



中华人民共和国国家标准

GB/T 25068.1—20XX/ ISO/IEC 18028-1

信息技术 安全技术 IT 网络安全 第 1 部分：网络安全管理

Information technology — Security techniques — IT network security —

Part 1: Network security management

(ISO/IEC 18028-1:2006, IDT)

(报批稿)

(2011 年 4 月 27 日)

20XX – XX – XX 发布

XXXX – XX – XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会 发布

目 次

前言	V
引言	VI
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
3.1 在其他标准中定义的术语	1
3.2 本部分定义的术语	2
4 缩略语	7
5 结构	8
6 目标	9
7 综述	9
7.1 背景	10
7.2 识别过程	11
8 企业信息安全策略要求的考量	13
9 网络体系结构与应用的评审	13
9.1 背景	13
9.2 网络类型	14
9.3 网络协议	14
9.4 网络应用	14
9.5 网络实现技术	15
9.5.1 局域网	15
9.5.2 广域网	15
9.6 其他考量	15
10 网络连接类型的识别	16
11 网络特征与相关信任关系的评审	18
11.1 网络特征	18
11.2 信任关系	18
表 2 中宜确定每个相关信任关系的参考类别。所有可能的类别在后面的表 3 中描述。	19
12 信息安全风险的识别	19
13 识别适当的潜在控制域	24
13.1 背景	24
13.2 网络安全体系结构	24
13.2.1 导言	24

13.2.2	局域网	25
13.2.3	广域网	27
13.2.4	无线网络	28
13.2.5	无线电网络	29
13.2.6	宽带网	30
13.2.7	安全网关	31
13.2.8	远程访问服务	32
13.2.9	虚拟专用网	33
13.2.10	IP 融合（数据、音频、视频）	34
13.2.11	使得对（组织）外部网络所提供服务的访问成为可能	35
13.2.12	万维网托管体系结构	36
13.3	安全服务管理框架	38
13.3.1	管理活动	38
13.3.2	网络安全策略	38
13.3.3	安全操作规程	39
13.3.4	安全合规检查	39
13.3.5	连接的安全条件	39
13.3.6	网络服务用户的文档化安全条件	39
13.3.7	事件管理	40
13.4	网络安全管理	40
13.4.1	导言	40
13.4.2	网络的各个方面	40
13.4.3	角色与责任	41
13.4.4	网络监视	42
13.4.5	网络安全评估	42
13.5	技术脆弱性管理	42
13.6	身份标识与鉴别	42
13.6.1	背景	42
13.6.2	远程登录	43
13.6.3	鉴别增强	43
13.6.4	远程系统身份标识	43
13.6.5	安全单点登录	44
13.7	网络审计日志的载入和监视	44
13.8	入侵检测	45
13.9	恶意代码的抵御	46
13.10	公共基础设施中基于密码的服务	46
13.10.1	导言	46
13.10.2	网络上的数据保密性	46
13.10.3	网络上的数据完整性	46
13.10.4	抗抵赖	47
13.10.5	密钥管理	47
13.11	业务持续性管理	49
14	安全控制措施的实施和运行	49

15 对实施的监视和评审	49
参考文献	52

前 言

GB/T 25068在《信息技术 安全技术 IT网络安全》总标题下，目前由以下5个部分组成：

- 第1部分：网络安全管理；
- 第2部分：网络安全体系结构；
- 第3部分：使用安全网关的网间通信安全保护；
- 第4部分：远程接入的安全保护；
- 第5部分：使用虚拟专用网的跨网通信安全保护。

本部分为GB/T 25068的第1部分。

本部分按照GB/T 1.1-2009给出的规则起草。

本部分使用翻译法等同采用国际标准ISO/IEC 18028-1: 2006《网络安全管理》（英文版）。

作了以下纠正：在第4章的缩略语中纠正一个缩略语的英文原文。纠正的缩略语的英文原文在所在页的边空白处用单竖线“|”标出。13.3.1节中原文有误，已纠正，在页边用单竖线“|”指示本部分由全国信息安全标准化技术委员会（TC 260）提出并归口。

本文件的某些内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任。

本部分由全国信息安全标准化技术委员会（TC 260）提出并归口。

本部分起草单位：黑龙江省电子信息产品监督检验院、中国电子技术标准化研究所。

本部分主要起草人：王希忠、姜波、黄俊强、马遥、方舟、王大萌、树彬、张清江、宋超臣、段志鸣、上官晓丽、许玉娜、王运福、吴梅艳。

引 言

通信和信息技术业界一直在寻找经济有效的全面安全解决方案。安全的网络应受到保护，免遭恶意和无意的攻击，并且应满足业务对信息和服务的保密性、完整性、可用性、抗抵赖、可核查性、真实性和可靠性的要求。保护网络安全对于适当维护计费或使用信息的准确性也是必要的。产品的安全保护能力对于全网的安全（包括应用和服务）是至关重要的。然而，当更多的产品被组合起来以提供整体解决方案时，互操作性的优劣将决定这种解决方案的成功与否。安全不仅是对每种产品或服务的关注，还必须以促进全面的端到端安全解决方案中各种安全能力交合的方式来开发。因此，GB/T 25068的目的是为IT网络的管理、操作和使用及其互连等安全方面提供详细指南。组织中负责一般IT安全和特定IT网络安全的人员应能够调整GB/T 25068中的材料以满足他们的特定要求。GB/T 25068的主要目标如下：

——GB/T 25068.1定义和描述网络安全的相关概念，并提供网络安全管理指南——包括考虑如何识别和分析与通信相关的因素以确立网络安全要求，还介绍可能的控制领域和特定的技术领域（相关内容在GB/T 25068的后续部分中涉及）；

——GB/T 25068.2定义一个标准的安全体系结构，它描述一个支持规划、设计和实施网络安全的一致框架；

——GB/T 25068.3定义使用安全网关保护网络间信息流安全的技术；

——GB/T 25068.4定义保护远程接入安全的技术；

——GB/T 25068.5定义对使用虚拟专用网（VPN）建立的网络间连接进行安全保护的技术。

GB/T 25068.1与涉及拥有、操作或使用网络的所有人员相关。除了对信息安全（IS）和/或网络安全及网络操作负有特定责任的、或对组织的全面安全规划和安全策略开发负有责任的管理者和管理员外，还包括高级管理者和其他非技术性管理者或用户。

GB/T 25068.2与涉及规划、设计和实施网络安全体系结构方面的所有人员（例如IT网络管理者、管理员、工程师和IT网络安全主管）相关。

GB/T 25068.3与涉及详细规划、设计和实施安全网关的所有人员（例如IT网络管理者、管理员、工程师和IT网络安全主管）相关。

GB/T 25068.4与涉及详细规划、设计和实施远程接入安全的所有人员（例如IT网络管理者、管理员、工程师和IT网络安全主管）相关。

GB/T 25068.5与涉及详细规划、设计和实施VPN安全的所有人员（例如IT网络管理者、管理员、工程师和IT网络安全主管）相关。

第1部分：网络安全管理

1 范围

GB/T 25068的本部分规定了网络和通信安全方面的指导，包括信息系统网络自身的互连以及将远程用户连接到网络。总的来说，它适用于那些负责信息安全管理，尤其是网络安全管理的相关人员。本部分支持识别和分析与通信相关的因素，这些因素宜在建立网络安全要求时考虑到；针对与通信网络连接相关的安全，介绍如何识别适当的控制域；综述可能的控制域，包括在GB/T 25068.2至GB/T 25068.5中详细论述的那些技术设计和实施主题。

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，仅所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 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/Z 20985-2007 信息技术 安全技术 信息安全事件管理指南（ISO/IEC TR 18044: 2004, MOD）

GB/T 25068.2-20xx 信息技术 安全技术 IT网络安全 第2部分：网络安全体系结构（ISO/IEC 18028-2: 2005, IDT）

GB/T 25068.3-20xx 信息技术 安全技术 IT网络安全 第3部分：使用安全网关的网间通信安全保护（ISO/IEC 18028-3: 2005, IDT）

GB/T 25068.4-20xx 信息技术 安全技术 IT网络安全 第4部分：远程接入的安全保护（ISO/IEC 18028-4: 2005, IDT）

GB/T 25068.5-20xx 信息技术 安全技术 IT网络安全 第5部分：使用虚拟专用网的跨网通信安全保护（ISO/IEC 18028-5: 2006, IDT）

ISO/IEC 13335-1:2004 信息技术.安全技术.信息和通信技术安全的管理.第1部分:信息和通信技术安全管理用概念和模型

GB/T AAAA 信息技术 安全技术 入侵检测系统的选择、部署和操作（ISO/IEC 18043: 2006, IDT）

3 术语和定义

3.1 在其他标准中定义的术语

GB/T 9387（所有部分）中给出的术语和定义适用于本文件。GB/T 22081中定义的术语和下列术语也适用：可核查性、资产、真实性、可用性、基线控制、保密性、数据完整性、影响、完整性、安全策略、抗抵赖、可靠性、风险、风险分析、风险评估、风险管理、控制、威胁和脆弱性。

3.2 本部分定义的术语

下列术语和定义适用于本文件。

3.2.1

报警 alert

“即时”指示信息系统和网络可能受到攻击或因意外事件、故障或人为错误而处于危险之中。

3.2.2

攻击者 attacker

故意利用技术性和非技术性安全控制措施的脆弱性，以窃取或损害信息系统和网络，或者损害合法用户对信息系统和网络资源可用性的任何人。

3.2.3

审计 audit

依照期望对事实进行的正规调查、正规检验或验证，以确认它们之间的符合性和一致性。

3.2.4

审计日志 audit logging

为了评审和分析以及持续监控而收集的有关信息安全事态的数据。

3.2.5

审计工具 audit tools

一种辅助分析审计日志内容的自动化工具。

3.2.6

业务持续性管理 business continuity management

当有任何意外或有害事件发生，且能够对基本业务功能和支持要素的持续性造成负面影响时，确保运行的恢复得到保障。

注：该过程还宜确保恢复工作按所要求的优先级、在规定的时间内完成，且随后将所有业务功能及支撑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规划和设施，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。

3.2.7

Comp128-1早期被SIM卡默认使用的一种专有算法。

3.2.8

非军事区 demilitarized zone

插在网络之间作为“中立区”的边界网络（也称作屏蔽子网）。

注：它形成一个安全缓冲区。

3.2.9

拒绝服务 denial of service

阻止对系统资源的授权访问或延迟系统的运行和功能。

3.2.10

外联网 extranet

组织的内联网的扩展，特别是在公共网络基础设施上的扩展，通过提供对其内联网的有限访问，使得组织和与它有往来的其他组织和个人共享资源。

3.2.11

过滤 filtering

根据指定的准则，接受或拒绝数据流通过网络的过程。

3.2.12

防火墙 firewall

设置在网络环境之间的一种安全屏障。它由一台专用设备或若干组件和技术的组合组成。网络环境之间两个方向的所有通信流均通过此安全屏障，并且只有按照本地安全策略定义的、已授权的通信流才允许通过。

3.2.13

集线器 hub

一种在OSI参考模型（GB/T 9387.1）中第1层工作的网络设备。

注：网络集线器中没有真正的智能，它只为联网系统或资源提供物理连接点。

3.2.14

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控制措施失效，或者一种可能与安全相关但以前不为人知的情况。

注：见GB/Z 20985。

3.2.15

信息安全事件 information security incident

由单个或一系列有害或意外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。

注：见GB/Z 20985。

3.2.16

信息安全事件管理 information security incident management

响应和处理信息安全事态和事件的正规过程。

注：见GB/Z 20985。

3.2.17

互联网 internet

公共域内互连网络的全球系统。

3.2.18

内联网 intranet

在组织内部建立的专用网络。

3.2.19

入侵 intrusion

对网络或连接到网络的系统的未授权访问，即对信息系统进行有意或无意的未授权访问，包括针对信息系统的恶意活动或对信息系统内资源的未授权使用。

3.2.20

入侵检测 intrusion detection

检测入侵的正规过程，其一般特征为采集如下知识：异常使用模式，以及已被利用的脆弱性的类型和利用方式（包括何时发生及如何发生）。

注：见ISO/IEC 18043。

3.2.21

入侵检测系统 intrusion detection system

用于识别某一入侵已被尝试、正在发生或已经发生，并可能对信息系统和网络中的入侵做出响应的技术系统。

3.2.22

入侵防护系统 intrusion prevention system

入侵检测系统的一种变体，专门设计来提供主动的响应能力。

注：见ISO/IEC 18043。

3.2.23

抖动 jitter

因被传输的信号偏离其参考值而造成的一种线路失真形式。

3.2.24

恶意软件 malware

被专门设计用来损害或破坏系统的恶意的软件，诸如病毒或特洛伊木马。

3.2.25

多协议标签交换 multi protocol label switching

一种为了在内部网络路由选择中使用而开发的技术，由此标签被分配给单个的数据路径或数据流，并用于切换连接，处于下层且是一般路由选择机制的附加。

注：标签交换能用作一种创建隧道的方法。

3.2.26

网络行政管理 network administration

日常运营和网络过程及用户的管理。

3.2.27

网络分析仪 network analyzer

用于截取网络中信息流并对其解码的设备。

3.2.28

网络元素 network element

与网络相连的信息系统。

注：安全元素的详细描述见GB/T 25068.2。

3.2.29

网络管理 network management

对网络进行规划、设计、实施、运行、监视和维护的过程。

3.2.30

网络监视 network monitoring

连续观察和评审在网络活动和运行中所记录数据（包括审计日志和报警）的过程以及相关分析。

3.2.31

网络安全策略 network security policy

组织为使用网络资源所制定的一组说明、规则和实践，并指出如何通过以上策略保护网络基础设施和服务。

3.2.32

端口 port

连接的端点。

注：在互联网协议的环境中，端口是TCP或UDP连接的逻辑信道端点。基于TCP或UDP的应用协议通常已分配默认端口号，如为HTTP协议分配端口80。

3.2.33

隐私 privacy

每个人都享有的不公开处理的私人和家庭生活、居所和通信的权利。

注：隐私不得受到当局干涉，而在依照法律，且对于国家安全、公共安全或国家经济与社会稳定，或者对于防止动乱或犯罪、保护健康或道德，或者对于保护他人的权利和自由有必要时除外。

3.2.34

远程访问 remote access

从另一网络或从一个正在访问但未在物理上或是逻辑上永久连接到网络的终端设备来访问网络资源的过程。

3.2.35

远程用户 remote user

所在位置与正被使用的网络资源位置不同的用户。

3.2.36

路由器 router 通过基于路由协议机制和算法选择路径或路由，来建立和控制不同网络之间数据流的网络设备。其自身能基于不同的网络协议。路由信息保存在路由表内。

3.2.37

安全维 security dimension

为处理特定网络安全方面而设计的安全控制措施集。

注：安全维的详细描述见GB/T 25068.2。

3.2.38

安全域 security domain

遵从于共同安全策略的资产和资源的集合。

3.2.39

安全网关 security gateway网络之间或网络内子部分之间或不同安全域内的软件应用之间的连接点，旨在按照给定的安全策略保护网络。

注：安全网关的详细描述见GB/T 25068.3。

3.2.40

安全层 security layers

表示一种由安全维保护的网络设备和设施分类的层次结构。

注：安全层的详细描述见GB/T 25068.2。

3.2.41

安全面 security plane

表示由安全维保护的某种类型的网络活动。

注1：安全面的详细描述见GB/T 25068.2。

3.2.42

滥发 spamming

发送大量未经请求的消息，从而对接收方信息系统资源的可用性造成不利影响。

3.2.43

欺骗spoofing

假冒成合法的资源或用户。

3.2.44

交换机 switch

利用内部交换机制来提供联网设备之间连通性的设备。

注：交换机不同于其他局域网互联设备（例如集线器），其原因是交换机中使用的技术是在点对点的基础上建立连接。这就确保网络通信流只对有地址的网络设备可见，并使几个连接能够并存。交换技术能在OSI参考模型（GB/T 9387.1）的第2层或第3层实现。

3.2.45

隧道 tunnel

通过使用协议封装、标签交换或虚电路等技术，在现有的网络基础设施上建立的联网设备之间的数据路径。

3.2.46

虚拟专用网 virtual private network

利用物理网络的系统资源而构建的限制性使用的逻辑计算机网络。例如，使用加密技术和/或虚拟网络的隧道链接来跨越真实网络。

4 缩略语

下列缩略语用于GB/T 25068的各个部分。

3G	第三代移动电话系统 (Third Generation mobile telephone system)
AAA	鉴别、授权和计费 (Authentication, Authorization and Accounting)
ACL	访问控制列表 (Access Control List)
ADSL	非对称数字用户线 (Asymmetric Digital Subscriber Line)
AES	高级加密标准 (Advanced Encryption Standard)
ATM	异步传输模式 (Asynchronous Transfer Mode)
CDPD	蜂窝数字分组数据 (Cellular Digital Packet Data)
CDMA	码分多址 (Code Division Multiple Access)
CLID	呼叫线路识别 (Calling Line Identifier)
CLNP	无连接网络协议 (Connectionless Network Protocol)
CoS	服务类别 (Class of Service)
CRM	客户关系管理 (Customer Relationship Management)
DEL	直接交换线路 (Direct Exchange Line)
DES	数据加密标准 (Data Encryption Standard)
DMZ	非军事区 (Demilitarized Zone)
DNS	域名服务 (Domain Name Service)
DoS	拒绝服务 (Denial of Service)
DSL	数字用户线 (Digital Subscriber Line)
EDGE	增强型数据速率GSM演进技术 (Enhanced Data-Rates for GSM Evolution)
EDI	电子数据交换 (Electronic Data Interchange)
EGPRS	增强型通用分组无线业务 (Enhanced General Packet Radio Service)
EIS	企业信息系统 (Enterprise Information System)
FTP	文件传输协议 (File Transfer Protocol)
GPRS	通用分组无线业务 (General Packet Radio Service)
GSM	全球移动通信系统 (Global System for Mobile communications)
HIDS	基于主机入侵检测系统 (Host based Intrusion Detection System)
HTTP	超文本传输协议 (Hypertext Transfer Protocol)
IDS	入侵检测系统 (Intrusion Detection System)
IP	互联网协议 (Internet Protocol)
ISP	互联网服务提供商 (Internet Service Provider)
IT	信息技术 (Information Technology)
LAN	局域网 (Local Area Network)
MPLS	多协议标签交换 (Multi-Protocol Label Switching)
MRP	制造资源计划 (Manufacturing Resource Planning)
NAT	网络地址转换 (Network Address Translation)
NIDS	网络入侵检测系统 (Network Intrusion Detection System)

GB/T 25068.1—20XX/ ISO/IEC 18028-1

NTP	网络时间协议 (Network Time Protocol)
OOB	带外数据 (‘Out of Band’)
PC	个人计算机 (Personal Computer)
PDA	个人数字助理 (Personal Data Assistant)
PIN	个人识别码 (Personal Identification Number)
PKI	公钥基础设施 (Public Key Infrastructure)
PSTN	公用电话交换网 (Public Switched Telephone Network)
QoS	服务质量 (Quality of Service)
RAID	独立冗余磁盘阵列 (Redundant Array of Inexpensive Disks)
RAS	远程接入服务 (Remote Access Service)
RTP	实时传输协议 (Real-Time Transport Protocol)
SDSL	对称数字用户线 (Symmetric Digital Subscriber Line)
SecOPs	安全操作规程 (Security Operating Procedures)
SIM	用户识别模块 (Subscriber Identity Module)
SNMP	简单网络管理协议 (Simple Network Management Protocol)
SSH	安全外壳协议 (Secure Shell)
TCP	传输控制协议 (Transmission Control Protocol)
TDMA	时分多址 (Time Division Multiple Access)
Telnet	在远程计算机上在线工作的终端仿真程序 (Terminal emulation program to work on-line on a remote computer)
TETRA	地面集群无线电 (TErrestrial TRunked RAdio)
TKIP	临时密钥整体性协议 (Temporal Key Integrity Protocol)
UDP	用户数据报协议 (User Datagram Protocol)
UMTS	通用移动通信系统 (Universal Mobile Telecommunications System)
UPS	不间断电源 (Uninterruptible Power Supply)
USB	通用串行总线 (Universal Serial Bus)
VHF	甚高频 (Very High Frequency)
VoIP	IP语音 (Voice over IP)
VPN	虚拟专用网 (Virtual Private Network)
WAN	广域网 (Wide Area Network)
WAP	无线应用协议 (Wireless Application Protocol)
WEP	有线等效隐私 (Wired Equivalent Privacy)
WLAN	无线局域网 (Wireless Local Area Network)
WORM	一写多读 (Write Once Read Many)

5 结构

GB/T 25068.1中采用的编排方法是：

——首先总结识别和分析与通信相关因素的整个过程，这些因素在确立网络安全要求时宜予以考虑；

——然后针对与连接相关的安全提供潜在控制域的指示，这些连接是与外部通信网络的连接和通信网络之间的连接。在此过程中，对ISO/IEC 13335和GB/T 22081-2008可能使用的相关内容提供指示符，并且在GB/T 25068.2至GB/T 25068.5中详细研究的技术设计和实施的主题也被引入。

描述三个简单标准以帮助负责信息安全的人员识别潜在控制域。这些标准识别以下内容：

- 不同网络连接类型；
- 不同网络特征和相关信任关系；
- 与网络连接（和经由这些连接所提供服务的使用）有关的潜在安全风险类型。

然后将这些标准组合起来的结果用于指示潜在控制域。随后，提供潜在控制域的概要描述，并指出更详细的来源。

研究的领域是：

- 网络安全体系结构，包括以下范围：

局域网；

广域网；

无线网络；

无线电网络；

宽带网络；

安全网关（见GB/T 25068.3）；

远程接入服务（见GB/T 25068.4）；

虚拟专用网（见GB/T 25068.5）；

IP融合（数据、音频和视频）；

保持对（组织）外部网络所提供服务的访问成为可能；

万维网代管体系结构；

（更多网络安全体系结构的细节见GB/T 25068.2。）

- 安全服务管理框架；

- 网络安全管理；

- 技术脆弱性管理；

- 识别和鉴别；

- 网络审计日志和监视；

- 入侵检测；

- 抵御恶意代码；

- 公用基础设施的密码服务；

- 业务持续性管理¹⁾。

然后研究安全控制措施的实施和运行，以及该实施的监视和评审。

6 目标

本部分的目标是提供：

- 识别和分析与通信相关因素的指导，这些因素在确立网络安全要求时宜予以考虑；
- 潜在控制域的指示，包括在GB/T 25068.2至GB/T 25068.5中详细研究的那些潜在控制域。

7 综述

7.1 背景

1) 这包括 IT 灾难恢复计划。

随着电子商务行为在全球的不断增加，大多数政府和商业组织的信息系统通过网络连接在一起。网络连接可以是组织内部的互联、组织间的互联或组织与公众的互联。

公开可用网络技术特别是互联网和相关的万维网的迅速发展，使得商务和在线公共服务的提供得以发展。其范围，从仅将互联网用作全球化连接手段来提供成本较低的数据通信，到更复杂的ISP服务。这意味着从使用在电路每一端的成本相对低的本地连接点，直到使用基于万维网的应用和服务，全面的在线电子交易和服务交付系统。此外，新技术（包括数据和语音的集成），使得远程上下班风格的业务模型有更大的发展空间。这使得员工能够在大部分时间内远离总部办公，通过使用拨号接入或逐渐增多的无线局域网连接等远程设施以建立与企业网络联系和访问业务支持信息和服务，来保持与总部的联系。

因此，在这种环境带来商业利益的同时，它也带来新的需要管理的安全风险。由于组织严重依赖信息的使用来进行业务活动，信息和服务的保密性、完整性、可用性、抗抵赖、可核查性、真实性和可靠性的损失能够对业务运行造成不利影响。因此，保护信息、对组织内部信息系统进行安全管理是非常重要的需求。

一个典型的联网场景的实例如图1所示，该场景能够在今天的很多组织机构中观察到。

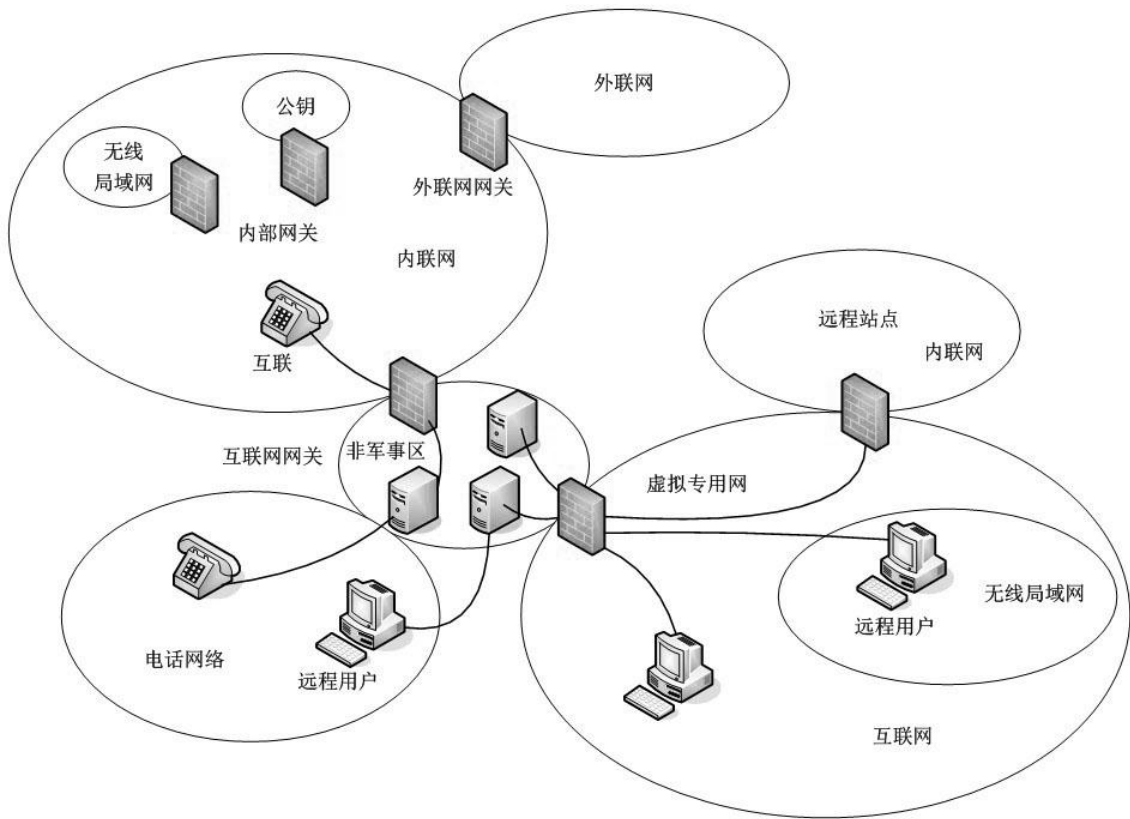


图1 典型联网环境

内联网规范组织内部依赖和维护的网络。通常情况下，只有组织的工作人员才有该网络的直接物理接入点，并且该网络在处于该组织拥有的前提下，某种级别的物理保护可以容易地实现。在大多数情况下，对于所使用的技术和安全要求而言，内联网不是同构的；可能有些基础设施需要的保护级别比内联网自身给出的要高。此类基础设施，例如公开密钥基础设施环境的基本部分，可在内联网的专用部分中运行。另一方面，某些技术可能需要某种隔离，因为它们引入额外风险，例如无线局域网基础设施。对于这两种情况，内部安全网关可用于实施这种分割。

如今大多数组织的业务需求都需要与外部伙伴和其他组织进行通信和数据交换。与最重要的业务伙伴的连接方式是直接将内联网扩展到伙伴组织的网络；外联网这个术语被普遍用于这种扩展。由于被连接伙伴组织的信任在大多数的情况下要低于组织内部的信任，所以外联网安全网关被用于应对由这些连接引入的风险。

如今公共网络，主要是互联网，被进一步用于为合作伙伴和客户（包括公众）提供成本最优化的通信和数据交换设施，并且提供各种形式的内联网扩展。由于公共网络特别是互联网中的低信任等级，需要高级的安全网关来帮助管理相关的风险。这些安全网关包括特定的组件来处理各种形式的内联网扩展以及合作伙伴和客户连接的要求。

远程用户可通过虚拟专用网技术来连接，他们可能进一步使用如公共无线局域网热点之类的无线连接设施来接入互联网。或者，远程用户可使用电话网络来建立与远程接入服务器直接拨号连接，远程接入服务器通常位于互联网防火墙的非军事区环境内。

当一个组织决定使用VoIP技术来实现内部电话网络之后，通常也需要在电话网络中合理的部署安全网关。

同时，在许多方面，用于该典型的联网方案中的技术带来了更多的商机和效益，例如通过降低和最优化成本，会导致环境十分复杂，且通常引入新的信息安全风险。因此，该环境下引入的风险需要被合理的评估，并且需要采取恰当的安全控制措施来降低风险。

换言之，这些新环境所提供的业务机会宜与较新技术产生的风险保持平衡。例如从安全的角度来看，互联网有若干能引起关注的技术特点。它最初的设计是具有弹性的，未优先考虑安全，并且普遍使用的很多底层协议本来就不是安全的。互联网的一个主要优点是它是一个非常开放的系统，最初是为响应美国政府的项目要求而在学术研究团体中开发的，能够广泛的公布结果以及免费分发软件和规范。这促进了互联网的普及和迅速发展，然而正是这种普及和开放产生了一个严重的脆弱性。在全球环境中有很多人有能力、知识和爱好来访问底层机制和协议并产生安全问题，其范围从未授权访问到全面的破坏性拒绝服务攻击。

总之，商业界和政府能否成功地利用现代网络所提供的机会，取决于在开放环境中运行的风险能否被管理和控制的程度。

7.2总结用于识别和分析与通信相关因素并指明潜在控制域的建议过程，这些与通信相关的因素宜在确立网络安全要求时予以考虑。然后由后面的章条提供这一过程的更多细节。

7.2 识别过程

当考虑网络连接时，组织中其责任与这种连接相关的所有人员宜清楚其业务要求和利益。此外，他们宜知晓这种网络连接的安全风险和相关的控制域。这些业务要求和利益可能会影响到在考虑网络连接、识别潜在控制域以及最终选择、设计、实施和维护安全控制措施的过程中所采取的很多决定和行动。因此，这些业务要求和利益宜在此过程中牢记。为了识别适当的、与网络相关的安全要求和控制域，宜完成以下几个任务（见GB/T 22081-2008）：

- 评审在组织的企业信息安全策略²⁾中阐明的网络连接一般安全需求（见第8章）；
- 评审与网络连接相关的网络体系结构和应用，为处理后续任务提供必要的背景（见第9章）；
- 识别宜考虑的网络连接类型（见第10章）；
- 评审网络提议的特征（网络和应用体系结构上的可用信息加以辅助），以及相关的信任关系（见第11章）；

2) 这将包括这一策略在以下方面的位置：（1）由相关法规或法律主体（包括国家政府机构）规定的、与网络连接相关的法律法规安全要求。（2）网络存储或传输的数据的类别。

——确定安全风险相关类型,可能辅以风险评估和管理评审结果—包括考虑对经由这种连接传输的信息以及可能以未授权方式通过这些连接进行访问的任何其他信息,进行业务操作的价值和所提供的服务³⁾(见第12章);

——识别控制域是否是适当的、符合网络连接类型、网络特征和相关信任关系、以及安全风险类型、确定的,同时文件化和评审技术安全体系结构选项并同意偏好选项⁴⁾(见第13章);

——实施和运行安全控制措施(见第14章);

——持续监视和评审安全控制措施的实施⁵⁾(见第15章)。

宜注意的是,识别控制措施的一般建议包含在GB/T 22081-2008中,包括在将出版的ISO/IEC 13335-2中。GB/T 25068.1是这些标准的补充,介绍如何识别与通信网络连接相关的安全适当控制域,GB/T 25068.2到GB/T 25068.5也如此。

图2说明识别和分析确立网络安全要求时考虑的与通信相关因素的整个进程,提供潜在控制域的指示。此过程的每一步都在图2后面的章条中加以详细描述。

在图2中,黑色实线表示该过程的主要路径,黑色虚线表示安全风险类型可能需要安全风险评估和管理评审的结果来帮助确定。

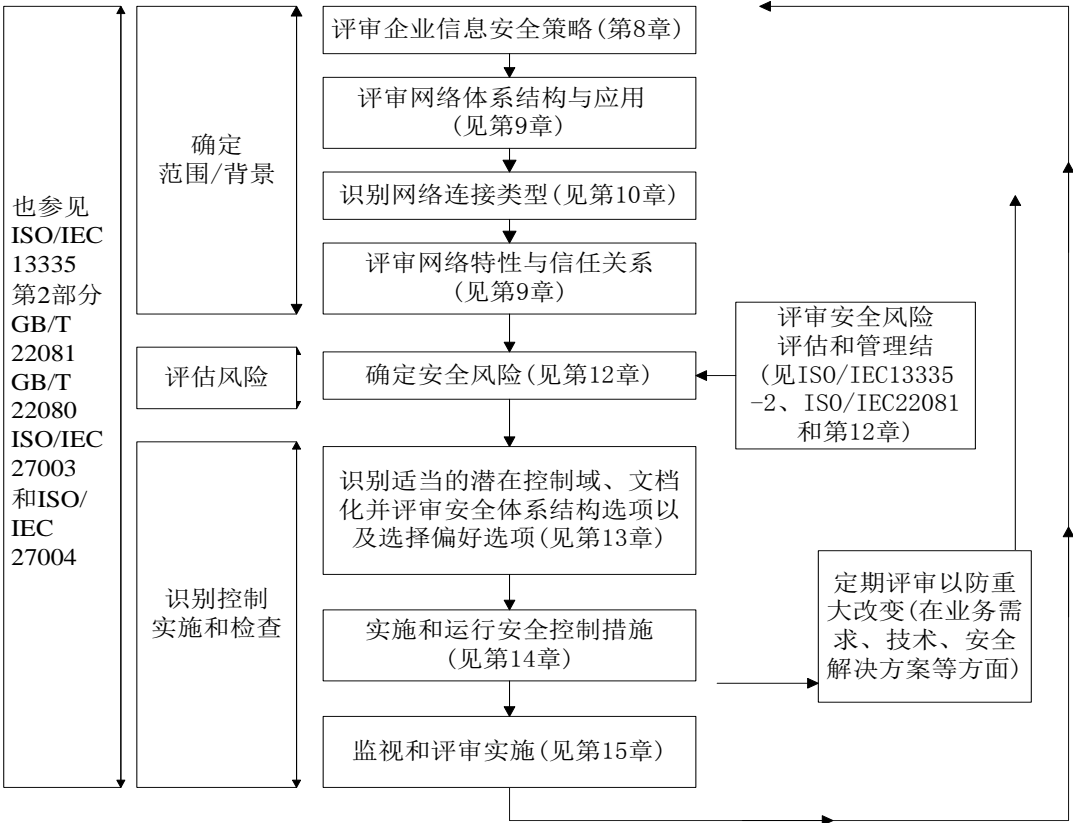


图2 安全环境中的管理进程

除了主要的过程路径外,在某些步骤中宜需要再次访问先前步骤的结果,以确保一致性,特别是“评审企业信息安全策略”和“评审网络体系结构与应用”这两个步骤。例如:

- 3) 这将包括(1)评估潜在违背由相关立法主体(包括国家政府机构)规定的,与网络连接相关的法律法规的风险。(2)使用约定的潜在不利服务影响,确认在网络上存储或传输的数据类别。
- 4) 这将包括要求遵守由相关立法主体(包括国家政府机构)规定的与网络连接机关的法律法规的控制措施。
- 5) 这将包括监视和评审要求遵守由相关立法主体(包括国家政府机构)规定的与网络连接机关的法律法规的控制措施。

——在确定了安全风险的类型之后，可能需要评审企业信息安全策略，因为实际上在该策略级别无法处理的某些事情已经发生；

——识别潜在控制域时，宜考虑企业信息安全策略，例如无论风险如何，企业信息安全策略都详细的说明了某个控制措施必须跨越组织加以实施；

——在评审安全体系结构选项时，确保网络体系结构与应用的兼容性得到考虑。

8 企业信息安全策略要求的考量

一个组织的企业信息安全策略可能包括对保密性、完整性、可用性、抗抵赖、可核查性、真实性和可靠性的要求的陈述，以及在威胁类型、控制要求方面的观点，这些均与网络连接直接相关。

例如，这一策略能够陈述：

——某些类型的信息或服务的可用性是主要的关注点；

——不许可任何经由拨号接入线路的连接；

——宜使得到互联网的所有连接均通过安全网关；

——宜使用特定类型的安全网关；

——若无数字签名则计费指令无效。

适用于组织或全社团的此类陈述、观点和要求，宜在确定安全风险类型（见第12章）和识别为网络连接潜在控制域（见第13章）时加以说明。如果有任何这样的安全要求，就宜在潜在控制域的草案列表中记载这些要求，并在必要时反映在安全体系结构选项中。企业信息安全策略文件在组织信息安全方法内的定位、其内容以及与其他安全文件关系的指南见ISO/IEC 13335-1和GB/T 22081-2008。其指南也见ISO/IEC 13335-2。

9 网络体系结构与应用的评审

9.1 背景

如前所述，完成网络所要求的潜在控制措施的确认的步骤是：

——识别要使用的网络连接类型；

——识别网络特征和所涉及到的相关信任关系；

——确定安全风险；

——开发所要求控制域的列表⁶⁾和相关设计。

接下来的这些步骤宜专用于已经存在或计划了的网络体系结构和应用的环境中。

因此，宜获得相关网络体系结构和应用的细节，且宜评审这些细节，从而为此进程的后续步骤提供必要的理解 and 环境。

通过在尽可能早的阶段澄清这些方面，识别相关安全要求辨识标准、识别控制域和评审技术安全体系结构选项以及决定宜采用哪一个方案的进程宜变得效率更高，最终得到较可行的安全解决方案。

在早期阶段对网络和应用体系结构方面加以考虑，如果可接受的安全解决方案实际上在当前的体系结构中不能够实现，就应有时间对这些结构进行评审和可能的修改。

宜考虑的不同域包括：

——网络类型；

——网络协议；

——网络应用；

6) 包括与密码使用有关的那些控制域，诸如保密性、完整性和鉴别。

——实现网络的技术。

评审这些域的一些问题在后面的9.2至9.6中讨论。第10章提供如何识别网络连接类型的指南，第11章提供如何确定网络特征和相关信任关系的指南，第12章提供识别安全风险的指南。（网络与应用体系结构的一般指南见GB/T 9387）

9.2 网络类型

依据其涉及的区域，网络能分类为：

- 局域网（LAN），用于在本地互连各个系统；
- 广域网（WAN），用于互连向世界范围的各个系统。

（一些资源也将术语城域网（MAN）定义为“限制本地使用的广域网”，如在一个城市内。但是，现在同样的技术被用于广域网，因此城域网和广域网之间没有任何显著的差异。此外，就本部分而言，个人局域网（PAN）将归类为局域网。）

9.3 网络协议

不同的协议有不同的安全特征，且宜给予特殊考虑。例如：

——共享介质协议主要用于局域网，且提供各种机制来调控连接到的各个系统之间共享介质的使用。当使用共享介质时，网络中的所有信息都可以通过全互联系统物理访问；

——路由协议用于信息在广域网中不同节点间传输时定义路由。路由经过的所有系统内的信息均可被物理访问，同时路由也可人为或自动更改；

——很多承载网络都基于的多协议标签交换协议，允许一个核心承载网络被多个专用网络共享，而一个专用网络中没有任何一个成员知晓还有其他专用网络共享该核心网络。其主要应用是VPN的实施，用不同的标签来识别和分割属于不同VPN的通信流（基于MPLS的VPN不基于数据加密机制）。这使得企业用户能够将内部网络外包给服务提供商，而不必部署和管理他们自己的核心IP网络。一个关键的好处是能够集中网络服务，诸如网络上的语音和数据，使用服务质量机制来确保实时性能。

网络中使用的很多协议不提供任何安全性。例如，从网络通信流中获取密码的工具常常被攻击者利用。这使得应用系统在公共网络上发送未加密的口令有高度的脆弱性。

很多协议可用于连接不同的网络拓扑和介质，且使用有线以及无线技术。在很多情况下，上述做法对安全特征有更多的影响。

9.4 网络应用

网络上所述应用的类型宜在安全的环境中考虑。这些类型能包括：

- 瘦客户端应用；
- 桌面应用；
- 基于终端仿真的应用；
- 消息基础设施与应用；
- 存储和转发或基于缓冲区的应用；
- 客户端服务器应用。

下面的例子展示应用特征如何影响它们可能使用的网络环境的安全需求：

——消息应用（如加密和消息的数字签名）可提供足够的安全等级，不必在网络上实施专用的安全控制措施；

——瘦客户端为获得特定的功能需要下载移动代码。然而在这种情况下，保密性可能不是主要的问题，完整性是重要的并且网络宜为此提供适当的机制。此外，如果必须满足较高的要求，移动代码的数

字签名将提供完整性和附加鉴别。这些经常应用框架本身之内完成，因此可能没有必要在网络中提供这些服务；

——基于存储和转发或缓冲区的应用通常为进一步处理而将重要数据临时存储。如果有完整性和保密性的要求，在网络中需要有适当的控制措施以保护传输中的数据。但是，由于数据暂时存储在中间主机，这些控制措施可能还不够。因此，可能也需要应用附加控制措施和保护在中间节点上存储的数据。

9.5 网络实现技术

网络可使用各种手段来实现，采用这些手段的常见结构以网络所覆盖的地理区域为基础。

9.5.1 局域网

局域网是在一个小的地理区域内把计算机和服务器互联在一起的网络。其规模范围从几个相互连接的系统（形成一个家庭网络）到几千个相互连接的系统（如在校网络中）。实现的典型服务包括共享打印机等资源，共享文件和应用。局域网通常也提供中央服务，如消息或日历服务。在某些情况下，局域网也用来替代其他网络的传统功能，如提供VoIP协议和服务来替代基于PBX的电话网络。小型局域网通常采用共享介质技术来实施。以太网协议是此环境中使用的标准技术，并且已经被扩展来提供较高的带宽和支持无线环境。由于共享媒体技术，特别是以太网对较大规模网络有限制，典型的广域网技术如路由协议也常用在局域网环境中。局域网是基于有线或基于无线的。

9.5.1.1 有线局域网

有线局域网一般由网络中使用联网电缆经由网络交换机或集线器连接起来的节点组成，它能提供高速数据联网能力。众所周知的有线局域网技术包括以太网(GB/T 15629.3)和令牌环网(GB/T 15629.5)。

9.5.1.2 无线局域网

无线局域网利用高频无线电波在空中发送网络包。其灵活性在于不需要进行网络布线便可迅速建立局域网。众所周知的无线局域网技术包括GB 15629.11-2003实现技术和蓝牙技术。

9.5.2 广域网

广域网用于将远端与其局域网连接在一起。广域网的构建能使用服务提供商的电缆、电路，更可能的是租赁电信运营商的服务。广域网技术允许通信流进行远距离传输和路由选择，并且通常提供扩展的路由特性，选择路由将网络包发送到正确的目的地局域网。通常情况下，公共物理网络基础设施用于局域网互连，例如：租用线路、卫星通信或者光纤。广域网可能是基于有线的或是基于无线的。

9.5.2.1 有线广域网

有线广域网一般由通过电信线路连接到公共或专用网络的路由设备（例如路由器）组成。众所周知的有线广域网技术包括ATM、帧中继和X.25协议。

9.5.2.2 无线广域网

无线广域网通常使用无线电波在空中远距离发送网络包，其距离能达到10km或以上。众所周知的无线广域网技术包括TDMA、CDMA、GSM和IEEE 802.16。

9.6 其他考量

在评审网络体系结构和应用时，也宜考虑现有的网络连接，包括该组织内部的、连接到组织的或组织发出的连接，以及到提出连接建议网络的连接。组织现有的连接可能会限制或阻止新的连接，例如，

受到协议或者合同的限制。在要求一个到达某网络连接之处，若存在到达该网络或从该网络发出的其他连接，就可能引入额外的脆弱性因而导致较高的风险，因此可能需要较强的和/或附加的控制措施。

10 网络连接类型的识别

组织或团体可能需要使用很多通用类型的网络连接。其中一些类型的连接能通过专用网（限制已知团体接入此网）实现，一些连接可通过公共网络（对任何组织或个人而言对其接入都是潜在可用的）实现。此外，这些类型的网络连接可用于各种服务，例如电子邮件或者电子数据交换，并且可涉及互联网、内联网或外联网设施的使用，每种连接都有不同的安全考量。每种类型的连接可能有不同的脆弱性，因而具有相关联的安全风险，其结果是最终需要不同的一组控制措施。（见GB/T 22081）

通用网络连接类型的一种分类方法如后面的表1所示，可用其来管理业务，每类都有描述性实例。

适当考虑相关的网络体系结构和应用（见第9章）。表1中所示的一种或一种以上的类型宜以适应于正在考虑的网络连接的方式被选择。

宜注意的是：本部分中描述的通用网络连接类型，是从业务角度而不是从技术角度进行组织和分类的。这意味着两种不同类型的网络连接，有时可能使用类似的技术手段来实施，并且在某些情况下控制措施可能是类似的，但在其他情况下它们是不同的。

表1 网络连接类型

参考	网络连接类型	描述性例子
A	组织中一个单独的、受控位置之内的连接。	在同一受控位置（如一个受控建筑或站点）之内，同一组织的不同部分之间的互联。
B	同一组织中不同地域相异部分的连接。	组织内部的区域办公室之间（和/或总部站点内的区域办公室）跨越广域网的互连。在这种类型的网络连接中，大多数用户-如果不是全部的话-都能够通过网络访问可用信息系统，但不是组织内的所有用户都得到授权，访问所有应用或信息（即用户的访问只与被赋予的权限相一致）。从组织的其他部分访问的一种类型用于实现远程维护的目的。这种类型的用户和连接有可能得到更多访问权限。
C	在远离组织位置工作的人员之间的连接。	员工使用移动数据终端（如销售人员从客户站点验证存货可用性）或者其他远程站点工作的员工未通过由组织维护的网络而建立到组织的计算系统的远程连接点工作。在这种类型网络连接中，用户具有本地系统用户的权限。
D	一个封闭团体内不同组织之间的连接，例如由于契约或其他具有法律约束的情形，或者具有相似业务利益，如银行或保险。	有业务需要的两个或多个组织的互连，以使跨组织的电子交易（例如银行界的电子资金转帐）便捷。这种类型网络连接与上面的‘B’类型类似，不同点在于互连的站点属于两个或两个以上的组织，并且该连接并未打算对每一个参与组织所使用的全部应用都提供访问。
E	与其他组织的连接。	可访问其他组织所有的远程数据库（如通过服务提供商）。在这种类型的网络连接中，所有用户，包括正连接组织的用户，都由正访问信息所属的外部组织，单独预先授权。然而，尽管所有用户都已预先授权，但有可能未屏蔽除了其支付所提供服务的潜力外的潜在用户。同时，也能够访问存储或处理组织信息的组织系统，这些组织信息可提供给组织外部用户。在此情形下，外部用户将是可知并得到授权的。一种其他组织的访问可用于实现远程维护的目的。这种类型的用户和连接可能得到更高的访问权限。
F	与普通公共域的连接。	访问能由组织的用户向公共访问数据库、Web 站点、和/或电子邮件设施（如通过互联网）发起，发起访问的目的包括检索信息、或从/向未被组织专门预先授权的人员和/或站点发送信息。在这种类型连接中，该组织的用户可为了组织（甚至可能是私人）目的来使用这一设施。然而这样的组织几乎没有-如果有的话-对所传输信息的控制。访问可由外部用户向组织的设施发起（如通过互联网）。在这种类型的网络连接中，单独外部用户的访问未获得组织的专门预先授权。
G	IP 环境至公共电话网的连接。	访问可由 IP 网络中的电话向 PSTN 发起。这种连接是不受控的，因为呼叫可在世界上的任何位置接受。接受。

11 网络特征与相关信任关系的评审

11.1 网络特征

宜评审现有或建议的网络的特征。这对于识别网络是以下哪一种尤为重要：

- 公用网-任何人均可访问的网络；
 - 专用网-如由自己拥有或租用线路构成的网络，因此认为它比公共网更安全。
- 了解网络所传输数据的类型也很重要，例如：
- 数据网络-主要传输数据和使用数据协议的网路；
 - 语音网络-针对电话但也能用于数据的网路；
 - 包括数据和语音甚至视频的网络。

其他信息也是相关的，诸如：

- 该网络是否是一个分组网络或交换网络；
- 它是否支持QoS，如在MPLS网络中。

（QoS关注一致的性能。网络服务宜被交付以提供可用的最低性能级别。例如，如果带宽不足，那么语音服务将断断续续和中止。QoS是指网络系统将某种服务维持在它所需要的最低性能级别或以上的能力）。

此外，也宜确立连接是永久的或是在需要之时才建立。

11.2 信任关系

一旦识别出现有的或提议的网络特征，且至少已确定该网络是公共的或专用的（见11.1），然后宜识别相关的信任关系。

首先，与网络连接相关的可应用的信任环境，宜使用以下简表加以识别：

- 低信任环境级别，诸如具有未知团体用户的网络；
- 中信任环境级别，诸如具有已知团体用户且在封闭业务团体（不止一个组织）的网络；
- 高信任环境级别，诸如只有组织内已知团体用户的网络。.....

其次，为了建立信任关系，相关信任环境（从低级、中级到高级）宜与可应用的网络特征（公共或专用）和所涉及的网络连接类型（从‘A’到‘G’）相关。这能够按类似表2所示来实现。

表2 信任关系的识别

网络连接类型 (见第 10 章)		信任环境		
		低级别	中级别	高级别
网络特征	公共	F G	D E	B C
	专用	E	D E	A B C

表2中宜确定每个相关信任关系的参考类别。所有可能的类别在后面的表3中描述。

表3 信任关系参考

信任关系类别	描述
低级别 / 公共	低级别信任，使用公共网络。
中级别 / 公共	中级别信任，使用公共网络。
高级别 / 公共	高级别信任，使用公共网络。
低级别 / 专用	低级别信任，使用专用网络。
中级别 / 专用	中级别信任，使用专用网络。
高级别 / 专用	高级别信任，使用专用网络。

当利用第12章来确定安全风险类型和识别潜在控制域时，宜使用这些参考。

这项任务必需时能通过网络体系结构和应用上的可用信息加以辅助（相关内容通过使用第9章获得）。

12 信息安全风险的识别

正如前面所反映的，现今多数组织依赖于使用信息系统和网络来支持其业务运营。此外，在许多情况下，对于在每个组织位置的信息系统与组织内外其他站点（包括与普通公用网）之间的网络连接的使用，均有明确的业务要求。当建立与另一个网络的连接时，宜相当小心以确保组织未受到（来自利用脆弱性的潜在威胁）额外风险。这些风险可能来自连接本身或来自网络连接的另一端。

其中一些风险可能与确保遵守相关法律法规相关。（对于隐私和数据保护的立法宜予以特别关注。对于收集、处理和传输个人数据，即与特定个人或人群相关的数据，若干国家具有对其加以控制的法律。根据各个国家的法律，此类控制措施可能强制通过网络收集、处理和传播个人信息，甚至可能

的人员限制其将数据传输到其他某些国家的能力，造成了额外重要的安全关注。可能受到此类法律控制的不那么明显的数据实例是一些硬件和IP地址。）

本章考虑的风险类型涉及对未授权访问信息、未经授权发送信息、引入恶意代码、拒绝接收或原发、拒绝服务连接，以及信息和服务不可用的关注。因此，组织可能面对的安全风险类型与以下几方面的损失相关：

- （在网络和在与网络相连的系统中）信息和代码的保密性；
- （在网络和在与网络相连的系统中）信息和代码的完整性；
- 信息和网络服务（以及与网络相连的系统）的可用性；
- 网络交易（委托）的抗抵赖；
- 网络交易的可核查性；
- 信息（这些也包括网络用户和管理员）的真实性；
- （在网络和在与网络相连的系统中）信息和代码的可靠性；
- 控制未授权使用和利用网络资源的能力，包括在组织策略（如为了个人利益而出售带宽或使用带宽）和有关法律法规的责任（如存储儿童色情描写）的内容中。

并非所有的安全风险类型都适用于每个位置或每个组织。然而，为了能够识别潜在控制域（和最终的选择、设计、实施和维护控制措施），宜识别相关的安全风险类型。

网络安全的概念模型如图3所示，它表明安全风险类型可能发生在何处。

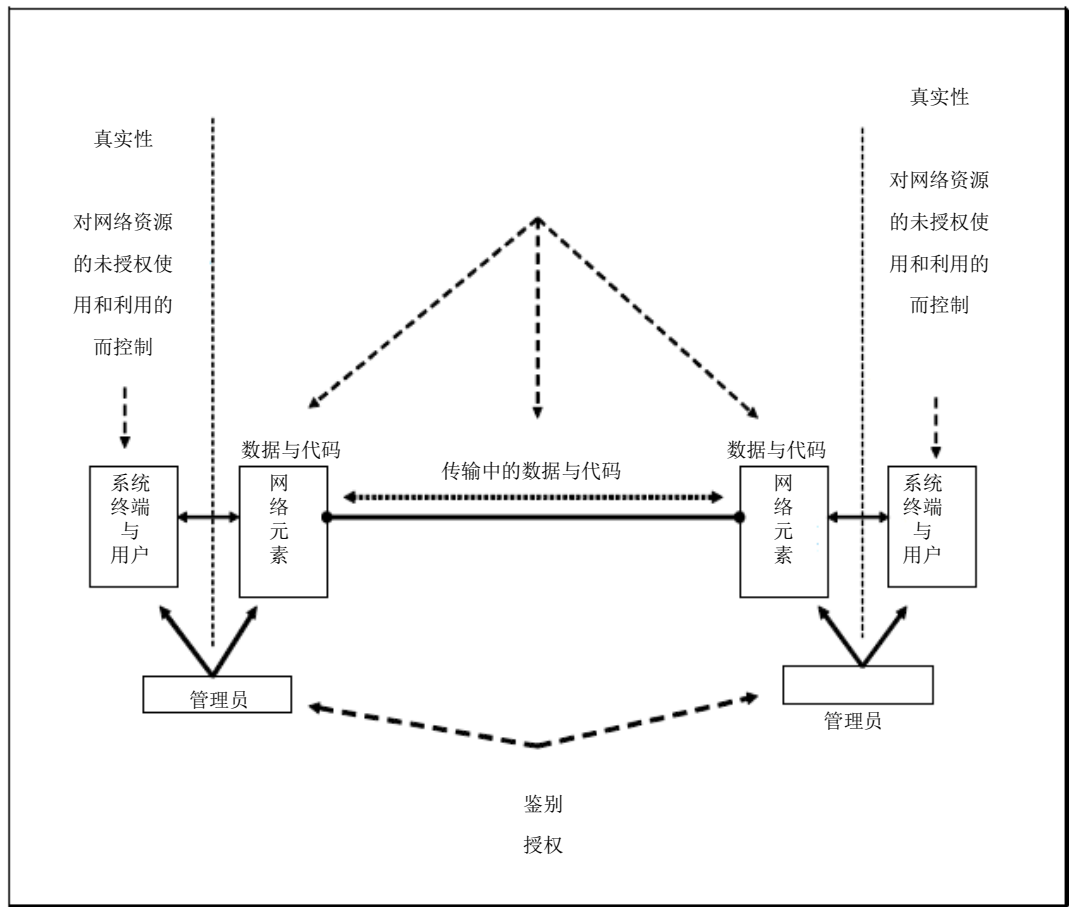


图3 网络安全风险域的概念模型

宜收集上面提到的对于涉及安全风险类型的业务运营有意义的信息，同时预先考虑信息涉及的敏感性或价值（表示为对业务的潜在不利影响）和相关潜在威胁和脆弱性。与此相关的是，如果对组织的业务运营可能有不止微小的负面影响，那么就宜参考后面表5中的矩阵。

应强调的是，在完成此任务时，宜使用针对网络连接进行的安全风险评估和管理评审⁷⁾的结果。这些结果将导致把重点放在：这种评审已经进行到何种详细程度；与上面列出的安全风险类型相关的、对业务的潜在不利影响以及威胁类型、脆弱性和关注的风险。

在安全风险评估和管理评审期间，应当考虑网络脆弱性时，可能需要分别考虑若干网络层面。后面的表4列出能在每个网络层面利用的脆弱性类型。

表4 潜在脆弱性类型

网络层面	潜在网络安全的弱性类型				
	中断	拦截	修改	入侵	诱骗
网络用户	用户可能承受损失或服务中断。	用户交易和/或网络活动可能被修改或破坏。	用户细节和用户数据可能被修改或破坏。	用户可能被冒充以获得对设施的未授权访问。	用户可能被冒充以进行欺诈性交易。

7) 安全网络评估和管理方法的指南在 GB/T 22081 中给出，并包含在将发布的 ISO/IEC 13335-2 中。

网络终端系统	终端系统可能暂时或永久不可用。	未授权人员可能读出终端系统上的数据或代码。	数据或代码可能被修改或破坏。	终端系统可能被冒充以获得对设施的未授权访问人员可能获得对系统帐户的访问并利用它们发起进一步攻击。	终端系统可能被冒充以进行欺诈性交易或发起进一步攻击。
网络应用	应用可能暂时或永久不可用。	在传输过程中被未授权人员拦截, 或从服务器上读出数据或代码可能。	数据或代码可能被修改或破坏。	未授权人员可能获得对系统帐户访问并利用它们发起进一步攻击。	未授权人员可能获得对系统帐户访问并利用它们发起进一步攻击。
网络服务	服务可能暂时或永久不可用。	在传输过程中被未授权人员拦截, 或从服务器上读出数据或代码可能。	数据或代码可能被修改或破坏。	未授权人员可能获得对系统帐户访问并利用它们发起进一步攻击。	网络服务器和设备可能被冒充以获得未授权访问, 拦截网络通信流, 或破坏网络服务。
网络基础设施	设施可能暂时或永久不可用。			未授权人员可能渗透到设备。	

把安全风险评估和管理评审结果作为主⁸指南, 相关信任关系参考宜使用第11章来确定, 并沿着表5中矩阵的顶部来识别, 该矩阵左侧为所关注的影响。然后在有关交叉点的参考宜得到关注, 它们是对潜在控制域的参考, 将在第13章中介绍。

表5 安全风险的类型与潜在控制域的参考

风险类型	信任关系参考					
	低级别 / 公共	中等级 / 公共	高级别 / 公共	低级别 / 专用	中等级 / 专用	高级别 / 专用
保密性损失	13.2.1 ⁸)	13.2.1	13.2.1	13.2.1	13.2.1	13.2.1
		13.2.7	13.2.7	13.2.7	13.2.7	13.2.8
	13.2.7	13.2.8	13.2.8	13.2.8	13.2.8	13.2.9
	13.2.8	13.2.9	13.2.9	13.2.9	13.2.9	13.3.2
	13.2.9	13.3.2	13.3.2	13.3.2	13.3.2	13.3.3
	13.3.2	13.3.3	13.3.3	13.3.3	13.3.3	13.3.4
	13.3.3	13.3.4	13.3.4	13.3.4	13.3.4	13.3.6
	13.3.4	13.3.5	13.3.6	13.3.5	13.3.5	13.3.7
	13.3.5	13.3.6	13.3.7	13.3.6	13.3.6	13.4
	13.3.6	13.3.7	13.4	13.3.7	13.3.7	13.5
	13.3.7	13.4	13.5	13.4	13.4	13.6.2

8) 注意此表中对 13.2.1 的所有参考, 该章条将以对所关注的网络场景适当的方式应用。

风险类型	信任关系参考					
	低级别 / 公共	中等级别 / 公共	高级别 / 公共	低级别 / 专用	中等级别 / 专用	高级别 / 专用
	13.4	13.5	13.6.2	13.5	13.5	13.6.3
	13.5	13.6.2	13.6.3	13.6.2	13.6.2	13.6.4
	13.6.2	13.6.3	13.6.4	13.6.3	13.6.3	13.6.5
	13.6.3	13.6.4	13.6.5	13.6.4	13.6.4	13.7
	13.6.4	13.7	13.7	13.7	13.7	13.8
	13.7	13.8	13.8	13.8	13.8	13.9
	13.8	13.9	13.9	13.9	13.9	13.10.2
	13.9	13.10.2	13.10.2	13.10.2	13.10.2	13.10.5
	13.10.2	13.10.5	13.10.5		13.10.5	
	13.10.5					
完整性损失	13.2.1	13.2.1	13.2.1	13.2.1	13.2.1	13.2.1
	13.2.7	13.2.7	13.2.7	13.2.7	13.2.7	13.2.8
	13.2.8	13.2.8	13.2.8	13.2.8	13.2.8	13.2.9
	13.2.9	13.2.9	13.2.9	13.2.9	13.2.9	13.3.2
	13.3.2	13.3.2	13.3.2	13.3.2	13.3.2	13.3.3
	13.3.3	13.3.3	13.3.3	13.3.3	13.3.3	13.3.4
	13.3.4	13.3.4	13.3.4	13.3.4	13.3.4	13.3.6
	13.3.5	13.3.5	13.3.6	13.3.5	13.3.5	13.3.7
	13.3.6	13.3.6	13.3.7	13.3.6	13.3.6	13.4
	13.3.7	13.3.7	13.4	13.3.7	13.3.7	13.5
	13.4	13.4	13.5	13.4	13.4	13.6.2
	13.5	13.5	13.6.2	13.5	13.5	13.6.3
	13.6.2	13.6.2	13.6.3	13.6.2	13.6.2	13.6.4
	13.6.3	13.6.3	13.6.4	13.6.3	13.6.3	13.6.5
	13.6.4	13.6.4	13.6.5	13.6.4	13.6.4	13.7
	13.7	13.7	13.7	13.7	13.7	13.8
	13.8	13.8	13.8	13.8	13.8	13.9
	13.9	13.9	13.9	13.9	13.9	13.10.3
	13.10.3	13.10.3	13.10.3	13.10.3	13.10.3	13.10.5
	13.10.5	13.10.5	13.10.5	13.10.5		
可用性损失	13.2.1	13.2.1	13.2.1	13.2.1	13.2.1	13.2.1
	13.2.7	13.2.7	13.2.7	13.2.7	13.2.7	13.2.8
	13.2.8	13.2.8	13.2.8	13.2.8	13.2.8	13.2.9
	13.2.9	13.2.9	13.2.9	13.2.9	13.2.9	13.3.2
	13.3.2	13.3.2	13.3.2	13.3.2	13.3.2	13.3.3
	13.3.3	13.3.3	13.3.3	13.3.3	13.3.3	13.3.4
	13.3.4	13.3.4	13.3.4	13.3.4	13.3.4	13.3.6
	13.3.5	13.3.5	13.3.6	13.3.5	13.3.5	13.3.7
	13.3.6	13.3.6	13.3.7	13.3.6	13.3.6	13.4

风险类型	信任关系参考					
	低级别 / 公共	中等级别 / 公共	高级别 / 公共	低级别 / 专用	中等级别 / 专用	高级别 / 专用
	13.3.7	13.3.7	13.4	13.3.7	13.3.7	13.5
	13.4	13.4	13.5	13.4	13.4	13.6.2
	13.5	13.5	13.6.2	13.5	13.5	13.6.3
	13.6.2	13.6.2	13.6.3	13.6.2	13.6.2	13.6.4
	13.6.3	13.6.3	13.6.4	13.6.3	13.6.3	13.6.5
	13.6.4	13.6.4	13.6.5	13.6.4	13.6.4	13.7
	13.7	13.7	13.7	13.7	13.7	13.8
	13.8	13.8	13.8	13.8	13.8	13.9
	13.9	13.9	13.9	13.9	13.9	13.11
	13.11	13.11	13.11	13.11	13.11	
抗抵赖损失	13.2.1	13.2.1	13.2.1	13.2.1	13.2.1	13.2.1
	13.2.7	13.2.7	13.2.7	13.2.7	13.2.7	13.2.8
	13.2.8	13.2.8	13.2.8	13.2.8	13.2.8	13.3.2
	13.3.2	13.3.2	13.3.2	13.3.2	13.3.2	13.3.3
	13.3.3	13.3.3	13.3.3	13.3.3	13.3.3	13.3.4
	13.3.4	13.3.4	13.3.4	13.3.4	13.3.4	13.3.6
	13.3.5	13.3.5	13.3.6	13.3.5	13.3.5	13.3.7
	13.3.6	13.3.6	13.3.7	13.3.6	13.3.6	13.4
	13.3.7	13.3.7	13.4	13.3.7	13.3.7	13.5
	13.4	13.4	13.5	13.4	13.4	13.6.2
	13.5	13.5	13.6.2	13.5	13.5	13.6.3
	13.6.2	13.6.2	13.6.3	13.6.2	13.6.2	13.6.4
	13.6.3	13.6.3	13.6.4	13.6.3	13.6.3	13.6.5
	13.6.4	13.6.4	13.6.5	13.6.4	13.6.4	13.7
	13.7	13.7	13.7	13.7	13.7	13.8
	13.8	13.8	13.8	13.8	13.8	13.9
	13.9	13.9	13.9	13.9	13.9	13.10.4
	13.10.4	13.10.4	13.10.4	13.10.4	13.10.4	13.10.5
	13.10.5	13.10.5	13.10.5	13.10.5	13.10.5	13.11
	13.11	13.11	13.11	13.11	13.11	

宜注意的是，该表似乎指明用户得到的信任越多，必要的控制措施就越多。其原因有两个：

首先，有若干控制措施在GB/T 22081（在已发布的ISO/IEC 13335-2中描述）中描述，因此在本部分不重复，这些控制措施将被选择来保护主机设施，包括识别、鉴别和逻辑访问控制。在低信任情形中，识别、鉴别逻辑访问控制的强度控制宜高于高信任情形。如果这一要求不能得到保证，就宜实施附加控制措施。在低信任情形中，许可（权限）的配置宜有助于确保：仅对信任模型和访问要求一致的资源提供访问。

其次，获得信任的用户通常可访问更重要/关键的信息和/或功能。这能够意味着，对附加控制措施的要求，反映被访问资源的价值而不是用户的信任。

13 识别适当的潜在控制域

13.1 背景

在风险评估和管理评审结果的基础上，并辅以在第12章中所标识的文献，然后宜从第13章（当然包括GB/T 22081）中识别和选择潜在控制域。在已发布的ISO/IEC 13335-2中提供相关信息。13.2涉及各种网络安全体系结构方面和相关潜在控制域，随后是13.3至13.11，介绍其他相关潜在控制域。13.2至13.11介绍一个特定安全解决方案实际上可能包含若干潜在控制。

值得强调的是，无论信息系统是否有网络连接，都有若干与之相关的控制措施，这些控制措施宜通过GB/T 22081的使用来选择。在已发布的ISO/IEC 13335-2中提供相关信息。

已识别的潜在控制措施列表宜在相关网络体系结构和应用的情况中得到全面评审。然后该表宜得到必要调整，随后被用作实施所要求安全控制措施的基础（见第14章），然后监视和评审该实施（见第15章）。

13.2 网络安全体系结构

13.2.1 引言

可能的安全体系结构选项的文档化提供不同解决方案的检验手段和折衷分析的基础。这也有利于将经常出现的与技术限制及业务需求与安全需求之间的争端相关的问题的解决。

在选项文件化时，宜预先考虑企业的所有信息安全策略要求（见第8章）、相关网络体系结构和网络应用（见第9章）以及使用第12和13章识别的潜在控制域列表。在完成这些工作时，宜考虑现存的所有安全体系结构。一旦选项已被文件化并经过评审，作为技术体系结构设计过程的一部分，首选的安全体系结构宜得到承认并记录在《技术安全体系结构设计控制规范》文件中（该文件与“技术体系结构设计”兼容，反之亦然）。然后，可能会改变网络和应用体系结构（以确保与首选安全体系结构的兼容性）和/或潜在控制措施列表（例如，因为各方一致认为安全体系结构只能以某种特定方式在技术上实施，所以需要已识别控制措施的备选方案）。

宜注意的是，GB/T 25068.2描述一个“参考”⁹⁾安全体系结构，它作为一个基点，对以下情况非常有用：

- 描述一致的框架来支持规划、设计和实施网络安全；
- 定义通用的、与安全相关的体系结构元素，适当应用这些元素，能提供端到端网络安全。

本部分基于“参考”安全体系结构，满足当今和不久的将来要求所需的，实际上不同的现实世界技术安全体系结构的描述在本标准中被引入，并在GB/T 25068.3至GB/T 25068.5中对其进一步开发。

在“参考”安全体系结构的中描述的原则，适用于任何现代网络类型，无论是数据、语音和混合网络，还是无线或无线电网络，均能独立于网络技术或协议栈中的位置而应用。它涉及到的安全关注相关于网络基础设施的管理、控制和使用。以及服务和应用，并提供一个全面的、自上向下的、端到端方面的网络安全。“参考”安全体系结构有3个组件：

- 安全维（也可称作“安全控制组”）；
- 安全层（也可称作“网络安全元素”）；
- 安全面（也可称作“安全领域”）。

安全维是处理某一方面网络安全问题的一组安全控制措施。在“参考”安全结构中标识8个这种组，且这些组扩展到应用和终端用户信息，例如：

- 抗抵赖；

9) 在第2部分上下文中所使用的“参考”一词，是指如何在非常高的级别表示技术安全体系结构的一个例子。可能还有其他例子。

- 数据保密性；
- 数据完整性；
- 可用性。

为了提供端到端的安全解决方案，安全维需要应用网络设备层次结构和设施分组，它们称为安全层：

- 基础设施安全层；
- 服务安全层；
- 应用安全层。

安全层构建在彼此之上，以提供基于网络的解决方案，即基础设施层使能服务安全层、服务安全层是应用安全层的使能器，并通过提供连续的网络安全方面来识别宜在产品和解决方案中的何处处理安全问题。

基础设施安全层包括网络传输设施以及受到为安全维而实施的机制保护的个网络部分。属于基础设施安全层的组件实例包括单个路由器、交换机和服务器以及在单个路由器、交换机和服务器之间的通信链接。

服务安全层处理服务供应商提供给客户服务的安全。这些服务的范围从基本的传输和连通性，到服务使能器，如提供互联网访问（例如鉴别、授权和可核查性服务、动态主机配置服务和域名服务等）所必需的那些使能器，以及诸如免费电话服务、QoS、虚拟专用网等增值服务。

应用安全层关注被服务提供商客户访问的基于网络应用的安全。网络服务使这些应用能够工作，且包括基本文件传输（例如FTP）和Web浏览应用、基本应用（如目录帮助、基于网络的语音消息和电子邮件）以及高端应用（如客户关系管理，电子/移动商务，基于网络的培训、视频协作等）。

安全面是被安全维实施的机制保护的某种网络活动类型。“参考”安全体系结构定义3个安全面来表示发生在网络上的受保护活动类型。安全面包括：

- 管理面；
- 控制面；
- 终端用户面。

这些安全面解决与网络管理活动、网络控制和信令活动以及终端用户活动各自相关的特定安全需求。网络宜按以下方式设计：一个安全面上的事态尽可能与其他安全面适当分隔。

以下章条介绍各种网络领域中实际上不同的现实世界技术安全体系结构。

这里强调的是，任何项目的技术安全体系结构，宜全部文件化并得到赞同，直至最终确定实施的控制措施列表。

13.2.2 局域网

13.2.2.1 背景

在受物理保护区域内，例如仅在组织自己的建筑物内使用局域网时，可能存在的风险只要求有基本技术控制措施。然而，在较大环境中使用局域网时，也包括使用无线技术时（见13.2.4），仅有物理保护不太可能保证任何安全等级。此外，在局域网内最常使用的介质共享技术确实允许从任何使用共享介质的系统来访问所有的网络通信流。

由于桌面是一个用户界面，所以它是一个易受攻击的区域。如果桌面没有锁定，那么用户就有可能在局域网上安装未授权软件。企业网络之内使用的服务器系统，无论是暴露给互联网还是暴露给与互联网无直接连接的内部服务器，这表示一个潜在的主要安全风险。虽然多数IT部门声称，他们在补丁可用时会尽快应用补丁，但是这一风险必须严肃对待。因为即使是一些大型组织也未能按时为所有服务器打上补丁，因而导致内部网络通信流被蠕虫破坏。

13.2.2.2 安全风险

在有线局域网中，安全风险将在物理连接到网络的节点上出现。总体而言，与局域网相关的关键安全风险包括：

- 未经授权访问和改变个人桌面计算机、服务器和其他与局域网连接的设备；
- 未打补丁的服务器；
- 弱口令；
- 硬件窃取；
- 电源供应故障；
- 通过电子邮件和网络访问导入的恶意代码；
- 未备份本地硬盘；
- 硬件故障，如硬盘；
- 到局域网（膝上型计算机）的未经授权连接；
- 未经授权访问集线器和补丁贮存柜；
- 集线器和交换机的管理端口的默认口令；
- 低物理安全。

13.2.2.3 控制措施

保持局域网空间安全要求局域网组件和连接设备均得到保护。因此，保护局域网环境的控制措施能够包括：

——物理和环境方面：

使用钢缆系统以防止中央处理器、显示器和键盘被窃；

使用装置上的挂锁，来防止内部等部件被偷；

使用临近装置，来防止在站点进行未经授权的移动；

确保局域网集线器和路由器都保存在安全通信房间中物理安全的机柜内；

为关键设备提供具有自动关机功能的UPS，如果用户不想丢失正在进行中的工作，也给用户的个人计算机提供UPS；

——硬件和软件方面：

用专用IP地址来配置装置；

强口令策略；

要求在每个工作站登录，至少用一个用户ID/口令对；

安装抗病毒软件，并定期自动更新；

实施安全注册表设置；

禁用软盘驱动器、CD-ROM驱动器和USB端口；

为实现冗余而使用镜像服务器驱动器（或实施RAID）；

卸载不必要的软件；

——运营方面：

记录软件和安全设置，以备将来配置新工作站时使用；

预定计划定期下载和安装操作系统补丁；

创建和维护当前的紧急修复磁盘，并保存在受控位置；

实施日志功能以记录维护问题和滥用工作站问题；

将所有工作站组件文件（文件/手册/磁盘）归档，以备服务技术人员使用；

确保备份制度；

确保所有集线器和交换机的默认口令被更改；

设置适当的网络管理协议口令/团体字符串；

如果审计日志可用，适当加以配置，并实施监视审计日志的过程；
 安排固件更新的定期安装；
 记载设备设置以备将来配置设备时使用；制作路由器配置文件的备份副本，并保存在安全的位置；
 测试与局域网连接的所有设备的脆弱性。

13.2.3 广域网

13.2.3.1 背景

常规的广域网原本是使用从服务商租用的在固定位置之间的连接来创建的，而服务提供商除了确保这些连接可操作之外，只具有与此类连接相关的最少管理活动。然而，广域网技术进步导致管理责任转交给服务提供商身上，其好处是组织不必部署和管理自己的网络。这意味着责任在服务提供商身上以确保其网络管理设施是安全的。此外，由于广域网主要用于为长距离的网络通信流选择路由，所以路由选择功能宜得到很好保护确保可靠性的功能，亦即网络通信流不会发送到错误的目的局域网。因此，穿过广域网的通信流容易被拥有广域网基础设施访问权限的人员拦截。由于广域网基础设施比局域网更容易访问，宜小心使用以确保在广域网中传输的敏感信息被加密。宜与服务提供商签订合同，以证明组织所要求的安全等级。

13.2.3.2 安全风险

有线广域网不但具有与有线局域网（见13.2.2）相同的主要安全风险，它还具有更多的安全风险，其原因是在广域网中网络通信流暴露的更多，这意味着控制，包括访问控制在内，它得到适当安排以确保有线广域网不能被轻易地攻破而造成广泛的破坏。同样地，无线广域网不但具有与无线局域网（见13.2.2）相同的主要安全风险，它还更容易受到破坏，因为用于传输网络包的系统有拥塞的可能性，总体而言，与广域网相关的关键风险包括：

- 入侵，此时信息被暴露或数据完整性不能得到保证；
- DoS攻击，此时资源对授权用户不可用；
- 一个人在家使用的第三方连接和拨号接入互联网帐号，能够容易地绕过在网络和服务级别实施的任何控制措施，使得企业网络暴露给电子邮件产生的蠕虫、特洛伊木马病毒和各种病毒；
- 延迟期延长，这将影响IP服务的语言；
- 网络上的抖动，这将影响语音质量（主要是因使用铜缆来提供服务而造成）；
- 设备故障；
- 电缆故障；
- 未安装补丁的设备；
- 传输站断电，它影响其他许多部分；
- 服务提供商的网络管理设施。

13.2.3.3 控制

要求保护广域网的关键安全控制措施，包括：

- 将Telnet和FTP之类内在不安全的协议替换为SSH和SCP之类安全协议；
- 给管理链接加密；
- 使用适当的设备报警SNMP报告来实施安全鉴别，以访问广域网设备；
- 保护每个站点的广域网物理设备，如使用具有接触警告的上锁机柜；
- 使用UPS以确保电源供应不受到破坏；
- 使用多种路由的双连接站点；

- 主动轮询广域网设备；
- 识别未授权设备的网络设备映射；
- 为管理设施安装补丁；
- 加密覆盖敏感数据；
- 从服务提供商获得服务保证，如延时和抖动的服务保证；
- 对访问广域网的设备实施审计和计费；
- 使用防火墙以丢弃进入网络的任何意外的通信流；
- 确保MPLS结构和地址是隐藏的；
- 分配不能在互联网上选择路由的IP地址；
- 使用网络地址转换，它隐藏内部IP地址，但允许具有能选择路由地址的设备从互联网发出请求；
- 使用抗病毒软件来防止恶意代码，如木马、病毒和蠕虫从网络内打开安全漏洞；
- 使用IDS来识别可疑通信流；
- 确保网络管理系统在逻辑上是安全的；
- 确保网络管理位置在物理上是安全的；
- 确保设备均有备份；
- 对网络管理人员进行可靠性检查。

13.2.4 无线网络

13.2.4.1 背景

无线网络被指定为覆盖地理上的小型区域且使用无线电波或红外线之类非基于连线的通信手段的网络。通常情况下，无线网用于实施与局域网相同的连通性，因此也称作无线局域网。它使用的主要技术在GB 15629.11-2003和蓝牙技术中被标准化。宜强调的是，无线网络是由不同类别的无线电网络构成的，如GSM、3G和VHF，这些网络利用天线进行传输（见13.2.5）。

无线局域网具有有线局域网的所有脆弱性，加上一些与无线链接特征相关的特定脆弱性。已经开发了一些特定技术（多数技术是基于加密的）来处理这些附加脆弱性，由于这些技术（如WEP）的较早版本具有结构性弱点，因此未满足关于保密性要求的期望。

13.2.4.2 安全风险

与使用无线局域网相关的关键安全风险包括：

- 窃听；
- 未授权访问；
- 干扰和拥塞；
- 配置错误；
- 安全接入模式被默认为关闭；
- 有缺陷的WEP或TKIP；
- 用于管理无线局域网的有缺陷的SNMP；
- 不是总能看到正在使用无线局域网的人。

13.2.4.3 控制措施

无线局域网需要的控制措施包括：

- 给企业基础设施中的无线局域网配置防火墙；
- 在客户和边界防火墙之间的无线局域网实施基于IPsec的VPN；

——考虑通过在客户端设备上配置个人防火墙、入侵检测和抗病毒软件来提高每个无线局域网设备的安全性；

——传输的控制以消除对组织物理域之外的传播；

——为只读访问配置SNMP；

——带外加密管理，例如使用SSH；

——维护无线接入点的物理安全；

——所有服务器组件的加固；

——系统测试；

——考虑在企业网络与无线网络之间部署IDS。

13.2.5 无线电网络

13.2.5.1 背景

无线电网络是指使用无线电波作为连接介质以物理覆盖广大区域的网络。无线电网络的典型例子是移动电话网络，它使用如GSM或UMTS等技术并提供公开可用的语音与数据服务。

这里要强调的是，使用无线电波来覆盖小区域的网络被认为是不同类别的网络，见13.2.4。

无线电网络的例子包括：

——TETRA；

——GSM；

——3G（包括UMTS）；

——GPRS；

——CDPD；

——CDMA。

13.2.5.2 安全风险

有若干能造成应用于无线电网络的风险，一般安全威胁场景：

——窃听；

——会话劫持；

——冒充；

——应用级威胁，如欺诈；

——拒绝服务。

某些类型无线电网络情形中风险的例子，如以下段落中所示。

与GSM有关的安全风险包括以下事实：

——A5/x算法和Comp128-1偏弱；

——一般的GSM加密是关闭的；

——SIM克隆是一种现实情况。

与3G有关的安全风险包括以下事实：

——手机易于受到电子攻击，包括恶意代码的插入，例如病毒；

——因为手机经常一直开机，所以受到攻击的机率偏高；

——服务可能会受到窃听；

——无线电网络可能拥塞；

——有可能插入虚假基站；

——网关可能受到未授权访问；

- 服务可能受到攻击和经由互联网的未授权访问；
- 有可能引入垃圾邮件；
- 管理系统可能会受到经由RAS的未授权访问；
- 由于工程支持设备（包括膝上型计算机）的丢失或被盗，而导致服务被攻击。

UMTS是全球3G移动技术系列中的关键成员，它提供大容量和较强的宽带能力来支持较多的语音和数据客户。它使用5MHz信道承载宽度来交付极高的数据速率并增大容量；提供无线电资源的最佳时间，特别是对于已被授予大量、连续频谱块的操作者而言（其范围通常从2x10MHz至2x20MHz），以降低部署3G网络的成本。

通过增强GSM网络功能得到的GPRS，是迈向第三代移动网络的至关重要的第一步。GPRS是在GSM网上传输数据的规范，它允许包交换通信流和电路交换通信流，同时在GSM的基础设施中存在。GPRS使用多达8个9.05Kb或13.4Kb的TDMA时间段，其全部带宽是72.4Kb或107.2Kb。GPRS同时支持TCP/IP和X.25通信。开启EDGE的GPRS网络能够实现EGPRS—增强版的GPRS，它将每个时间段的带宽增加到60Kb。GPRS开启一个“永远打开”的互联网连接，这是一个潜在的安全问题。GPRS网络提供商一般试图通过提供在GPRS网络与互联网之间的防火墙来提升该链接的安全性，但因应将其配置为允许有效服务工作而可能被第三方利用。

CDPD是一个支持无线接入互联网和蜂窝电话网络上其他公共包交换网络的规范。CDPD支持TCP/IP和CLNP。CDPD使用具有40比特密钥的RC4流加密。CDPD在IS-732标准中定义。该算法并不强壮，能被穷举攻击解密。

CDMA（一种扩频形式），是一种已使用多年的数字通信技术系列。广谱技术的核心原则是使用类噪声载波，它具有的带宽比数据传输速率相同的简单点对点通信所要求的带宽要宽得多。数字编码技术允许CDMA防止有意或无意的窃听。CDMA技术把声音分割成在广谱频率上传输的几个小比特。对话（或数据）中的每个小比特通过只有CDMA手机和基站才知道的数字编码来识别。这意味着实际上没有任何其他设备能接收此呼叫。由于任何呼叫都有数以百万计的代码组合可用，所以它抵御窃听。

13.2.5.3 安全控制措施

有若干技术安全控制措施来管理已识别威胁对无线电网络的风险，包括以下方向：

- 安全鉴别；
- 使用有效算法加密；
- 受保护的基站点；
- 防火墙；
- 恶意代码（病毒、木马等）防护；
- 反垃圾邮件。

13.2.6 宽带网

13.2.6.1 背景

宽带网是一组允许单个用户高速接入一个互联网存在点的技术。目前，有四种主要技术：

- 3G；
- 电缆；
- 卫星；
- DSL。

DSL有两种主要类型，分别是非对称的DSL（ADSL）和对称的DSL（SDSL）。ADSL从用户端上传的速度要比下载的速度慢（是下载速度的四分之一到一半），而SDSL的上传和下载的速度相同。这两种类型的下载速度范围通常在128kbps至2-8Mbps之间，依赖于产品。电缆和卫星技术也有相似类型的产品。

采用宽带技术的主要原因是，它们是高速的，总是使用比常规通信技术更廉价的技术。所有技术都允许介入到互联网，因此仅将互联网跨越到用户的处所。使用互联网作为通用承载允许至其他站点的链接被快速、便宜地构建，可能对安全的链接部署VPN。

13.2.6.2 安全风险

. 6.2 安全风险

宽带仅是一个在用户与互联网之间“永远打开”的高速链接。这些特点使得颠覆宽带连接系统成为黑客一个有价值的命题，并直接导致下列风险：

- 泄露、修改或删除信息，作为未授权远程访问的成果；
- 恶意代码的传播；
- 上传/下载和执行未授权代码；
- 身份盗窃；
- 错误配置客户端系统；
- 软件脆弱性的引入；
- 网络拥塞；
- DoS。

13.2.6.3 安全控制措施

有若干技术安全控制措施来管理已识别威胁对宽带通信的风险，包括：

- 小型办公室/家庭办公室（SOHO）防火墙；
- 反恶意代码（包括病毒）软件；
- IDS，包括IPS；
- VPN；
- 软件更新/打补丁。

13.2.7 安全网关

13.2.7.1 背景

按照文件化的安全网关服务访问策略，适宜的安全网关布置，宜保护组织的内部系统，并安全地管理和控制通过它的通信流（见13.2.7.3）。

13.2.7.2 安全风险

黑客每天都用更先进的手段来尝试攻破业务网络，而网关是其兴趣的中心。在未授权方面的尝试可以是恶意的，如导致DoS攻击，它们可能是滥用资源或能够获其有价值的信息。网关需要保护组织，免受来自外界（如来自互联网或第三方网络）的此类入侵。内容未得到监控而流出组织，导致法律问题和知识产权的潜在损失。此外，随着越来越多的组织正在连接到互联网上以满足其组织要求。他们面临的需求是控制对不当或有异议的Web站点的访问。如果没有这种控制，组织就会用非生产性Web浏览而面临生产力损失、责任暴露和带宽分配不当的风险。如果这些威胁未得到处理，就会有以下风险：与外界的连接不可用、数据损坏或有价值的企业资产遭受未授权泄露。未经适当授权就把数据放在网站上或传输，也可能招致法律的惩罚，如内幕交易。

13.2.7.3 安全控制措施

安全网关宜：

- 分隔逻辑网络；
- 对于逻辑网络之间流经信息提供限制和分析功能；
- 被组织用作对出入组织网络访问的进行控制的手段；
- 提供可控可管的网络单一接入点；
- 强化组织对网络连接的安全策略；
- 提供日志的单一记录点。

宜为每个安全网关都开发一个单独的服务访问（安全）策略文件，并实施其内容以确保只允许得到授权的通信流通过。该文件宜包含网关所要求的规则集来管理和配置网关。宜可能按照通信协议和其他细节来分别定义许可的连接。因此，为了确保只有合法用户和合法通信流获得通信连接访问权，该策略宜规定并详细记录适用于流入和流出安全网关之通信流的约束和规则，以及各种管理和配置参数。所有安全网关宜充分利用可用的身份识别和鉴别、逻辑访问控制和审计设施。此外，他们宜定期检验。安全网关是否有未授权的软件和/或数据，如果发现此类软件或数据，宜按照组织和/或团体的信息安全事件管理方案（见GB/Z 20985）生成事件报告。

值得强调的是，与网络的连接仅在所选择的安全网关经检验符合组织和/或团体的要求，且此类连接所造成的风险能够被安全地管理之后，才宜发生。宜确保不可能绕过安全网关。

防火墙是一个良好的安全网关例子。防火墙通常宜达到与所评估风险一致的、适当的保证级别，它使用标准防火墙规则集，通常开始时，拒绝内部网络与外部网络之间所有访问，并添加显式规则仅满足所要求的通信路径。

有关安全网关的更多细节见GB/T 25068.3（以及GB/T 22081-2005和ISO/IEC 13335-2）。

宜注意的是，虽然个人防火墙（一种特殊的防火墙类型）的网络安全方面，未在GB/T 25068.3中讨论，但也宜考虑。与受到专用防火墙保护的很多中心站点不同，远程系统可能无法保证支持这些设备的开销和专业技能。可能代之以使用个人防火墙来控制流入（有时是流出）远程计算机的通信流。防火墙规则（策略）的常规管理可能由中心站点的人员远程执行，以减轻对远程系统用户技术理解的要求。然而，如果不可能做到这一点，那么就宜小心以确保有效的配置，如果远程站点的工作人员不是IT专业人士就更应如此。一些个人防火墙也能限制到授权程序（甚至图书馆）的网络传输能力，限制恶意软件传播的能力。

13.2.8 远程访问服务

13.2.8.1 背景

RAS的目标是允许数据远程站点与中心服务之间交换。为此有各种解决方案，包括：

- 经由互联网通信；
- 拨号接入IP服务。

经由互联网的通信越来越多地使用ISP提供的ADSL链接来提供中心站点到远程站点的高带宽和远程站点到中心站点的较低带宽。除了敏感性最低的数据外，一些形式的VPN（见13.2.9）宜被用来为交换的数据流提供安全。

拨号接入IP服务允许远程站点（通常是单个用户）拨号接入中心的调制解调器组。鉴别之后，打开远程站点与中心服务之间的连接。除非应用实施安全协议，否则这种模式的通信通常以明文方式进行。RAS访问可能使用ISDN或模拟线路实施。用户都拨号接入到具有某个鉴别等级的中心点。RAS访问仅提供明文数据的传输。

13.2.8.2 安全风险

存在若干可能与RAS有关的安全风险，包括：

- 未经授权而访问组织的系统、服务和信息（包括通过窃听），从而导致信息和/或服务的泄露，

未授权变更或破坏；

- 将恶意代码引入到组织的系统、服务和信息，使其被篡改、不可用和遭到破坏；
- 针对组织服务的DoS攻击。

13.2.8.3 安全控制措施

远程接入要求中心服务保护自身免受未经授权访问。同样的，期望远程系统本身具有免受若干安全威胁的保护的能力。可能要求的控制措施包括：

- 防火墙（包括个人防火墙）；
- 路由器ACL；
- 互联网访问链接的加密；
- 呼叫线路标志；
- 强鉴别；
- 抗病毒软件；
- 审计管理。

有关远程接入服务安全的更多细节见GB/T 25068.4。

13.2.9 虚拟专用网

13.2.9.1 背景

VPN是一种通过使用现有网络设施而实施的专用网络。从用户的角度来看，VPN的表现类似专用网络，它提供类似的功能和服务。VPN可用于各种情形，诸如：

- 移动或非现场员工实现对组织的远程访问；
- 将组织不同位置链接在一起，包括冗余链接以实现回退基础设施；
- 为其他组织/业务伙伴建立到组织网络的连接。

换言之，VPN允许两个计算机或网络通过不安全的介质（例如互联网）进行安全的通信。传统上，这种通信一直是使用具有链接加密器的租用线路来执行，所以费用很高。然而，随着高速互联网链接和在每一端的适当终止设备的出现，站点之间可靠而安全的通信能通过使用VPN来建立。

13.2.9.2 安全风险

在不安全网络上通信的关键安全风险包括：敏感信息可能被未授权方访问，从而导致信息受到未授权的泄露和/或修改。除了通信与局域网和广域网相关的风险外（见13.2.2.2和13.2.3.2），与VPN相关的一般风险包括：

- 不安全的实施，通过：
 - 未测试的或有缺陷的加密套件；
 - 能够容易猜中的弱共享秘密；
 - 不良网络拓扑结构；
 - 远程客户端安全的不确定性；
 - 用户鉴别的不确定性；
- 下层服务提供商安全的不确定性；
- 低劣的性能或服务可用性；
- 不符合某些国家中有关加密技术使用的法律法规要求。

13.2.9.3 安全控制

在VPN中，密码技术一般用于网络和/或应用协议中以实现安全功能和服务，尤其是当其上构建VPN的网络是公共网络（例如互联网）时。在大多数的实现中，参与者之间的通信链路都被加密以确保保密性，而鉴别协议用于验证连接到VPN系统的身份。通常，被加密的信息是通过一个连接到组织网关的安全“隧道”来传输并保持信息的保密性和完整性。然后由网关来识别远程用户并且让用户只访问那些被授权接收的信息。

因此，VPN是一种基于协议隧道的机制—将一个完整的协议（客户端协议）作为一个简单的比特流来处理，并将其封装到另一个协议（承载协议）之内。通常，VPN协议为客户端协议提供安全性（保密性和完整性）。在考虑VPN的使用时，宜得到处理的体系结构方面包含：

- 端点安全；
- 终止点安全；
- 恶意软件保护；
- 鉴别；
- 入侵探测；
- 安全网关（包括防火墙）；
- 网络设计；
- 其他连通性；
- 隧道分离；
- 审查日志和网络监控；
- 技术脆弱性管理。

关于VPN的更多细节，包括这些体系结构的每一方面，见GB/T 25068.5。

13.2.10 IP 融合（数据、音频、视频）

13.2.10.1 背景

由于语音和数据融合日益普及，其安全问题宜被认识和处理。尽管目前的拨号服务实现要求安全控制措施来防止话费欺诈和语音邮件以及其他安全违规，这些系统并未集成到企业数据网络内，未受到IP数据网络相同的风险。随着语音和数据的融合，需要实现安全控制措施来降低被攻击的风险。

VoIP应用通常包括驻留在开放的或市售的硬件上的专用软件和操作系统。服务器的数量取决于供应商的实现以及实际的部署。这些组件经由以太网之上的IP进行通信，并经由交换机和/或路由器彼此互连。

13.2.10.2 安全风险

主要的风险领域能够与针对供应商特定的软件脆弱性进行的基于IP的攻击、硬件和托管VoIP应用的操作系统平台相关。与VoIP组件相关的风险包括对基于网络的设备和应用的攻击，可能被VoIP组件解决方案的设计或实施中的脆弱性激活或促进。考虑的风险领域包括：

- QoS—没有全面的QoS就没有质量的损失，或者由于包丢失而导致的呼叫中断，以及穿越网络的传播延迟；
- 用DoS攻击或路由表的变更而导致的服务不可用；
- 完整性和可用性可能受到病毒的影响，病毒可能会设法通过不安全的VoIP系统进入网络，从而可能导致服务降低甚至造成服务损失，还可能传播到网络中的服务器，从而导致数据存贮受损；
- 客户端个人计算机上的软电话是一个重大风险，它们能够是病毒和入侵的进入点；
- VoIP服务器和VoIP管理系统若没有防火墙的保护将存在风险；

——由于防火墙上的多个端口被打开以支持VoIP，可能导致数据网络安全降级。一次VoIP会话有很多相关的协议和端口号。H. 323使用很多协议来发送信号，H. 323和SIP都使用RTP。其结果是H. 323会话可能使用多达11个不同的端口；

——欺诈是拨号服务的一个关键问题，如果安全未得到处理，那么VoIP只能增加到风险之列。黑客能够通过欺骗、重放攻击及连接劫持来获得对VoIP服务的未授权访问。话费欺诈，或未授权呼叫用户付费特服号码，也会导致重大损失；

——保密性违规可能由通信拦截所致，诸如中间人攻击，在员工和其他人员访问网络时，是有可能在网络内发生的；

——窃听语音呼叫；

——由于IP电话要求有电源才能运行，所以电话网络在电源失效的情况下不能是可操作；

——由于使用通用组件，如局域网，所以语音和数据服务均有较大的失效风险。

13.2.10.3 安全控制措施

有若干安全控制措施技术来管理针对IP融合网络的已识别威胁的风险，包括：

——QoS设施在融合网络中应该应用，否则语音质量可能受损。网络服务交付以及其他可能的情况下，IP链接宜通过光纤被交付到站点以确保抖动（它影响语音质量）最小；

——所有VoIP服务器宜配置恶意软件防护；

——PC支持的软件电话宜安装个人防火墙，且病毒检查软件宜频繁更新；

——VoIP服务器和VoIP管理系统宜被保护于防火墙之后，以防护它们免遭攻击；

——设计者宜确保在防火墙上只开启最少的端口来支持VoIP服务；

——为了对付话费欺诈和反欺骗，需要实施反重放控制措施来防止连接劫持；

——对管理服务器的所有访问宜被鉴别；

——语音和数据服务宜在可能的情况下被分隔；

——对于服务器支持的VoIP服务宜考虑IDS；

——当敏感信息要在VoIP网络上讨论时，宜考虑数据路径加密；

——IP电话宜由UPS支持的以太网集线器供电；

——可能需要提供常规语音服务，它有独立的电源供其在紧急情况下使用。

13.2.11 使得对（组织）外部网络所提供服务的访问成为可能

13.2.11.1 背景

对组织开放电子邮件和互联网服务以满足合法业务要求会带来各种威胁，这些威胁能够用于利用脆弱的系统，除非这些服务的设计和运行良好，否则它们会给组织带来相当大的风险。例如，尽管滥发垃圾邮件者在接近工作人员方面有屏障，但垃圾邮件仍然给企业及其员工们造成很大问题。由于滥发垃圾邮件者试图收集员工名字，大多数企业将需要部署反垃圾邮件技术，并教育用户保护其电子邮件。此外，用户需要被保护，以免在访问互联网时将恶意软件，如木马带回到组织。这种恶意软件将导致信息系统和组织声誉受到代价高昂的损失。要始终牢记的关键点是：互联网是不可信的。

13.2.11.2 安全风险

开启对组织外部网络所提供服务的访问的关键风险领域和在互联网和电子邮件服务中能够被利用的脆弱性包括：

——潜在导入破坏性恶意软件，诸如木马；

——接收压倒性的垃圾邮件；

- 丢失组织信息；
- 破坏信息完整性或者丢失信息；
- DoS攻击；
- 未授权使用互联网和电子邮件服务，包括不遵从组织策略（例如为了自身利益而使用服务）以及不遵从法律法规（例如发送恐吓电子邮件）。

13.2.11.3 安全控制

管理互联网/电子邮件解决方案中已识别威胁之风险的技术安全控制措施，包括：

- 使用防火墙且其保证级别与被评估风险相当，并且防火墙规则集包括：

默认“否认一切”策略；

只流出Web（例如http/https）；

双向电子邮件。

- 在路由器上使用访问控制表（ACL）和网络地址转换（NAT）来限定和隐藏IP地址结构；

——启动反欺骗来防止外部攻击。反欺骗控制采取的形式为：不接受来自外部（例如来自互联网）却声称源自组织内部的消息，反之亦然；

——启动Web和电子邮件代理作为工作站用户与互联网之间的中介，使得企业能够确保安全、常规管理控制和缓存服务。安全通过以下几种方式强制执行：针对“黑”名单和“白”名单（对于互联网访问）来比较所请求的URL，扫描已知模式的数据，在内部地址与外部地址之间进行转换，创建请求和请求者的审计日志以及拥有基于代理的抗病毒设施；

——在Web和电子邮件代理上的抗病毒控制措施。典型控制措施包括隔离可疑文件的设施（例如根据内容类型），针对“黑”名单筛选所请求URL或电子邮件地址（宜注意的是，不能认为黑名单是十分安全的，特别是在此类名单是从他处获得时。可能有误判的危险。）有关抗病毒控制措施的更多信息见13.9；

——电子邮件服务器上的反中继转信和反向DNS查找。反中继转信控制措施检测传入的电子邮件是否来自正确的发送组织，若不是，则该电子邮件被载入日志（或被隔离）。并且电子邮件服务器不采取进一步动作；

——启用报警和SNMP陷阱。SNMP能够用于联网设施的远程控制，还可以用作发送消息（或“陷阱”）的设备来通知此设备处条件的监控台；

- 网络审计日志载入和监控（见13.7）；

——设定带外数据（OOB），它与对数据使用不同网络的实践和管理有关，用来确保攻击者不能可连接到其目标设备；

——确保用于访问互联网服务的客户端软件（例如Web浏览器）中的脆弱性通过使用适当的脆弱性和补丁管理过程而被适当的穿过。

13.2.12 万维网托管体系结构

13.2.12.1 背景

万维网托管服务由许多网络服务提供商以规范服务的形式来提供，它经常包括用于处理持久性数据的数据库设施以及作为基本应用的运行时环境。尽管实施和提供Web托管服务所需的大部分组件超出本部分的范围（诸如Web服务器或数据库软件），但是关于整个服务自身的一些考量在这里被文件化，因为许多人把Web托管看作是网络提供的一个完整部分。

万维网托管站点会面临各种各样的风险，特别是它们被连接到互联网的时候，例如一些著名的组织可能处于边缘团体的攻击之下。因此，重要的是，所有潜在的威胁被识别，然后是可能被威胁利用的所

有脆弱性被关闭。这些最好通过结构设计无脆弱性来加以实现。通过按照所提供的指南来处理这些问题，就应有可能设计一个安全、可靠且被破坏风险低的Web站点。

13.2.12.2 安全风险

关键风险领域包括以下所示几个方向：

- 攻击者对具有单个边界保护漏洞的应用和数据访问；
- 暴露基础结构组件的脆弱性；
- 多重单点故障；
- 因硬件故障而丢失服务；
- 没有取得维护服务的能力；
- 公共用户对数据存储范围的无意讨论；
- 被上传到系统内的恶意软件；
- 使用交换功能的Web站点漏洞；
- 没有进行备份而不影响Web站点性能的能力；
- 未授权泄露IP编址规划从而使得对Web站点的攻击更便利；
- 对管理站与Web站点之间的连接加以利用；
- 未被发现的攻击；
- 跟踪设备之间入侵的困难性；
- 没有恢复数据的能力；
- 没有满足服务等级协议要求的能力；
- 没有维持服务持续性的能力；
- 未授权使用Web服务，包括违反组织策略（例如为自身的利益而使用服务器）和不遵从法律法规（例如保存侵犯版权的资料或保存儿童色情资料）。

13.2.12.3 安全控制措施

管理来自Web站点已识别威胁之风险的技术安全控制措施，包括：

- 提供分区和深度安全来限制成功攻击影响；
- 规范不同的防火墙类型以反击可能的防火墙脆弱性。（有关防火墙的更多信息见13.2.7和GB/T 25068.3）；
- 弹性：宜检查设计是否有潜在的单点故障并宜将其消除；
- 预防设备故障容错转移/负载共享；
- 在24×7的环境中高可用性的集群是必要的；
- 限制对Web站点内访问的代理服务 and 开启高等级日志载入；
- 上传时的抗病毒控制，用来阻止恶意软件进入。（更多有关检测和阻止恶意代码控制措施的信息见13.9）；
- 通常在Web站点设计中使用的第2层交换。除非是业务相关的要求，诸如负载共享，否则不宜使用第3层交换。此外，同一物理转换不宜在防火墙的任何一侧使用。测试点宜包含在交换机设计中；
- 按功能分隔的虚拟局域网（VLAN），使得入侵监测系统（IDS）更容易被调整，因为任何VLAN上都有一个简化的协议集。此外，备份VLAN的实施将允许备份在一天中的任何时段执行，而不会危害站点的性能；
- IP编址规划将公共地址的数量限定到最少，并将IP编址规划保持在“最严格的保密”状态，因为有关它的知识可以用于在Web网站上展开攻击；

GB/T 25068.1—20XX/ ISO/IEC 18028-1

——在管理链接通过公共网络彼此连接时，它们宜被加密（更多有关远程接入的信息见GB/T 25068.4）。这至少包括在控制台端口连接上的报警/简单网络管理协议（SNMP）陷阱；

——来自每个设备的所有事务和事态日志都被复制到审计服务器，然后被复制到备份介质，诸如CD。（更多有关网络审计日志载入和监控的信息见13.7）；

——实施时间同步服务，因为这是分析未授权访问和能够通过日志文件跟踪其踪迹的关键。这要对所有日志文件和服务器被同步到加/减1秒或更低。（网络时间协议（NTP）与此有关，更多信息见GB/T 22081和10.6）；

——集中式化备份服务，选择它的原因是它更可能被按需执行；

——由于在很多情况下，Web站点需要每天24小时运行，这要求能承受此环境的高质量硬件。Web站点的服务器基础设施宜被规定为支持“24×7”运行。支撑操作系统宜被固化，并且所有服务器和其他设备也宜经历安全测试以确保所有设备均被完全固化；

——实施健壮的应用软件，其代码的结构已得到检查，它在逻辑上是正确的，并使用许可的鉴别软件。

也宜注意的是，在设计Web站点时，业务持续性管理问题经常未被充分考虑。全部业务持续性管理活动宜与Web站点联系起来进行。（更多有关业务持续性管理参考的信息见13.11。）

13.3 安全服务管理框架

13.3.1 管理活动

对于任何网络，一个关键的安全要求是它受到安全服务管理活动支持，这些活动将发起并控制安全的实施和运行。这些活动宜发生以确保组织或团体的所有信息系统的安全。关于网络连接，管理活动宜包括：

- 定义所有与网络安全有关的责任，并指定担负全面责任的安全管理者；
- 网络安全策略文件化，并附文件化技术安全体系结构；
- 文件化安全操作（SecOP）；
- 进行安全合规检查，包括安全测试，以确保安全被维持在所要求的等级；
- 在外部组织或人员许可连接之前，文件化连接遵从的安全条件；
- 文件化网络服务用户的安全条件；
- 文件化安全事件管理方案；
- 文件化并测试业务持续性/灾难恢复计划。

宜注意，本章以GB/T 22081和ISO/IEC 13335-2中描述的内容为基础。本部分只进一步描述上述主题中对网络使用尤其重要的那些主题。因此，更多的信息（例如有关网络安全策略和安全操作规程的内容）和这里未进一步提及的主题，读者宜查阅GB/T 22081和ISO/IEC 13335-2。

13.3.2 网络安全策略

明显地接受和支持组织的网络安全策略（在GB/T 22081中所提到的）是管理的责任。这一网络安全策略宜来自于组织的信息安全策略，并与其相一致。此策略宜能得到实施，容易被组织中得到授权的成员使用，并包含有关以下方面的清晰陈诉：

- 组织对可接受网络用法的立场；
- 安全使用特定网络资源、服务和应用的明确规则；
- 不遵从安全规则的结果；
- 组织对网络滥用的态度；
- 策略及所有特定安全规则的基本原理。

（在某种情况下，如果这些清晰的陈述更方便和/或它们对员工更清晰，它们可能与信息安全策略相结合。）

网络安全策略的内容通常宜包括安全风险评估和管理评审结果的概要（它提供在控制措施方向花费理由），包括选中的、与评估风险相当的所有安全控制措施的细节（见第12章）。

13.3.3 安全操作规程

为支持网络安全策略，应开发和维护SecOP文件，适当覆盖每个网络连接。它们宜包含与安全相关的日常操作规程的细节，以及何人员负责其使用和管理。

13.3.4 安全合规检查

对于所有的网络连接，安全合规检查按照综合核查表进行，该核查表按照如下几个方面中规定的控制措施进行构造：

- 网络安全策略；
- 相关SecOP；
- 技术安全体系结构；
- 安全网关服务访问（安全）策略；
- 业务持续性规划；
- 连接的相关安全条件。

这种检查宜发生在任何网络连接的有效操作和主要的新发布之前（与重要的业务或网络有关变更相关），否则每年进行一次。

这种检测宜包括进行针对认可标准的安全测试，测试时使用安全测试策略及预先生成的相关计划，该计划精确地规划要进行何种测试、使用什么、何时何处进行。通常它宜包含脆弱点扫描与渗透测试的组合。在任何此类测试开始之前，宜检查测试计划以确保测试将以完全符合相关法律的方式进行。在执行这种检查时，不应忘记，网络不可能仅限于一个国家之内-它可能分布于具有不同法律的不同国家。该测试结束后，其报告宜指出所遇到脆弱性的细节和要求的修正及其优先级。

13.3.5 连接的安全条件

除非连接的安全条件适当并且实际上被认可，否则，组织实际上要接受与其域外的网络另一端连接的相关风险。此类风险可能与隐私/数据保护相关，即连接可能被用于交换位于一端或两端并受到国家法律保护的个人数据，而网络连接的另一端（在组织的域之外）位于另一个国家，且其法律可能是不同的。

例如，组织A可能要求组织B在能够经由网络连接而与其系统相连接之前，B宜保持并展示其系统涉及此连接的特定安全性等级。通过这种方式，能够向A保证B正在以一个可接受的方式管理其风险。在此情况下，A宜生成连接安全条件文件，该文件详述B端提供的控制措施。这些控制措施宜由B实施，随后是该组织签署对将保持的效果和安全的绑定声明。A将保留委托权或对B进行合规检查。

在有些情况下，一个团体中的各个组织彼此认可一个“连接安全条件”文件，该文件记录所有各方的义务和责任，包括相互的合规检查。

13.3.6 网络服务用户的文档化安全条件

宜给已得到远程工作授权的用户颁发“网络服务用户安全条件”文件。该文件宜描述用户对硬件、软件、与网络有关数据以及安全的责任。

13.3.7 事件管理

在有网络连接之处（和没有网络连接相反），信息安全事件较有可能发生，并对结果有较严重的不利影响。此外，特别是对于到其他组织的网络连接，可能有与事件有关联的重大法律意义。

因此，具有网络连接的组织宜适当安排良好的文件化的并被实施的信息安全事件管理方案和相关的基础设施，它们能够在事件被识别时快速响应，将其影响最小化并吸取教训以试图防止此类事件再次发生。这个方案宜能够处理信息安全事态（系统、服务或网络的一种可识别状态的发生，它可能是对信息安全策略的违反或防护措施的失效、或是和安全关联的一个先前未知的状态）和信息安全事件（单个的或一系列有害或意外的信息安全事态，它们具有损害业务运作和威胁信息安全的极大可能性）。

更多有关信息安全事件管理的细节见GB/Z 20985。

13.4 网络安全管理

13.4.1 引言

所有网络的管理都宜以安全的方式来承担，并且确实为全面的网络安全管理提供支持。这宜通过适当考虑可用的不同网络协议及相关安全服务来完成。

为促进这一点，组织宜考虑若干控制措施，其中的大多控制措施能够使用GB/T 22081和ISO/IEC 13335-2加以识别。此外，无论是虚拟的还是物理的远程诊断端口，宜得到保护免遭未经授权访问。

13.4.2 网络的各个方面

网络的各个方面可分类如下：

网络用户-作为网络用户和/或管理员的人员。其用户的范围从经由互联网、拨号或无线连接来访问远程资源的个人，到使用连接到局域网的工作站或个人计算机的个人。连接到局域网的用户也能经由可能在其局域网和其他网络之间存在内部网络连接与远程资源相连接。此类底层连接可能对用户是透明的；

终端系统-连接到网络上的计算机、工作站和移动装置（例如智能电话和PDA）它们包括用于访问联网设施的装置（例如客户端系统）和用于提供服务的装置（例如服务器和主控计算机系统）。此分类包括硬件、操作系统软件 and 所有本地应用软件，包括用于访问网络的软件。

网络应用-在联网服务器或主机系统上运行的应用软件，经由计算机网络连接来访问，它提供例如：

- 金融交易服务；
- 企业软件服务（例如CRM、EIS和MRP等）；
- 基于Web的服务；
- 在线数据库服务；
- 在线存储设施。

网络服务-由网络提供的服务，通常在构成网络基础设施一部分的终端主机或服务器系统的软件中实现。例如：

- 连通性；
- 电子邮件
- 文件传送；
- 目录服务。

网络服务可能：

- 由组织拥有并运作；
- 由组织拥有但由外部机构按合同运作；
- 从外部机构租借；
- 专门从外部提供商购买；
- 以上情形的组合。

网络基础设施-底层硬件和软件设施，例如：

- 安装场所；
- 布线；
- 无线设施；
- 网络设备（例如路由器、交换机、调制解调器等）。

如前面的第12章所述，网络安全的这些方面宜被模型化为网络分面。这些分面实际上构建在彼此之上以形成网络安全管理框架，如下面的图4所示：

网络用户
网络终端系统
网络应用
网络服务
网络基础设施

图4 网络安全管理框架的分面

由于有些系统在所有实际网络场景中履行多个角色，所以难免产生一些重叠。然而，功能的这些概念层面宜辅助所要求评估的系统过程，来确定在任何特定网络场景中出现的安全风险。概念安全框架中的每一层面宜被单个管理，并且所有层面均被共同管理，从而确保安全网络的所有目标均得到满足。

13.4.3 角色与责任

与网络安全管理相关，宜得到激励的角色和责任如下。（宜注意的是，这些角色可按照组织的规模进行组合。）

高级管理：

- 规定组织的安全目标；
- 创立、批准、发布和利用组织的安全策略、规程和规则；
- 创立、批准、发布和利用组织可接受的使用策略；
- 确保安全和可接受的使用策略得到强制执行。

网络管理：

- 制定详细的网络安全策略；
- 实施网络安全策略；
- 实施可接受的使用策略；
- 管理与外部利益相关者/外部服务提供商的接口，以确保其符合内部和外部网络安全策略。

网络安全团队：

- 获得、开发、测试、检查和维护安全组件与工具；
- 维护安全工具和组件以紧密跟踪威胁的演进（例如更新病毒特征码文件）；
- 根据变化的业务需要，更新与安全有关的配置（例如访问控制列表）。

网络管理员：

- 安装、更新，使用和保护网络安全服务与组件；
- 执行必要的日常任务以应用实施中的安全策略所要求的安全规范、规则和参数；
- 采取适当措施来保证网络安全组件的保护（例如备份、监视网络活动、响应安全事件或报警等）。

网络用户：

- 交流其安全要求；
- 遵守企业安全策略；
- 遵守企业可接受的网络资源使用策略；
- 报告网络安全事件；
- 提供对网络安全效力的反馈。

审计员（内部的和/或外部的）：

- 评审和审计（例如定期测试网络安全的效力）；
- 检查系统与网络安全策略的符合性；
- 检查和测试操作安全规则与当前业务要求和法律限制的符合性（例如网络访问的许可列表）。

13.4.4 网络监视

网络监视是网络安全管理中非常重要的一部分。它将在后面的13.7中处理。

13.4.5 网络安全评估

网络安全是一个动态概念。安全人员宜始终跟上该领域的发展，并确保任何网络都能够使用供应商提供的最新安全补丁和更正来连续工作。宜定期采取步骤按照已确定的基准来审计现有安全控制措施，包括使用安全测试-脆弱性扫描等。安全宜成为评估新的网络技术时的主要考量。

13.5 技术脆弱性管理

网络环境，与其他复杂系统一样，不可能没有错误。技术脆弱性经常出现在网络中被频繁使用的组件中并为其而发布。利用这些技术脆弱性能够对网络安全造成严重影响，这些影响常常在可用性和保密性方面观察到。因此技术脆弱性管理宜覆盖网络中的所有组件，并且宜包括：

- 及时获得有关技术脆弱性的信息；
- 评估网络对这些脆弱性的暴露程度；
- 规定适当的控制措施来处理相关的风险；
- 所规定控制措施的实施和验证。

技术脆弱点管理的必要条件宜是可使用所有网络组件的当前完整目录，提供必要的技术信息，例如设备类型、供应商、硬件版本号、固件或软件，以及组织信息，例如负责的常规管理人员。

如果组织已经配置完整的技术脆弱性管理程序，那么将网络组件的技术脆弱性管理集成到整体任务中宜成为推荐的解决方案。（更多有关技术脆弱性管理的信息，包括实施指南，见GB/T 22081。）

13.6 身份标识与鉴别

13.6.1 背景

重要的是确保通过对经由授权人员（无论是组织内还是组织外的）的连接进行的访问加以限制来保护网络服务及相关信息的安全。对这些要求并未排除使用网络连接，因此使用网络连接的适当细节宜通过使用GB/T 22081来获得。ISO/IEC 13335-2也提供相关细节。

与使用网络连接相关的4个控制域，与此类连接直接相关的信息系统，见13.6.2至13.6.5。

13.6.2 远程登录

远程登录，无论是来自远离组织工作的授权人员，来自远程维护工程师，还是来自其他组织的人员，可通过拨号接入到组织、互联网连接、来自其他组织的专线或者通过经由互联网的共享访问来完成。这些连接由内部系统或使用公共网络的合作伙伴按需建立。每种远程登录类型宜有与连接类型性质相称的附加控制措施。控制措施的例子是：

- 不允许从远程接入帐户直接访问系统和网络软件，除非是在已经提供了附加鉴别（见13.6.3）和可能的端到端加密之处；

- 保护与电子邮件软件和由组织人员在组织办公室外使用的、存储在个人计算机或膝上型计算机上的目录数据相关的信息，免授权访问。

13.6.3 鉴别增强

使用用户ID/口令对是鉴别用户的一种简单方式，但是他们能够被泄露或猜测。还有其他更安全的方式来鉴别用户，特别是远程用户。在未授权人员极有可能获得对被保护的和重要系统访问权时，宜要求鉴别增强。这可能是，例如，因为该访问可能是使用公共网络发起的，或者访问的系统可能在组织的直接控制之外（例如通过膝上型计算机）。

在要求网络连接、鉴别增强（例如按照合同）或者由风险证明网络连接鉴别增强正当之处，组织宜考虑通过实施相关控制措施来增强人员鉴别过程。

简单的例子使用以下技术：

- 主叫线路识别（CLID），可把该项技术当作源自电话号码被接收设备看到。尽管CLID作为呼叫方所声称的ID有些价值，但它对欺骗是开放的且不宜用作被证明的ID不需进一步鉴别。在站点之间（特别在点ISDN上）通过备份链路时，CLID经常被用作快速识别符；

- 经由调制解调器的链接。这种链接在不使用时断开，且仅在呼叫方身份验证后才连接。

更复杂但非常重要的例子，特别是在远程接入情景中：

- 使用其它身份识别手段来支持用户鉴别，例如远程验证令牌和智能卡（例如通过附属于个人计算机的阅读器），手持一次性口令密钥生成设备和基于生物识别的设施；

- 确保令牌或卡只能与授权用户的已鉴别帐户（最好是用户的个人计算机和位置/接入点）以及，例如，任何相关的个人识别号码（PIN）或生物特征档案，一起作用。

通常，称其为健壮的、双因子鉴别。如果使用令牌，就要求用户知道一个PIN，具有令牌的PIN能产生唯一的鉴别值。至于智能卡，能够将其看作是自动使用令牌访问。为了使卡能够被“打开”，用户在将卡插入智能卡阅读器后，宜提供此卡的PIN。然后，每当中央或远程系统要求鉴别时，可使用嵌入在智能卡中的密钥，直接“调用”智能卡来给数据“签名”（提供鉴别）。

13.6.4 远程系统身份标识

正如前面13.6.3中所隐含的，相关鉴别宜通过对进行外部访问的系统（以及位置/接入点）加以验证来增强。

应当承认，不同的网络体系结构能够提供不同的身份识别能力。因此，组织可通过选择适当的网络体系结构来实现增强的鉴别。所选择网络体系结构的所有安全控制能力宜加以考虑。

13.6.5 安全单点登录

在涉及网络连接之外，用户可能遇到多重身份识别和鉴别检查。在这种情形下，用户可能被诱导采用不安全的做法，如写下口令或重新使用相同的鉴别数据。安全的单点登录能够通过减少用户需记忆的

口令数来降低此类行为的风险。除降低风险外，也可提高用户工作效率和减少与口令重置相关的帮助平台工作量。

然而，宜注意的是，安全单点登录系统出现故障的后果可能很严重，因为不是一个而是多个系统和应用将处于危险之中，并暴露于漏洞之下（有时称其开放术语为“王国的钥匙”风险）。

因此，可能需要比一般要更健壮的身份识别和鉴别机制，并且从安全单点登录体制中去掉对高权限（系统级）功能的身份识别和鉴别是可取的。

13.7 网络审计日志的载入和监视

非常重要的一点是，要通过审计日志载入和持续监视，并对安全事态及事件进行快速检测、调查和报告，并作出响应，来确保网络安全的有效性。没有这种活动，就不可能保证网络安全控制措施一直保持有效以及对业务运行有相关不利影响的安全事件不会发生。

充足的错误条件和有效事态的审计日志信息，宜被记录，从而能够对可疑的和真实的事件进行彻底评审。然而，由于认识到记录大量与审计相关的信息使得分析难以管理，且能够影响性能，所以必须注意在过去的时间内实际上都记录了些什么。对于网络连接，宜维护包括以下事态类型的审计日志：

- 附带日期和次数的远程登录失败的尝试；
- 失败的再次鉴别（或令牌使用）事态；
- 安全网关通信流违规；
- 远程尝试访问审计日志；
- 具有安全意义的系统管理警报/警告（例如IP地址复制、载体电路中断）。

在联网环境中，审计日志宜从若干资源得到，如路由器、防火墙、IDS中并发送到中央审计服务器进行合并和彻底分析。宜对所有审计日志进行实时和离线检查。在实时检查时，日志可能在屏幕上滚动的显示，并用于对潜在攻击预警。离线分析是必要的，因为它允许进行趋势分析来确定概述。首先，攻击的最初迹象可能是在防火墙日志中存在大量的“滴”，指明针对潜在的目标的探究活动。IDS系统也可能针对攻击特征码实时检测它。因此要强调的是，在选择正确的审计日志分析工具时宜格外注意，以便提供快速的、集中的且容易理解的输出。

按照组织需求，审计踪迹宜在线保持一段时间，同时所有的审计踪迹按照确保完整性和可用性的方式，例如使用如CD的WORM介质进行备份和存档。此外，对于那些希望通过网络连接来攻击系统的人来说，审计日志包含敏感信息或使用信息，拥有审计日志可能会在发生争议时提供通过网络传输的证据—因此它在确保完整性和抗抵赖的环境中是非常有必要的。因此所有审计日志宜得到适当保护，包括存档CD在指定日期被销毁。按照组织要求和国家法律审计踪迹宜被安全地保留一段时间，同样重要的是，对于所有的审计踪迹和相关服务器时间同步问题应被妥善处理，例如使用NTP，特别是对于辩论和起诉时可能要用到的审计踪迹。

正在进行的监视宜包括以下范围：

- 来自防火墙、路由器、服务器等的审计日志；
- 来自审计日志等的警报/警告，将其预配置为通知来自防火墙、路由器、服务器等的某些事态类型；
- IDS的输出；
- 网络安全扫描活动产生的结果；
- 由用户和支持人员报告的事态及事件信息。

（还有安全合规性评审的结果）。

事态可能转化成安全事件但已被阻止，例如，“失败”的登录，或者实际上已导致事件发生但现在已被检测到，例如识别出用户进行了未授权的数据库变更。

需要强调的是，网络监视应以完全符合相关的国家和国际法律法规的方式来进行。这包括数据保护法律和调查法规（按照法律在对其进行任何监视之前所有用户都必须被通知到）。用一般术语表述为，监视宜负责任的进行，而不是，例如，用于评审具有非常有限的隐私法律的国家中员工的行为。很明显，所采取的行动宜与组织的安全和隐私策略相一致，且具有相关责任的适当规程应得到适当安排。如果审计日志证据将用于刑事或民事起诉，网络审计日志载入和监视也宜以辩论上安全的方式进行。

多数网络审计日志载入和监视控制能够通过使用GB/T 22081所要求的、与网络连接和相关信息系统有关的和ISO/IEC 13335-2来确定。

13.8 入侵检测

由于网络连接的增加，入侵者更容易：

- 找到多种方式来渗透到组织或团体的信息系统和网络；
- 伪装其初始接入点；
- 通过网络和目标的内部信息系统来访问。

此外，入侵者正在变得更加老练，而且更先进的攻击方法及工具很容易在互联网或公开的文献中得到。事实上，这些工具中大部分都是自动的，能够非常有效，并易于使用—包括被经验有限的人员使用。

对于大多数组织，阻止所有潜在的渗透在经济上是不可能的。因此，可能会发生入侵。与这些渗透中的大多数相关的风险，宜通过实施良好的身份标识和鉴别、访问控制和计费及审计控制、在经过证明的情况下加上入侵检测能力来处理。这种能力提供一些手段来检测入侵、实时识别入侵并发出适当警报。使得能够在本地收集入侵信息、随后进行合并和分析，以及分析组织正常信息系统的行为模式 / 使用模式。

在很多情况下，可清楚的发现一些未授权的或是有害的事态正在发生。它可能是由于显然未知的原因而导致的轻微的服务降格，或者它可能是不正常的、意外的访问次数，或者它可能是拒绝特定服务。在多数情况下，重要的是要尽快知道入侵的原因，严重程度及范围。

宜注意的是，与前面13.7中隐含的审计日记分析工具和方法以及GB/T 22081和ISO/IEC 13335-2中相关章条相比这种能力更高级。更有效的入侵检测能力使用特别的后处理器，处理器被设计为使用规则来自动分析审计踪迹中记录的以往活动和其他日志来预测入侵，并针对恶意行为或非典型正常使用行为的已知模式来分析审计踪迹。

因此，IDS是一种用于检测进入网络的入侵的系统。有两种类型的IDS：

- 基于网络的入侵检测系统（NIDS）；
- 基于主机的入侵检测系统（HIDS）。

NIDS监视网络中的包并试图通过将攻击模式与已知攻击模式数据库相匹配来发现入侵者。一个典型的例子是寻找到目标机器上很多不同端口的大量TCP连接请求（SYN），因而发现是否有人正在尝试TCP端口扫描。网络入侵检测系统通过混杂地观察所有网络通信流来嗅探网络通信流。

HIDS监视主机（服务器）上的活动，它通过监视安全事态日志或检查对系统的更改，诸如更改关键系统文件或系统注册表来实现这种监视。有两种类型的HIDS：

- 系统完整性检查器，它监视由入侵者作出的对系统文件和系统注册表的更改；
- 日志文件监视器（它监视系统日志文件）。操作系统生成有关关键安全问题的安全事态，诸如用户获得系统级/管理员级的特权。

在某些情况下对检测到的入侵响应能在IDS中自动执行。

更多关于入侵检测的细节见ISO/IEC 18043。

13.9 恶意代码的抵御

用户宜意识到恶意代码，包括病毒，可能会通过网络连接而引入其环境。恶意代码能够导致计算机执行未经授权的功能（例如在给定日期和时间用消息攻击给定目标），或者是，一旦它复制了用于尝试发现其他易受攻击主机的重要资源，就真正销毁它们（如删除文件）。在未造成损害之前恶意代码可能未被检测到，除非实施适当的控制。恶意代码可能造成安全控制的漏洞（例如捕获和泄漏口令），非故意泄露信息，非故意更改信息、破坏信息和/或未授权使用系统资源。

有些形式的恶意代码使用特殊的扫描软件来检测和移除。扫描器可用于防火墙、文件服务器、邮件服务器和针对某种类型恶意代码的工作站。此外，为了能够检测新的恶意代码，非常重要的是要确保该扫描软件总是保持最新，最好是每日更新。然而，用户和管理员宜意识到不能依赖扫描程序来检测所有的恶意代码（甚至是所有特定类型的恶意代码），因为新形式的恶意代码正不断产生。通常情况下，要求其他形式的控制来增强由扫描程序提供的（在扫描程序存在之处）保护。

总之，反恶意代码软件的工作是扫描数据和程序来识别与病毒、蠕虫及木马（有时被统称为“恶意软件”）相关的可疑模式。所扫描的模式库被称作特征码，并且宜被定期更新，或者在新的特征码对于高风险恶意软件警报可用时更新。在远程接入的情况下，抗病毒软件宜在远程系统上运行，也宜在中心系统的服务器上—特别是在窗口和电子邮件服务器上运行。

具有网络连接的系统的用户和管理员宜意识到，当与外部各方通过外部链接交易时，存在着比一般风险更大的与恶意软件相关的风险。宜开发用户和管理员指南来概述规程和做法，以降低引入恶意代码的可能性。

用户和管理员宜特别小心地来配置与网络连接相关的系统和应用，关闭此环境中不必要的功能（例如，PC应用可以配置为宏被默认为关闭，或在执行宏之前要求用户确认）。

更多有关恶意代码保护的细节见GB/T 22081和ISO/IEC 13335-2。

13.10 公共基础设施中基于密码的服务

13.10.1 导言

随着电子形式取代其基于纸张的对应物，对安全性和增强隐私的需求日益增加。互联网的出现和企业网络扩展为包括来自组织外部的客户和提供商的访问，加快了对基于加密技术解决方案的需求，以支持鉴别和VPN，以及确保保密性。

13.10.2 网络上的数据保密性

在保持保密性的重要环境中，宜考虑使用加密控制措施给流经网络连接的信息加密。使用加密控制的决定宜考虑有关的政府法律法规、对密钥管理的要求、以及用于所涉及网络连接类型和所要求保护等级的加密机制的适当性。

加密机制措施在ISO/IEC 18033中被标准化。块加密是一种常用的加密技术，使用块加密进行加密保护的方式，称作操作模式，在ISO/IEC 10116中标准化。

13.10.3 网络上的数据完整性

在保持完整性重要的环境中，宜考虑使用数字签名和/或消息完整性控制措施来保护流经网络连接的信息。数字签名控制措施能提供与消息鉴别控制措施类似的保护，但也有允许它们启动抗抵赖规程的特性（见13.10.4）。使用数字签名或消息完整性控制措施的决定宜考虑到相关的政府法律法规、相关的公钥基础设施、对密钥管理的要求、用于所涉及的网络连接类型和所要求的保护等级的下层机制的适用性、以及与用于数字签名协议的密钥（被证实在何处相关的）相关的可靠且可信的用户或实体的注册。

消息完整性控制措施，被称作消息鉴别码（或MAC），在ISO/IEC 9797中被标准化。数字签名技术在ISO/IEC 9796和ISO/IEC 14888中被标准化。

13.10.4 抗抵赖

要求确保能够提供实质性证据，证明信息由网络承载过，宜考虑的此类控制措施如下：

- 提供提交确认的通信协议；
- 要求提供原发方地址或标识符并检查此信息存在与否的应用协议；
- 检查发送方和接收方地址格式中语法的有效性及与相关目录中信息的一致性的网关；
- 确认来自网络的交付，并允许确定信息顺序的协议。

重要的是信息的传输或接收，在有争议时能够得到证明，进一步保证宜通过使用标准数字签名方法来提供。信息的发送方，在要求源证据时，宜使用数字签名把信息封装到普通标准。在要求交付证据时，发送方宜请求使用数字签名封装的答复。

更多有关抗抵赖的信息见ISO/IEC 14516和ISO/IEC 13888。

13.10.5 密钥管理

13.10.5.1 概述

作为对所有其他密码服务的基本服务，密钥管理确保所有必需的加密密钥在其完整的生命周期内得到管理，并以安全的方式被使用。

但是在仅有几个连接的非常小的环境中，使用组织的手工规程（例如手工交换对称密钥）就能实现密钥管理。在较大的环境中需要预定义和自动的规程，并且在多数情况下使用公钥/私钥加密技术将带来好处。

公钥/私钥加密技术确实解决对称加密技术的一个主要问题。对称的技术要求相同的密钥在通信双方出现（也被称作共享秘密技术），因此意味着对称加密密钥的传送。由于对称加密密钥本身必须是保密的，为交换密钥就需要一个已经建立起来的安全数据信道。公钥/私钥加密技术通过提供两个密钥并要求其中只有一个被传送到另一个通信实体，来解决这个问题。因为这个密钥不是保密的（被称作公钥）所以它能够通过公共通信信道传送。来被传送的另一个密钥必须被保密处理（被称作私钥）。

然而，某些问题仍然存在，主要是：

- 公钥的可信传输，或者如何准确地获得另一通信实体的公钥；
- 私钥的适当保护。

公钥的传输必须确保接收实体得到发送实体确定发送的公钥。换言之，该传输需要是可信的，否则，窥视公钥传输的潜在攻击者，可能把一个未识别的密钥调换成另一个（有时称之为“中间人攻击”）。

有数个技术可用于检查被传送的公钥的真实性。最显而易见的方式是检查发送和接收的公钥是否相同。该检查通常通过以交互方式比较发送和接收的密钥的散列值（在这种情形中经常被称为“指纹”）来完成。因此密钥的发送和接收实体可能使用单独的信道（例如电话线），重要的是这种信道容许适当鉴别发送和接收实体。（例如，如果接收实体能够通过识别发送方的话音来鉴别他/她）。

然而这种双向的公钥交换方式仅在涉及少量通信实体的情况下才可行，不能按比例增加。这个问题能够通过引入基础设施来提供每个实体的公钥并证明所提供公钥的真实性加以解决。此类基础设施，通常称为PKI，由各种组件组成。新实体的加入由注册机构注册，该机构的主要任务是验证实体的适当身份。然后认证机构基于此注册，能够证实的公钥，并且通常提供目录服务使得被证实的公钥（通常被称为“证书”）对所有被指定使用系统的实体是可用的，在技术上，一个证书包括一组良好定义的实体属性（例子是用户实体的名字和电子邮件地址）和实体公钥，并且此信息的真实性由认证机构对此信息的数字签名来保证。

对于使用由PKI提供和管理的公钥的所有加密服务，由于其安全依赖于这些密钥的真实性，所以PKI具有非常高的安全要求。例如，若攻击者对认证机构进行访问，他/她可能会颁发使冒充实体成为可能的证书。

由于功能性原因，大多数PKI需要被附加到网络上，因此要特别注意适当的网络安全控制，以使其能够满足PKI的高安全性要求。在很多情况下这些安全控制包括为核心PKI组件建立专用网络，并且通过适当的安全网关或防火墙保护此网络。

关于私钥的适当保护，这种保护对于安全性也是至关重要的，因为如果攻击者访问实体的私钥，他/她就有冒充该实体的可能。通常，依赖于具体组织、环境或应用的安全要求，若干解决方案已经可用。

最简单的解决方案是保护私钥，其方式是以对称加密形式将它保存在实体的系统上，稍好一点的方式是将其保存在可移动介质上。然后该实体通常键入一个口令（它构造对称加密密钥）来为私钥解锁，并把它提供给服务和应用进一步的使用。此解决方案具有的显著优点，是其完全基于软件的，因此能在大多数环境中相对容易地实施。然而，从安全的角度看，它存在主要缺点，因为保护：

- 依赖于所选择口令的质量；

- 依赖于实体所使用的系统的完整性。若一个攻击者获得此系统的控制权，他/她可在处理加密函数期间复制以未加密的形式存储在内存中的私有密钥，或者他/她可通过获得实体的口令和加密形式的公钥，得到相同的结果。

基于智能卡的解决方案可用于克服这些缺点。它们为私钥访问提供双因素鉴别（通常拥有智能卡且知道口令或PIN以将其解锁）。其结构确定保证私钥决不会离开智能卡，这意味着所有要求私钥核心加密计算在智能卡本身上处理。作为一个显著的优点，这种解决方案，即使是在被实体使用的系统的完整性受到损害时也保护私钥。基于智能卡的解决方案，其主要缺点是需要分配和整合与特定智能卡相关的实体及其系统硬件。虽然该领域有技术标准可用，但这通常是一个相当复杂和成本密集的过程。

要强调的是，本章只提供密钥管理主题的简要概述。有关该主题和PKI之类的相关主题或有关身份管理主题的更多信息，宜参照其他文件和标准，诸如：

- GB/T 17901-密钥管理；
- GB/T 16264.8-目录：公钥和属性证书框架；
- ISO 11166-2-银行业务-借助非对称算法的密钥管理；
- ISO IS 11568-银行业务-密钥管理零售；
- ISO IS 11649-银行业务-多中心密钥管理；
- ISO IS 13492-零售密钥管理数据元素；
- ISO IS 21118-银行公钥基础设施。

13.10.5.2 安全性考量

在密钥管理环境中，特别是在使用或实施PKI服务时，要进行若干安全性考量。

这些考量包括的主题有：

- 范围和用法-PKI的预期用法对实际安全具有重大影响。例如，使用已颁发的证书确实主要影响PKI的安全要求；

- 策略-所提供的PKI服务及其目的、PKI中所实施的保护的等级，以及交互过程需要在认证策略（CP）和认证业务规则声明（CPS）中适当文件化；

- 实施问题-组织可选择在内部实施PKI（“内委PKI”）或可能决定只购买PKI服务（“外包PKI”），或者可以选择实现两者的结合（例如只购买核心认证服务，但在本地实施其他服务，如漫游目录）；

- 特定功能要求，例如对于漫游用户-很多功能要求需要制定特定安全控制措施。一个例子是如何为漫游用户提供私有密钥及访问证书的保护；因此解决方案之一是使用智能卡（见下面）；

- 智能卡使用-智能卡可用于满足较高的安全要求（例如前面13.10.5.1提到的）或解决漫游用户环境中的问题。但是，使用智能卡确实要求有很多的进一步的考量，如智能卡的生命周期过程、智能卡的物理分配和处理、故障恢复过程（例如当用户忘记他/她的智能卡）、所使用的读卡器的硬件与客户端系统上的适当整合软件的安全问题；

——操作问题，例如根认证机构的在线/离线操作-特定的操作措施能够用来满足特定的安全要求。例如，在不使用根认证机构的服务时让其处于离线状态，并结合适当的物理保护，这种方法可用于为系统最敏感部分提供较高级别的保护。

13.11 业务持续性管理

重要的是，一旦灾难性事件发生，就绪的控制措施通过在适当时间框架内，提供恢复被中断业务每一部分的能力来确保进行中的业务功能。因此，组织宜适当安排业务持续性管理计划，其过程涵盖所有业务持续性阶段-建立业务恢复优先级、时间安排和要求（由业务影响分析评审支持）、业务持续性策略的构想、业务持续性计划的产生、业务持续性计划的测试，确保所有员工的业务持续性意识，持续的业务持续性计划的维护以及降低风险。只有遵循所有阶段，才能确保：

- 所要求的业务优先级和时间安排符合业务需求；
- 被识别的推荐业务持续性策略选项与优先级和时间安排相当；
- 正确且必要的计划与设施得到适当安排，并被测试，包括信息、业务流程、信息系统和服务、语音和数据通信、人员和物理设施。

对业务持续性管理的指南作为一个整体，包括适当业务持续性策略和相关计划的制订及随后的测试，能够从GB/T 22081和ISO/IEC 13335-2中得到。

从联网的角度看，网络连接的维护、有足够能力的替代性连接的实现、有害事态发生后连接的恢复，都必须得到处理。这些方面和要求宜基于随时间推移连接对业务功能重要性和损害发生时所产生的不利业务影响。损害发生时连通性能够给组织提供很多优势，同时，根据灵活性和利用创造性方法的能力，它们也能够表示脆弱点和“单点故障”，这些可能对组织有重大的破坏性影响。

14 安全控制措施的实施和运行

一旦技术安全体系结构安全控制措施被识别、文档化和达成协议，就宜实施网络安全控制措施。在允许联网操作开始之前，其实施宜被评审、测试，且任何已识别的安全缺陷宜得到处理（见第15章）。然后，一旦安全已被“签核”，宜开始有效操作。随着时间的推移，如果发生了显著变化，就宜进行进一步的实施评审（见第15章）。

15 对实施的监视和评审

如第14章所述，宜评审首个实施是否符合下面文件中指定的文档化的技术安全体系结构和所要求的安全控制措施：

- 技术安全体系结构；
- 网络安全策略；
- 相关安全操作规程（SecOP）；
- 安全网关服务访问（安全）策略；
- 业务持续性计划；
- 连接的相关安全条件。

符合性评审宜在有效操作之前完成。当所有的缺陷都已经由高级管理人员识别、修复、并签核时评审才完成。后有效操作、持续监视和评审活动也宜进行，尤其要在与业务需求、技术、安全解决方案等相关重大变化相关的主要新版本颁布之前进行，否则每年进行一次。

要强调的是，这宜包括针对认可标准进行的安全性测试，使用安全测试策略及预先制订的相关计划，这些计划严密地规划，要进行哪些测试、使用什么、何地、何时进行。通常这宜包括一个脆弱性扫描和

渗透测试的组合。在任何此类测试开始之前，宜检查测试以确保该测试将以一种完全符合相关法律法规的方式进行。当进行这项检查时，不应忘记网络可能不只是限定于一个国家之内-它可能会分布在具有不同法律的国家中。测试之后，其报告宜指出所遇到的脆弱性的详情以及所要求的修正，以及处于什么优先级，其附录证实所有给定的修正已被应用。此类报告宜由高级管理人员签核。

参 考 文 献

- [1] ISO/IEC TR 14516:2002, Information technology — Security techniques — Guidelines for the use and management of Trusted Third Party services
- [2] ISO/IEC 13888 (all parts), IT security techniques — Non-repudiation
- [3] ISO/IEC 7498-1:1994, Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model
- [4] GB/T 9387.2-1995 信息处理系统 开放系统互连 基本参考模型 第2部分：安全体系结构 (ISO/IEC 7498-2:1989, IDT)
- [5] GB/T 9387.3-2008 信息技术 开放系统互连 基本参考模型 第3部分：命名与编址 (ISO/IEC 7498-3:1997, IDT)
- [6] GB T 9387.4-1996 信息处理系统 开放系统互连 基本参考模型 第4部分：管理框架 (ISO/IEC 7498-4:1989, IDT)
- [7] ISO/IEC 27005, Information technology — Information security risk management
- [8] 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)
- [9] ITU-T X.810 | ISO/IEC 10181-1:1996, Information technology — Open Systems Interconnection — Security frameworks for open systems: Overview
- [10] IETF Site Security Handbook (RFC 2196), September 1997
- [11] IETF IP Security Document Roadmap (RFC 2411), November 1998
- [12] IETF Security Architecture for the Internet Protocol (RFC 2401), November 1998
- [13] IETF Address Allocation for Private Internets (RFC 1918), February 1996
- [14] IETF SNMP Security Protocols (RFC 1352), July 1992
- [15] IETF Internet Security Glossary (RFC 2828), May 2000
<http://www.ietf.org/rfc/rfc2828.txt>
- [16] NIST Special Publications 800 series on Computer Security, including:
—NIST Special Publication 800-10: Keeping Your Site Comfortably Secure: An Introduction to Firewalls