或政府。

### D.3 预警、建议和报告中心

#### D.3.1 引言

预警、建议和报告中心(WARP)模型[6]自2003年起一直在用，该模型不仅为公共行业的组织间也为私有行业的组织间共享敏感信息提供了一个有效的机制。

通常在自愿的基础上，一个警告、建议和报告中心在具有相似利益的人或组织间共享信息。WARP基于代表信息共享团体成员的人员之间的个人关系。一个典型的WARP包含一个略懂利益主体但主要能擅长与成员沟通的操作者。它的成员数一般在20个到100个之间，否则WARP可能会缺少人与人间的接触，且这些成员属于具有强共同利益的一个团体(小型企业、当地政府、服务提供商、利益群体等)。

WARP成员同意作为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。此共享团体可基于一个产业或市场行业、地理位置、技术标准、利益群体、风险群体或其他任何具有商业意义的共享利益。

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操作员使用网页、电子邮件、电话、短信和偶尔会面(在可能的情况下)给成员发送关于预警和建议的个性化服务。这些通常是IT安全建议(因为安全建议数量多且变化快)，但也包含其他材料(其他威胁、电子犯罪、应急规划等等)。同时，通过使用公告板、会议及通用通信技能，操作员利用成员自身的知识去帮助其他成员。为了其他成员的利益(有点像“邻里照看”方案)，一个成功的WARP通过建立足够的信任以鼓励成员匿名谈论它们自己的事件和问题。

#### D.3.3 WARP服务

##### D.3.3.1 概述

WARP通常提供三种核心服务：

——过滤预警服务-成员从在线标记列表中选择，只接收它们需要的安全信息；

——建议中介服务-成员可通过某个成员的公告板学习其他成员的举措和经验；

——可信共享服务-由于报告匿名，这样成员可以借鉴彼此的攻击和事件而不用害怕遭受尴尬或指责。

##### D.3.3.2 过滤预警

过滤预警服务允许WARP成员接收到基于成员利益范围过滤出来的预警和报告。过滤预警应用

软件使用一个允许 WARP 成员轻松修改和维护他们选择的订阅树'标记列表',帮助 WARP 操作员轻松的及时分类和分发预警和报告。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 团体成员在一个安全环境中讨论良好实践和信息安全问题。在一方已经完成某方面的工作而另一方还正在考虑时,此服务也能使成员向其他人提供他们的经验和技能,这有可能会建立在交易的基础上。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,WARP 的成员可以在了解共享敏感信息将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,报告可通过电话、电子邮件或面对面达成。对事件信息采取安全措施且进行适当匿名处理后,这类事件信息也可传递给其他与其具有信任关系的 WARPs,并传递给政府,以核对和监视国家趋势。此服务实现了 WARP 的报告部分。

#### D.3.3.5 其他服务

WARP 可提供对他们的团体成员有益的其他服务。但是,为了使 WARP 操作员支持他们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 益处

通过提供如下益处,WARPs 为成员提供有效和低成本的信息安全:

——可信环境;

——安全信息过滤;

——获取专家建议;

——对威胁的风险提示;

——战略决策支持;

——改进的安全意识。

与建立 WARP 相关的许多潜在益处中的一些有:

——工作效率:WARP 促进信息共享和共同任务的协调,转而这将减少重复工作。通过提高效率将使企业或政府的提供商获益。

——避免信誉受损:随着组织转向使用更多在线途径与公众互动,网站成为一个关键因素。如果一个网站不可用或网站外观有损伤,这会引起信誉问题并可能阻止网站服务的可接受性。通过成为 WARP 成员,所服务的团体将会得到更好的保护。

——风险提示:找出其他人正在经历的问题和使用的解决方法,并在 WARP 团体内分享这些信息。这将促进独特的和个性化的服务,而甚至是大型商业提供商的服务可能也无法与之匹敌。

——政府和其他 WARPs 的支持:属于这样一个集中式团体的优势意味着从可信源头共享和分发有用建议的能力。来自其他 WARPs 操作上的支持可以通过 WARP 操作者论坛得到很好的建立。过滤预警应用的端到端合作使得其他 WARPs 的预警和报告能够容易的分发。

——低成本:该模型旨在通过最少的人员数量(或虚拟团队)实现低成本。

——全面且免费的工具箱:一个 WARP 提供者有权使用从现有 WARPs 经验中创建的 WARP 工具箱。它包括背景信息,如何启动、创建与运行 WARP,以及一个从报刊文章到市场资料的广泛下载列表。

——可持续性:随着许多相关组织已经成功的运用这种途径验证了其可持续性,目前 WARPs 已开

始广泛建立。

——软件：WARP 提供商有权可使用为支持所有三种 WARP 服务而开发的专业软件。

——增强的可信性：具有非盈利特点及与已有最佳实践的结合，将有助于获得团体信任和增强组织可信性，特别是在公益活动中。

——符合性：WARP 成员关系将帮助成员组织满足 GB/T 22081—2008 中识别的组织接触控制。

——发展潜力：许多现有的 WARP 提供商正在建立进一步的 WARPs 的过程中。这些 WARPs 建立在支持较低成本和较好的可持续性的现有的基础设施和专业知识上。WARPs 目前出现在很多行业，并开始呈现国际化。

——企业社会责任：成为 WARP 的一员增强了成员组织的企业社会责任，从而赢得团体信任，潜在的支持了操作者和成员的其他业务策略。

### D.3.5 结论

WARP 模型为具有相似目的的组织间进行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、自愿基础上运行的情况。

## 参 考 文 献

[1] ISO/IEC 27005:2008 信息技术 安全技术 信息安全风险管理指南(Information technology—Security techniques—Information security risk management)

[2] ISO/IEC 27006:2007 信息技术 安全技术 信息安全管理对认证机构的认可要求(Information technology—Security techniques—Requirements for bodies providing audit and certification of information security management systems)

[3] Internet 工程任务组. RFC 4021: Registration of Mail and MIME Header Fields [S/OL]. (2005-5)[2011-10]. http://datatracker.ietf.org/doc/rfc4021/

[4] O'REILLY, Tim. What Is Web 2.0-Design Patterns and Business Models for the Next Generation of Software. O'Reilly Web Blog [EB/OL]. (2005-9-30)[2011-10]. http://oreilly.com/web2/archive/what-is-web-20.html

[5] WIKIPEDIA, THE FREE ENCYCLOPEDIA. Pareto distribution [EB/OL]. (2011-4-25)[2011-10]. http://en.wikipedia.org/wiki/Pareto_distribution

[6] CENTRE FOR THE PROTECTION OF NATIONAL INFRASTRUCTURE (UK). WARP Homepage [EB/OL]. (2010-4)[2011-10]. http://www.warp.gov.uk