[a] ICS 35.040
[b] L80

中华人民共和国国家标准

GB/T 25068:1—20XX/ISO/IEC 27033-1:2015
代替 GB/T 25068:1-2010

信息技术 安全技术 网络安全 第1部分：综述和概念

Information technology — Security techniques — Network security —Part 1:Overview and concepts

（ISO/IEC 27033-1:2015，IDT）

（报批稿）

（本稿完成时间：2019 年 10 月 18 日）

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

目　　次

前　言

GB/T 25068《信息技术 安全技术 网络安全》由以下几个部分组成：

——第1部分：综述和概念；

——第2部分：网络安全设计和实现指南；

——第3部分：参考网络场景——威胁、设计技术和控制要素；

——第4部分：使用安全网关的网间通信安全保护；

——第5部分：使用虚拟专用网的跨网通信安全保护；

——第6部分：无线IP网络访问安全保护

本部分是GB/T 25068的第1部分。

注：GB/T 25068可能还会有其它部分。这些部分可能覆盖的主题包括局域网、城域网、宽带网、网页寄存、互联网电子邮件、接入第三方组织的路由。这些部分主要涉及威胁、设计技术和控制等问题。

本部分按照GB/T 1.1《标准化工作导则 第1部分：标准的结构和编写规则》、GB/T 20000.2《标准化工作指南 第2部分：采用国际标准》给出的规则起草。

本部分代替GB/T 25068.1—2010《信息技术 安全技术 IT网络安全 第1部分：网络安全管理》。GB/T 25068.1—2010转制于ISO/IEC18028-1:2006，ISO/IEC 18028-1:2006已经被ISO/IEC 27033-1:2015取代，并做了技术上的修订，本标准等同采用ISO/IEC27033-1:2015，对GB/T 25068.1—2010进行修订。与GB/T 25068.1—2010相比，主要技术变化如下：

——本部分名称由《信息技术 安全技术 IT网络安全 第1部分：信息技术 安全技术 IT网络安全 第1部分：网络安全管理》修改为《信息技术 安全技术 网络安全 第1部分：综述和概念》；

——对标准文本结构进行了调整，由原来的15章调整为现在的14章。对每个章节的名称及内容进行了重新归纳和修改，增加了“支持控制措施”、“参考网络场景—威胁、设计技术和控制要素”、“开发和测试安全解决方案”等章节，删除了“目标”、“公共基础设施中基于密码的服务”等章节；

——第2章中删除了对GB/T 22081—2008、GB/T 25068.2—2012、GB/T 25068.3—2010等标准的注日期的引用，增加了对GB/T 22080、GB/T 22081、GB/T 31722等标准的不注日期的引用；

——第3章术语中删除了“安全维”、“滥发”等术语及定义，增加了“架构”、“信息安全策略”等术语及定义；

——第4章删除了“Telnet”、“TETRA”等缩略语，增加了“BPL”“CA”、“DPNSS”等缩略语；

——删除了GB/T 25068.1—2010中表1-4，对GB/T 25068.1—2010中的图1-4进行了重新编辑和排序，增加了图5、图6；

——增加了附录A和附录B。

本部分使用翻译法等同采用ISO/IEC 27033-1:2015《信息安全 安全技术 网络安全 第1部分：综述和概念》。

本部分还做了下列编辑性修改：

——按照汉语习惯对一些编排格式进行了修改；

——将一些适用于国际标准的表述改为适用于我国标准的表述。

本部分由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本部分起草单位：黑龙江省网络空间研究中心、中国电子技术标准化研究所、西安西电捷通无线网络通信股份有限公司、北京安天电子设备有限公司、杭州安恒信息技术有限公司。

本部分主要起草人：方舟、曲家兴、马超、谷俊涛、树彬、刘佳、李锐、宋雪、马遥、王大萌、吴琼、姜国春、冯亚娜、张弘、司丹。

本部分所代替的历史版本发布情况为：

——GB/T 25068.1—2012。

引　　言

当前，商业和政府组织大多数都通过网络连接他们的信息系统（如图1），其中，网络连接类型可能包括如下一个或多个：

——组织内部的网络；

——不同组织间的网络；

——组织和公众之间的网络。

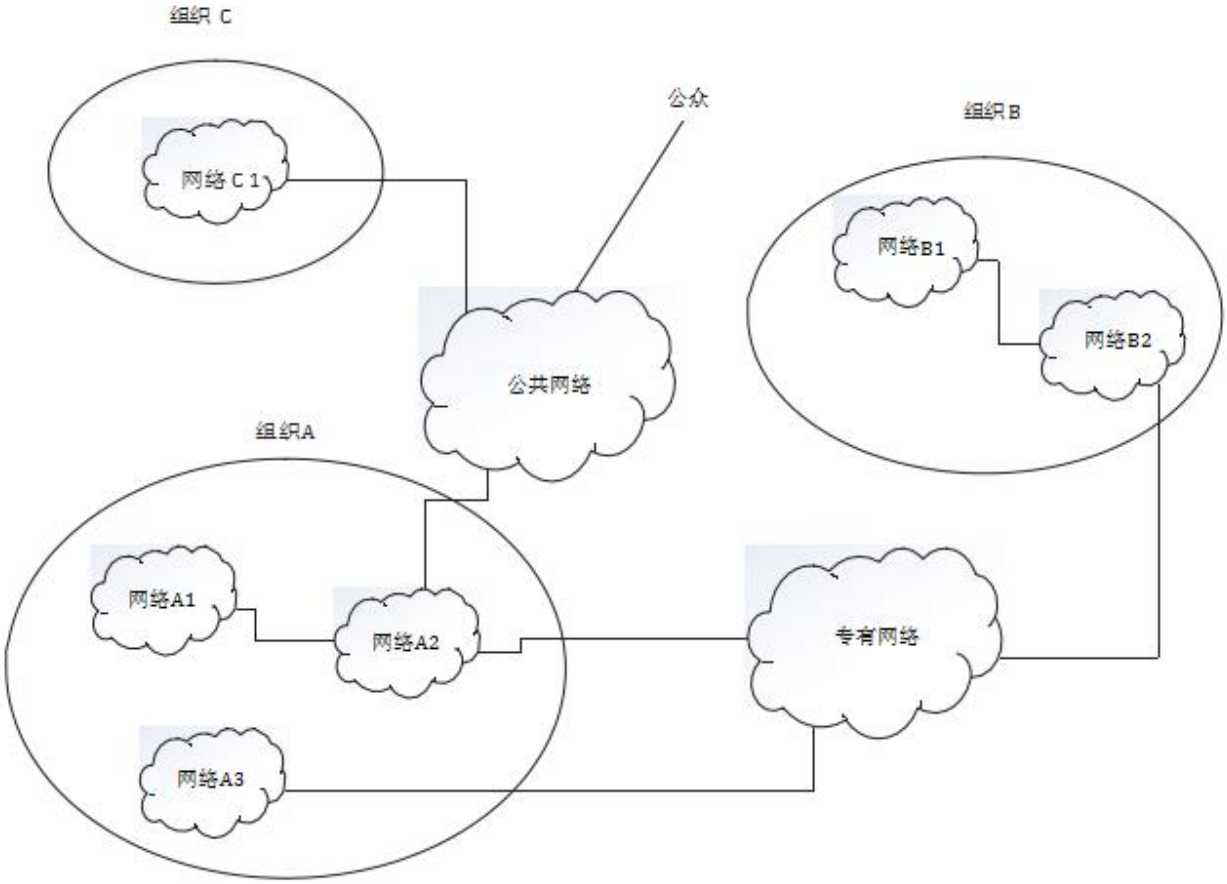

图1 典型的网络类型及连接方式

此外，快速发展的网络技术（特别是通过互联网发展起来网络技术）提供了重要商业机会，越来越多的组织机构开展全球性的电子商务以提供在线公共服务。这些商业机会不仅实现了将互联网作为简单的连接媒介以提供低成本的数据通信，也实现了由互联网服务提供商（ISP）提供更复杂的服务。这也就意味着，通过在电路的每一端使用相对低成本的本地连接，可以完整实现在线电子交易和服务交付系统，例如采用基于Web的应用及服务技术。此外，新的技术（包括数据、语音和视频的集成）为远程工作提供了可能（也称为“远程工作”或“远程办公”），使员工能够在一段时间内离开他们的工作地点，还能通过远程设备访问组织网络、社区网络，以及相关业务支持信息和服务。

这种环境有利于获得重大商业利益，但又存在新的安全风险。随着组织越来越依赖于信息和相关网络，那么信息保密性、完整性及可用性的缺失将会对开展业务造成极大负面影响。因此，有必要适当保护网络、信息系统和信息的安全。换句话说，实施和维护充分的网络安全对任何组织业务稳定运行来说都是至关重要的。

在这种情况下，电信和信息技术产业正在寻求成本效益均衡的安全解决方案，旨在保护网络免受恶意攻击和无意的不正当行为，满足信息和服务保密性、完整性和可用性的业务要求。适当的网络安全对于确保服务计费和使用信息的准确性是必不可少的。产品的安全能力对整体网络安全（包括应用和服务）至关重要，然而，随着更多解决方案将产品组合起来形成的一个整体，产品间是否具备互操作性将决定解决方案成功与否。安全性是每个产品或服务的关注点，它必须依靠提高整体安全解决方案的安全能力进行开发。

本标准的目的是为信息系统网络的管理、运行、使用及互联互通提供安全方面的详细指导。组织内负责信息安全，特别是网络安全的人员应能够采纳本标准以满足其特定需求。其主要目标如下。

——GB/T 25068.1，定义和描述与网络安全相关的概念并提供管理指导。包括网络安全概述及相关定义，指导网络安全风险识别和分析，进而定义网络安全需求。它还介绍了如何达成优质的技术安全架构，以及与典型网络场景和网络“技术”领域相关的风险、设计和控制等方面（GB/T 25068其余部分将详细介绍）。

——GB/T 25068.2，定义了组织应该如何规划、设计、实现高质量的网络安全体系，以确保网络安全适合相应的业务环境。可借助模型框架（本部分标准利用模型框架来描述一类技术安全架构、设计的结构和内部运行机制），使用一致的方法，进行网络安全规划、设计与实现。同时，本部分标准也适用于参与到网络安全规划、设计和实施网络安全架构的人员参考（例如，网络架构师、设计人员、网络管理员和网络安全主管）。

——GB/T 25068.3，定义与典型的网络场景相关的具体风险、设计技术和控制要素，与所有参与网络安全架构方面规划、设计和实施的人员（例如，网络架构师、设计人员、网络管理员和网络安全主管有关）。

——GB/T 25068.4，定义使用安全网关保护的网络之间信息流的具体风险、设计技术和控制要素。与所有参与安全网关的详细规划、设计和实施的人员（例如，网络架构师、设计人员、网络管理员和网络安全主管）有关。

——GB/T 25068.5，定义使用虚拟专用网络建立安全连接的具体风险、设计技术和控制要素。这与所有参与VPN安全性详细规划、设计和实施的人员（例如，网络架构师、设计人员、网络管理员和网络安全主管）有关。

——GB/T 25068.6，定义保护IP无线网络的具体风险、设计技术和控制要素。与参与详细规划、设计和实施无线网络安全的人员（例如，网络架构师、设计人员、网络管理员和网络安全主管）有关。

需要强调的是，本标准在国家标准GB/T 22081的基础上，进一步对网络安全控制提供了详细的实施指导。

应注意的是，本标准不是法规和立法要求的参考或规范性文件。因为网络安全取决于业务类型等因素，所以本标准仅强调这些影响的重要性而不做具体说明。

除非另做说明，否则GB/T 25068本部分标准所参考的指南仅适用于当前及规划的“网络”或“此网络”。

信息技术 安全技术 网络安全
第1部分：综述和概念

1 范围

本部分规定了网络安全概述和相关定义。定义和描述与网络安全相关的概念，并提供有关网络安全的管理指导。（本部分中网络安全不仅适用于通过通信链路传送的信息安全，还适用于设备安全，以及与设备、应用（服务）和最终用户相关的管理活动的安全）。

本部分的使用者包括拥有、运行或使用网络的任何人，包括高级管理人员和其他非技术管理人员或用户，以及对信息安全及网络安全、网络操作负有特定责任的或对组织的整体安全计划和安全策略制定负责的经理和管理员。此外，还包括参与网络安全架构方面的规划、设计和实施的所有人。

本部分还包括以下内容：

——提供了识别和分析网络安全风险的指南，并基于上述分析定义网络安全需求；

——提供了支持网络技术安全架构和相关技术控制的综述，以及不仅适用于网络的技术和非技术控制；

——介绍了如何实现高质量的网络技术安全架构，以及与典型网络场景和网络“技术”领域相关的风险、设计和控制要素（在GB/T 25068的其他部分中详细论述），简述了与实施和运行网络安全控制有关的问题，以及对其实施进行持续监督和评审的相关问题。

本部分提供了GB/T 25068标准的概述和对其他部分的指引。

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（包括所有修正）适用于本文件。

GB/T 9387（所有部分），信息技术 开放系统互连 基本参考模型：命名与编址（ISO/IEC 7498，IDT）

GB/T 22080，信息技术 安全技术 信息安全管理体系要求（ISO/IEC 27001，IDT）

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

GB/T 31722，信息技术 安全技术 信息安全风险管理（ISO/IEC 27005，IDT）

3 术语和定义

为实现本文件的目的，GB/T 9387（所有部分）、GB/T 29246、GB/T 22080、GB/T 22081、GB/T 31722给出如下适用的术语和定义。

注：以下条款及定义同样适用于本系列其他部分。

3.1

警报 alert

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

3.2

架构 architecture

构成系统的各组成部分及其相互关系，以及该系统与环境的关系，还包括指导其设计和演进的基本原则。

[见GB/T 22032—2008， 4.5]

3.3

攻击者 attacker

故意利用技术和非技术安全控制的脆弱性，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为目的的任何人。

3.4

审计日志 audit logging

以评审、分析和持续监视为目的的相关信息安全事态的数据记录。

3.5

审计工具 audit tools

一种辅助分析审计日志内容的自动化工具。

3.6

认证机构（CA）certification authority

被一个或多个用户信任的机构，该机构创建和分配公钥证书。

注1：需注意的是，认证机构可以创建用户密钥。

注2：在此过程中认证机构的作用是保证被授予唯一证书人的身份真实性。通常，这表示身份核查机关已与提供被核查人身份确认资料的机构达成协议。认证机构是信息安全和电子商务的一个重要组成部分，因为它们保证了交换信息双方的身份真实性。

3.7

信息安全策略 corporate information security policy

根据业务要求和相关法律法规描述管理方向和支持信息安全的文件。

注：该文件描述了整个组织必须遵循的高级信息安全需求。

3.8

非军事区（DMZ） demilitarized zone

介于网络之间作为“中立区”的边界网络（也称为屏蔽子网）。

3.9

拒绝服务（DoS）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，并导致授权用户可用性受损。

3.10

外联网 extranet

是对组织内联网的扩展，特别是通过公共网络提供对其内联网的有限访问，以支持组织与组织之间、组织与个人之间共享资源。

注：例如，可以允许组织的客户对组织内部网络的某些部分进行访问，从而创建外联网，但是从安全的角度来看，不能认为这些客户是“可信的”。

3.11

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。

3.12

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。

3.13

集线器 hub

一种工作在开放系统互联（OSI）参考模型第1层的网络设备。

注：网络集线器不是智能设备，它只为联网系统或设备提供物理连接点。

3.14

互联网 the Internet

在公共领域中由相互连接的网络组成的全球系统。

3.15

互联网络 internet

相互连接的网络集合。

3.16

内联网 intranet

支持组织成员利用互联网络协议和网络连接，安全地分享组织的部分信息和操作的私有计算机网络，简称内网。

3.17

入侵 intrusion

对网络或联网系统的未授权访问，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。

3.18

入侵检测 intrusion detection

检测入侵的正式流程。通过分析异常特征以及已被利用的脆弱性类型和利用方式，发现入侵的时间和方式。

[见GB/T 28454，2.15]

3.19

入侵检测系统（IDS）intrusion detection system

用于识别尝试、正在进行或已经发生的入侵，并可能对信息系统和网络中的入侵做出响应的技术系统。

[见GB/T 28454，2.15]

3.20

入侵防御 intrusion prevention

积极应对以防止入侵的正规过程。

3.21

入侵防御系统（IPS）intrusion prevention system

入侵检测系统基础上的一种扩展，专门设计用来提供入侵主动响应能力的技术系统。

[见GB/T 28454，2.15]

3.22

恶意软件 malware

被专门设计用于损坏或中断系统、破坏保密性、完整性和可用性的软件。

注：病毒和特洛伊木马都是恶意软件。

3.23

多协议标签交换（MPLS） multi protocol label switching

一种为网间路由而开发的技术。该技术通过为每个数据路径或数据流分配标签来实现连接交换，通常用作一般路由协议的底层或补充。

注：标签切换可以作为建立隧道的一种方法。

3.24

网络日常管理 network administration

对网络业务流程、资产的日常运行和管理。

3.25

网络分析器 network analyzer

用于观察和分析网络中信息流的软件或设备。

注：在进行信息流分析之前，应该以特定的方式收集信息，例如使用网络嗅探器。

3.26

网元 network element

与网络连接的信息系统。

3.27

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。

3.28

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的过程，包括日志审计、警报和分析。

3.29

网络安全策略 network security policy

组织为使用网络资源所制定的一组声明、规则和措施，以保护网络基础设施和服务。

3.30

网络嗅探器 network sniffer

用于捕获网络中信息流的软件或设备。

3.31

端口 port

连接的端点。

注：在互联网协议的语境下，端口是TCP（传输控制协议）连接或UDP（用户数据报协议）消息的逻辑信道端点。基于TCP或UDP的应用协议，通常已分配默认端口号，如为HTTP（超文本传输协议）的端口号是80。

3.32

远程访问 remote access

从另一网络或从一个终端设备访问网络资源的过程，这种访问通过物理的或逻辑的方式且不会永久连接所访问的资源。

3.33

远程用户 remote user

不在网络资源所在地并使用该网络资源的用户。

3.34

路由器 router

基于路由协议机制和算法，通过选择路径或路由，来建立和控制不同网络之间数据流的网络设备。

注1：网络可以自主选择不同的协议。

注2：路由信息被保存在路由表内。

3.35

安全域 security domain

遵从共同安全策略的资产和资源的集合。

3.36

安全网关 security gateway

在网络或各子网之间，或在不同安全域内的软件应用之间，一种旨在按照给定的安全策略来保护网络的连接点。

3.37

垃圾邮件 spam

可能携带恶意内容或欺诈消息的非请求电子邮件。

3.38

欺骗 spoofing

假冒成合法资源或用户的行为。

3.39

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，其中的交换技术通常在OSI参考模型的第2层或第3层实现。

3.40

隧道 tunnel

在现有网络基础设施上建立的联网设备之间的数据路径。

注：可通过使用诸如协议封装、标签交换或虚电路等技术建立隧道。

3.41

虚拟本地网络 virtual local area network

基于物理网络创建的独立逻辑网络。

4 缩略语

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 非对称数字用户线路（asymmetric digital subscriber line）
AES 高级加密标准（advanced encryption standard）
ATM 异步传输模式（asynchronous transfer mode）
BPL 宽带电力线路（broadband over power line）
CA 认证机构（certification authority）
CDPD 蜂窝数字分组数据（cellular digital packet data）
CDMA 码分多址（code division multiple access）
CLID 用户呼叫识别器（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）
DPNSS 数字专网信令系统（digital private network signaling system）
DoS 拒绝服务（denial of service）
DSL 数字用户线路（digital subscriber line）
EDGE 增强型GSM演进数据速率（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）
FiOS 光纤服务（fiber optic service）
FTP 文件传输协议（file transfer protocol）
FTTH 光纤入户（fiber to the home）
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 基于主机的入侵检测系统（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）
IPS 入侵防御系统（intrusion prevention system）
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 swithing）
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）
NTP 网络时间协议（network time protocol）
OOB 带外（out of band）
PABX 专用程控（电话）交换机（private automated branch (telephone) exchange）
PC 个人电脑（personal computer）

PDA 个人数据助理（personal data assistant）
PIN 个人识别号（personal identification number）
PKI 公钥基础设施（public key infrastructure）
PSTN 公共交换电话网（public switched telephone network）
QoS 服务质量（quality of service）
RAID 冗余磁盘阵列（redundant array of inexpensive disks）
RAS 远程访问服务（remote access service）
RTP 实时协议（real time protocol）
SDSL 对称数字用户线路（symmetric digital subscriber line）
SecOPs 安全操作规程（security operating procedures）
SIM 用户身份识别卡（subscriber identity module）
SNMP 简单网络管理协议（simple network management protocol）
SPIT 通过 IP 电话的垃圾呼叫（spam over IP telephony）
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）
TKIP 临时密钥完整性协议（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 电话（voice over IP）
VLAN 虚拟局域网（virtual local area network）
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 有线等效隐私协议（wired equivalent privacy）
WLAN 无线局域网（wireless local area network）
WORM 写一次读多次（write once read many）
WPA Wi-Fi 访问保护（Wi-Fi protected access）

5 文档结构

GB/T 25068 标准的结构或称“路线图”，如图 2 所示；

在图 2 中，实线表示 GB/T 25068 中各部分的自然层次。虚线表示：（a）第 1 部分与第 3、4、5、6 部分之间可能存在引用有关安全风险方面信息的关系；（b）第 2 部分与第 3、4、5、6 部分可能存在引用有关设计技术和控制要素信息的关系。此外，第 3 部分中的有关内容将在第 4、5、6 部分进行详细叙述，因此在第 3 部分中不做赘述。

因此，对于新建网络的任何组织或准备对现有网络进行重大评审的组织，应依次采用第 1、2 部分的内容，必要时参阅第 3 到 6 部分中涉及到的安全风险、设计技术和控制要素的内容。

如果一个组织计划部署一个新的网络环境，需使用 IP 聚合、安全网关和无线网络，以及网络托管和互联网（例如针对电子邮件和输出在线访问）。

在依据 GB/T 25068.1 中描述的过程来确定新网络环境的安全风险时，组织应同时考虑 GB/T 25068 其他相关部分信息的风险。这些部分定义了特殊安全风险（包括设计技术和控制要素），其内容涉及 IP 聚合、安全网关和使用无线网络，以及网络托管和互联网的使用（如电子邮件和输出在线访问）。

在依据 GB/T 25068.2 确定网络技术安全架构需求时，组织应同时考虑 GB/T 25068 其他相关部分的设计技术和控制要素的信息。这些部分定义了具体设计技术和控制要素的信息（连同安全风险），其内容涉及 IP 聚合、安全网关和无线网络的使用，以及网页寄存服务和互联网的使用（如电子邮件和在线访问）。

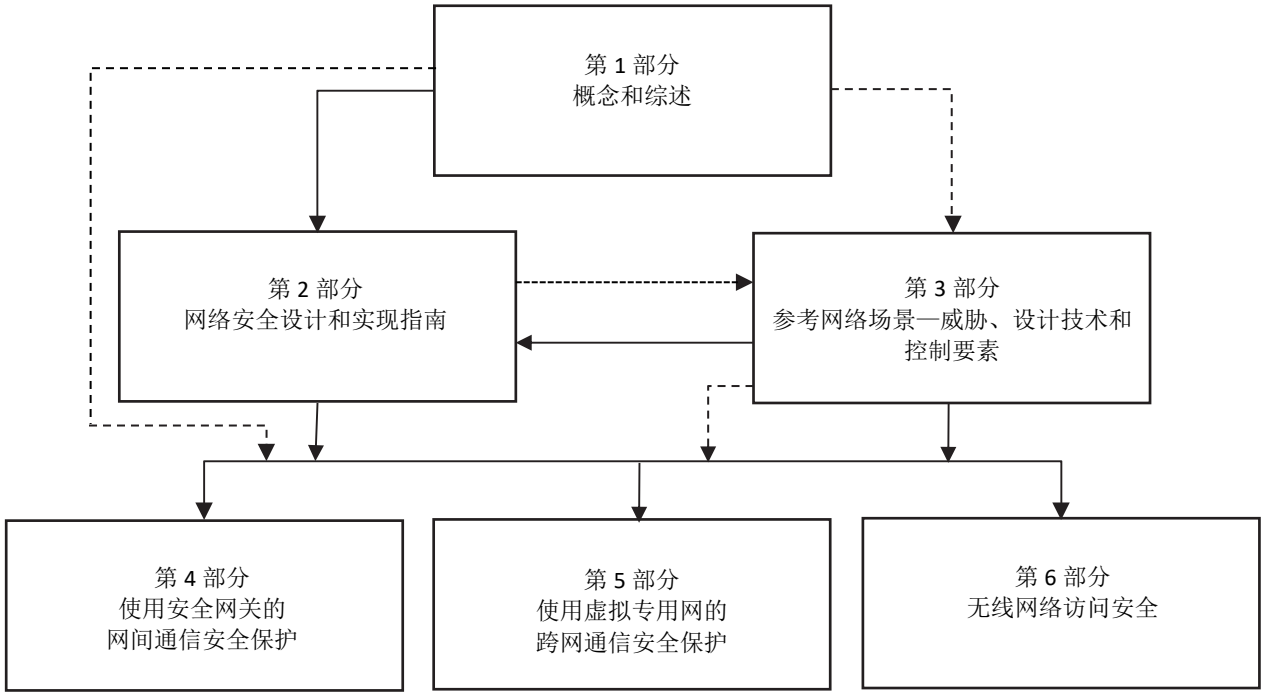

图 2 GB/T 25068“路线图”

本部分结构包括：

——网络安全方法概述（见第 6 章）；

——识别网络相关风险和准备识别安全控制的过程的总结，即建立网络安全需求（见第 7 章）；

——关于支持网络安全技术架构及其相关技术控制的概述，以及不仅适用于网络的其他控制；（见第 8 章），相关内容请参考 GB/T 22080、GB/T 22081、GB/T 31722 ；

——介绍如何运用辅助模型框架，通过一致性方法规划和设计网络安全，以实现高质量的技术安全架构，并确保其适用于组织的业务环境（即 GB/T 25068.2 中的内容介绍，见第 9 章）；

——介绍参考网络场景相关的特定风险、设计、技术和控制要素（即 GB/T 25068.3 内容的介绍）（见第 10 章）；

——介绍网络技术层面特定的风险、设计、技术和控制要素（即 GB/T 25068.4-GB/T 25068.6 和未来其他部分的介绍）（见第 11 章）；

——介绍开发、实施和测试网络安全解决方案（见第 12 章），运行网络安全解决方案（见第 13 章）以及持续开展网络安全实施监视和评审相关的问题（见第 14 章）；

——以表格形式给出了GB/T 22080、GB/T 22081中有关网络安全控制条款和GB/T 25068.1中子条款之间交叉引用关系，参见附录A。

6 概述

6.1 背景

目前，许多组织中常见的网络环境如图3所示（图3仅为本章的示意图）。

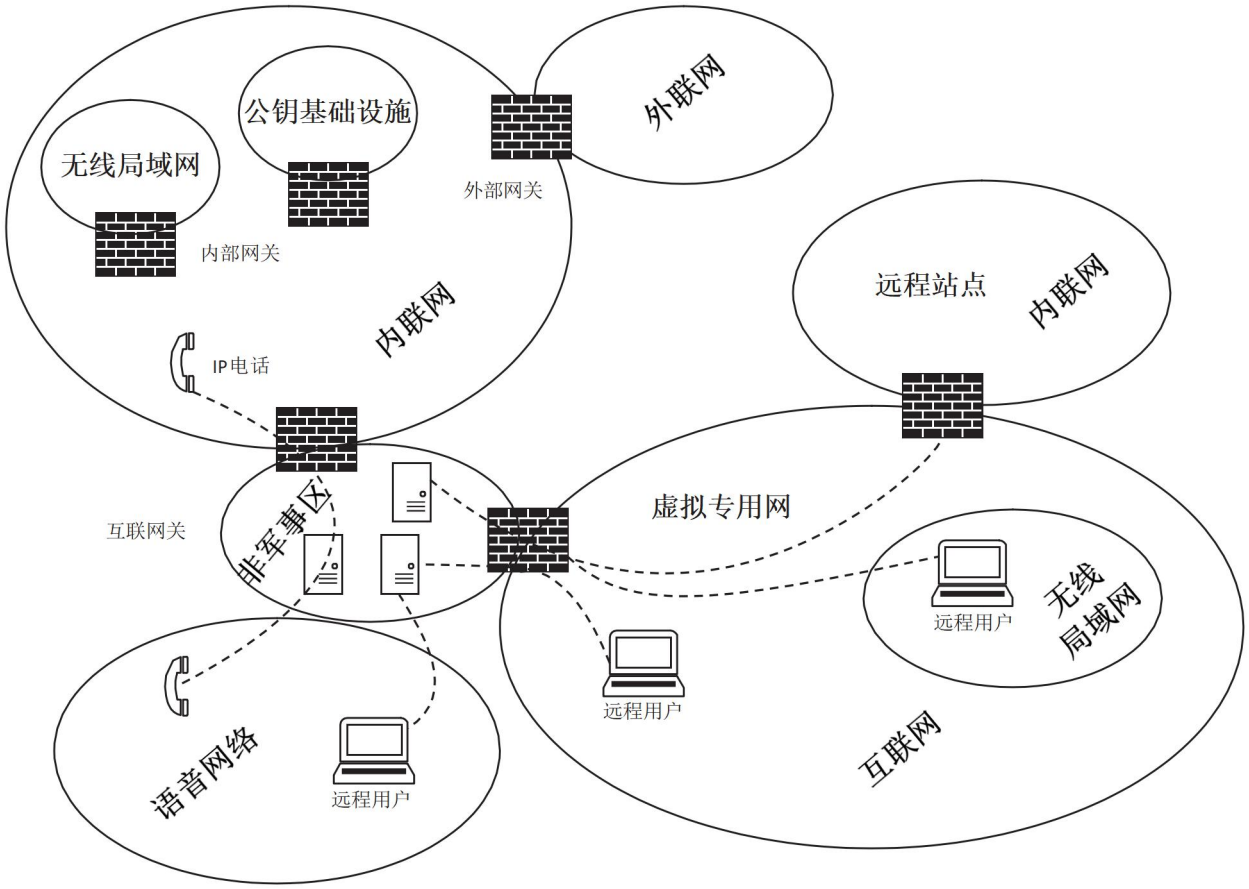

图 3 典型网络环境

内联网指的是组织内部依赖和维护的网络。通常情况下，只有该组织的内部工作人员才有权直接物理接入。由于网络位于该组织拥有的场所内，因此可以实现一定程度的物理保护。在大多数情况下，内联网由于采用的技术和安全需求不同，不能一概而论，但往往有些基础设施需要的保护级别比内联网预设的要高。此类基础设施，例如公钥基础设施（PKI）环境的主要部分，可在内联网的专属分区中运行。另一方面，某些技术（例如无线局域网基础设施）可能需要某种程度的隔离和鉴别，因为它们引入了额外的风险。对于这两种情况，可以用内部安全网关来进行分段。

多数组织的业务需求都需要与外部合作伙伴和其他组织进行通信和数据交换。通常，与最重要的业务伙伴的连接方式是直接将内联网扩展到业务伙伴组织的网络，外联网这个术语被普遍用于这种扩展。

在大多数情况下，由于被连接的合作伙伴组织中的信任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而引入的风险。

公共网络中最常见的是互联网，目前被进一步用于向合作伙伴、客户和一般公众提供性价比最高的通信和数据交换的设施，并且提供各种形式的内网的扩展。由于公共网络（特别是互联网）的低信任级别，需要复杂的安全网关来帮助应对所带来的风险。这些安全网关包括特定组件，以满足各种形式的内联网扩展需求，以及合作伙伴和客户对网络连接的需求。

远程用户可以通过虚拟专用网（VPN）技术连接，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，远程用户可以使用电话网络来建立与远程接入服务器的直接拨号连接。远程接入服务器通常位于互联网防火墙的非军事区（DMZ）环境内。

当一个组织决定使用 IP 电话（VoIP）技术来实现内部电话网络时，通常还需要在电话网络之间合理地部署安全网关。

新网络环境提供的商业机会应与新技术带来的风险相平衡。例如，互联网具有许多技术特征，从安全角度来看，它们应引起关注，因为最初设计时，优先考虑到的是具有弹性而不是安全性，并且许多常用的底层协议天生是不安全的。全球环境中，许多人具有访问底层机制和协议的能力、知识和倾向，并制造网络安全事故，包括未授权的访问，甚至于全面的破坏性拒绝服务。

6.2 网络安全规划和管理

当考虑网络连接时，组织中所有负责网络连接的工作人员应该清楚业务需求和效益、相关的安全风险以及相关的技术安全架构、设计技术和安全控制区域。在考虑网络连接、识别技术安全架构、设计技术和潜在安全控制区域，最终选择、设计、实施和维护安全网络的过程中，这些业务需求和效益将会对所采取的诸多决策和行动造成影响。

实现和维护所需的网络安全的总体过程可以总结如下：

a) 确定范围及情境，然后评估安全风险：

——收集有关当前及规划的网络环境的信息。

——评审企业信息安全策略。这些策略中的网络安全相关风险一般是高等级的，但无论被评估的网络安全风险等级如何，都需要实施网络安全控制。

——需知此策略还应包含组织对遵守法律法规的立场，包括：1.有关监管机构或立法机构（包括政府机构）规定的与网络连接相关的监管和立法安全要求；2.需要在网络上存储或传输的敏感信息。

——收集和评审关于当前或规划的网络（架构、应用、服务、连接类型和其他特性）的信息，确定对于风险的识别和评估，以及网络技术安全架构、设计而言，哪些信息是可能产生影响的。

——收集其他信息，以便能够评估潜在的负面业务影响、威胁和脆弱性（包括通过网络连接传输的对业务运营有价值的信息、可能通过未经授权的方式而获取的信息，以及提供的服务的一切信息）。

——识别和评估网络安全风险，以及可能的潜在控制区域。

——进行网络安全风险评估和管理评审，包括使用与所需网络情景和“技术”主题相关的风险信息来定义安全需求（见第10和11章）（1.评估潜在违反相关监管或立法机构（包括政府机构）规定的,与网络连接有关的监管和立法安全要求所产生的风险;2.使用默认潜在负面影响的业务，确保在网络上存储或传输的敏感及分类信息）。

b) 确定支持的安全控制——不仅适用于网络的非技术策略和技术策略（见第8章）。

c) 评审技术安全架构、设计选项，在考虑网络情景和“技术”主题的同时，选择和记录首选技术安全架构、设计和相关的安全控制（见第9至11章）（需知这将包括相关监管机构或立法机构(包括政府机构)定义的与网络连接相关的相关法规和立法所需的控制）。

d）开发和测试安全解决方案（见第12章）。

e）实施和操作安全控制（见第13章）。

f）监控和评审实施情况（见第14章）。

—应定期进行评审，一旦出现重大变化（业务需要、技术和安全解决方案等），就应重新访问和更新上述早期阶段的结果。

网络安全规划和管理过程的概述如图4所示。

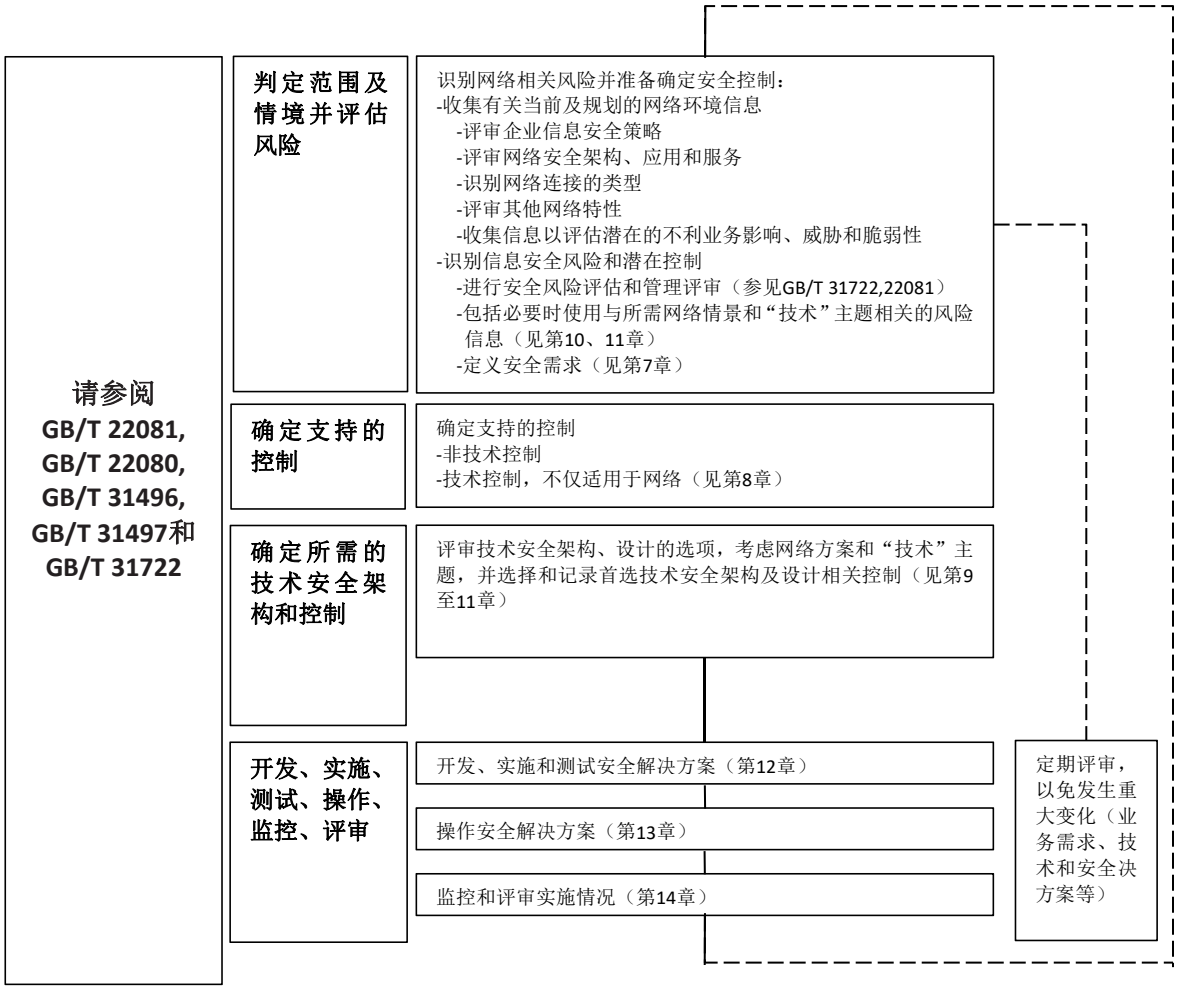

图4　网络安全规划和管理过程

应强调的是，在整个过程中应适当参考GB/T 22080、GB/T 22081及GB/T 31722，包括关于识别安全控制的一般建议。本部分是对这些标准的补充，并依据GB/T 25068.2-GB/T 25068.6的内容，介绍了如何识别适当的网络安全控制。

7　识别安全风险和准备确定安全控制

7.1　简介

如上文第6章所述，识别和评估网络相关风险和准备识别安全控制的第一阶段是收集有关当前及规划的网络环境的信息，第7.2章节为此提供了指导。第二阶段是确定和评估网络安全风险以及适当的潜在控制区域，第7.3章节为此提供了指导。

7.2 有关当前及规划网络的信息

7.2.1 组织信息安全策略中的安全需求

组织（或社区）的信息安全策略可包括关于保密性、完整性、不可否认性和可用性的声明，有关威胁和风险类型的表述，以及必须实施的网络安全控制。因此，第一步应该是评审企业信息安全策略，以了解所有一直被视为高等级的网络相关风险以及必须实施的网络安全控制的细节。

例如，这类策略可以描述为：

——某些类型的信息或服务的可用性是一个主要问题；

——不允许通过拨号线连接；

——所有与互联网的连接均应通过安全网关进行；

——应使用特定类型的安全网关；

——没有数字签名，则付款指令无效。

在进行风险评估和管理评审以及确定技术安全架构、设计方面和潜在的安全控制时，应考虑这些要求。任何此类要求应记录在潜在控制区域清单草案中，并在技术安全架构、设计选项中反映出来。

关于信息安全策略的指导在 GB/T 22081 和 GB/T 31722 中给出。

7.2.2 有关当前及规划网络的信息

7.2.2.1 简介

下一步应该是收集和评审关于当前及规划的网络——架构、应用及服务、连接类型和其他特性的信息——这将有助于识别和评估风险，并确定可能的网络技术安全架构、设计。具体描述如下。

7.2.2.2 网络架构、应用及服务

应获取相关的当前及规划的网络架构、应用程序和服务的详细信息，并对其进行评审，以便为网络安全风险评估、管理评审以及考虑网络技术安全架构选项提供必要的理解和背景。对上述内容的阐述应尽早在前期阶段完成，那么在识别、评估安全风险及相关安全控制，以及确定网络技术安全架构之后，将会得到更有效、更可行的安全解决方案。

此外，如果安全解决方案不能满足当前及规划中实际环境的要求，那么在早期阶段应对网络架构、应用和服务进行评审和必要地修订。

根据覆盖的区域，网络可以广义地分为两种类型：

——局域网（LAN），用于在本地互联各个系统；

——广域网（WAN），用于世界范围的系统互联。

（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”，即在一个城市内可用。然而，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。当今使用的另一个术语是全球区域网（GAN），即全球 WAN。注意，有些用于存储相关网络的术语，例如存储区域网络（SAN）和网络连接存储（NAS），但这些不在 GB/T 25068 系列标准的范围内，有关技术安全的内容参见 ISO/IEC 27040 存储安全）。

不同的协议具有不同的安全特性，应给予特殊考虑。例如：

——共享介质协议主要用于局域网，并提供各种机制来调控连接到各个系统之间共享介质的使用。当使用共享介质时，网络中的全部信息都可以通过所有互联系统进行物理访问，例如以太网；

——为允许进入网络而设计的访问控制协议，例如 IEEE 802.1x 和 WPA；

——路由协议用于广域网或局域网中不同节点间传输信息时定义路由。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；

——许多运营商网络均基于多协议标签交换（MPLS）协议，该协议允许一个核心承载网络被多个专用网络共享，而互相不产生干扰。MPLS 的主要应用场景是 VPN，用不同的标签来识别和分隔属于不同 VPN 的通信流（基于 VPN 的 MPLS 不依赖于数据加密机制），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。一个重要的优点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。

网络中使用的许多协议不具备任何安全性。例如，从网络通信流中获取密码的工具常常被攻击者利用。这使得像 Telnet 这样的网络协议在公共网络上发送的未加密口令具有高脆弱性。

注：Telnet 是在远程计算机上在线工作的终端仿真程序。

网络拓扑、传输媒介、有线网络和无线网络技术可以通过网络协议实现聚合。这对安全特性有更深远的影响。

基于安全性考量的网络应用类型可以包括：

——瘦客户端应用；

——桌面应用；

——终端仿真应用；

——信息传送基础设施与应用；

——存储、转发或假脱机的应用；

——客户端服务器应用。

以下示例显示应用程序特性如何影响其可能使用的网络环境的安全要求：

——信息传送应用（为消息提供加密和数字签名）可以提供足够的安全级别，而无需在网络上实施专用的安全控制；

——瘦客户端下载移动代码以实现特定的功能。在这种情况下，保密性可能不是主要的问题，完整性才是重要的，且网络应为此提供适当的机制。此外，如果需要满足更高的要求，移动代码的数字签名将提供完整性和附加鉴别。通常这是在应用框架内完成的，因此可能不需要在网络中提供这些服务；

——存储、转发或假脱机的应用通常为得到进一步处理而将重要数据临时存储在中转节点。如果存在完整性和保密性的要求，则需要在网络中进行适当的控制以保护传输中的数据。然而，由于数据暂时存储在中间主机，这些控制可能还不够。因此，可能需要应用附加控制以保护存储在中转节点上的数据。

还应安在安全语境下考虑网络服务类型（例如，DNS、电子邮件和语音等）。

在评审网络架构、应用和服务时，还应考虑到已有的组织或社区内部间或组织/社区内部与外部间往来的网络连接，甚至是计划的网络连接。组织、社区的现有连接可能因协议或合同的变更而限制或阻止新的连接。其他内外往来的网络连接均可能引入额外的漏洞，并可能而因此引入更高的风险，由此应需要更强的或附加的控制。

（有关网络和应用程序体系结构的一般指南可以在 GB/T 9387 中找到。）

7.2.2.3 网络连接类型

组织或社区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（仅已知社区可访问）实现，一些连接可以通过公共网络（任何组织或个人均可访问）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，考虑到这些连接的不同安全需求，这些连接也会涉及到互联网、内联网或外联网设施的使用。每种类型的连接可能有不同的漏洞，因而具有不同的安全风险，其结果是最终需要不同的控制。

按照业务需求，将通用网络连接类型分类如下：

——同一受控区域内同一组织的不同部分之间的互连，如单个受控楼宇或场所；
——同一组织不同地理位置上独立部门之间的互连，如地区办事处与总部通过广域网实现的互连。全部或大多数用户能够访问可用的信息系统，但并不是组织内的所有用户都具有访问所有应用或信息的授权；
——组织场所和在远离组织场所工作的人员之间的连接，或者由从家庭或其他远程站点工作的员工建立到组织运算系统的远程连接，而不是通过组织维护的网络连接；
——在封闭行业内的不同组织之间的连接，如由于合同或其他具有法律约束力，或类似的商业利益（如银行或保险）产生业务关联的情况。对于每个参与的组织来说，这种连接不提供全部应用程序的访问权限；
——与其他组织的连接，如访问其他组织所持有的远程数据库。在这种类型的网络连接中，连接组织的用户将获得被访问组织的单独预授权；
——与公共区域的连接，如组织内的用户发起对公共数据库、网站及电子邮件设施（例如，通过互联网）的访问；
——IP 环境与公共电话网的连接，即 IP 网络发起的向 PSTN 的电话连接。这种连接是不受控制的，因为从世界上的任何位置都可以接收这种连接。

无论使用什么分类方法，都应当评审当前及规划的网络环境中的不同类型连接的安全影响，并且所获得的信息应当用于识别和评估安全风险、相关的安全控制以及网络技术安全架构选项，最终决定采用哪一种网络连接方法。

7.2.2.4 其他网络特征

评审当前及规划网络的其它特征。另外，最重要的一点是确定使用的网络或将要使用的网络是公共网络（任何人都可访问）还是专用网络（专享或专线网络，被认为比公共网络更为安全）。同样，知道网络传输的数据类型也很重要，例如：

——数据网络——主要传输数据和使用数据协议的网络；
——语音网络——针对电话但也能用于数据的网络；
——“混合”网络包括数据、语音甚至视频的网络；

其它信息，例如：

——网络是经转换的数据包还是 MPLS 网络；
——MPLS 网络是否支持 QoS。（QoS 能够提供稳定的性能，具有可靠性和可用性。其提供的网络服务应使得性能最差的网络也可使用。例如，如果带宽不足，语音服务将会卡顿、崩溃）。

而且，还应确定是建立永久连接，还是在需要时建立连接。

一旦确定当前及规划网络的特征，表明至少已建立了公共网络或专用网络，接下来才会考虑网络安全风险评估和管理评审投入。因此，我们粗略将网络定义为：

——未知用户群；
——已知用户群和封闭的行业群（内含多个组织）；
——组织内部唯一（特定的）的已知用户群。

然后考虑使用的网络和将要使用的网络是公共网络还是专用网络，再进一步细化为：

——使用公共网络的未知用户群；
——使用公共网络的封闭业务群中的已知用户群；
——使用公共网络的组织内部唯一的已知用户群；
——使用专用网络的未知用户群；
——使用专用网络封闭业务群中的已知用户群，；
——使用专用网络的组织内部唯一的已知用户群。

无论采用哪种评审方法，某些组合可能意味着具有比其他组合更低的风险等级。所获得的信息应当用于识别和评估安全风险、相关的安全控制以及网络技术安全架构选项，以确定最终采用何种网络连接方法。

7.2.2.5 其他信息

最后，为GB/T 22082和20081兼容网络安全风险评估和管理评审，应收集其他信息，包括要仔细定义评审的边界范围。尽早收集其他信息是为了避免以后出现歧义和不必要的工作，并能提高评审的重点和效果。边界范围的界定应清楚的指明在执行网络安全风险评估和管理评审时应考虑的事情：

——信息类型；

——业务进程；

——实际的或可能的硬件构成、软件、服务、连接等细节；

——实际的或可能的环境（例如，位置和设施）；

——活动（操作）；

这些信息，同上述7.2章节结合起来，应用于网络安全风险评估和管理评审，其活动总结在7.3章节中，如下所示。

7.3 信息安全风险和潜在的控制区域

如前所述，现在大多数组织依赖于使用网络、相关的信息系统和信息以支持其业务的经营。而且，大多数情况下，对每个组织所在地信息系统的访问以及对组织其他场所内网和外网的访问有着明确的业务需求边界，这种访问包括面向和来自于公众的。当与第三方网络连接时，我们需要极其小心以确保连接组织不会暴露在附加风险之下（潜在的漏洞利用风险）。风险可能来源于连接本身或者网络连接的另一端。

还有一些风险可能与遵守相关法律法规有关（尤其要注意隐私和数据保护法律。一些法律法规对个人数据收集、处理和传播有法律管控，即那些与具体的个人有关的数据。例如，根据法律法规，将对通过网络收集、处理和传播的个人信息进行追责，甚至可能限制数据转移到特定地区或国家，这些都会产生重大的安全隐患。某些硬件和IP地址中少数不具有显著特征的数据也适用于这些法律法规）。

因此，面临的风险可能涉及对信息的未授权访问或发送、引入恶意代码、拒绝数据发送或接收、拒绝服务连接和无法获得信息和服务。这些风险可能造成如下损失：

——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（在网络和在与网络相连的系统中）；

——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）的抗抵赖性；

——网络交易的可追究性；

——信息（包括网络用户和管理员）的真实性；

——信息和代码的可靠性（在网络或与网络相连的系统中）；

——利用未授权控制和网络资源的能力，应体现在组织的网络安全策略（如为了个人利益而出售带宽或使用带宽）和有关法律法规（如存储儿童色情信息）中；

——控制滥用权限的能力。

该网络安全概念模型展示了可能出现的安全风险类型，如图5所示。

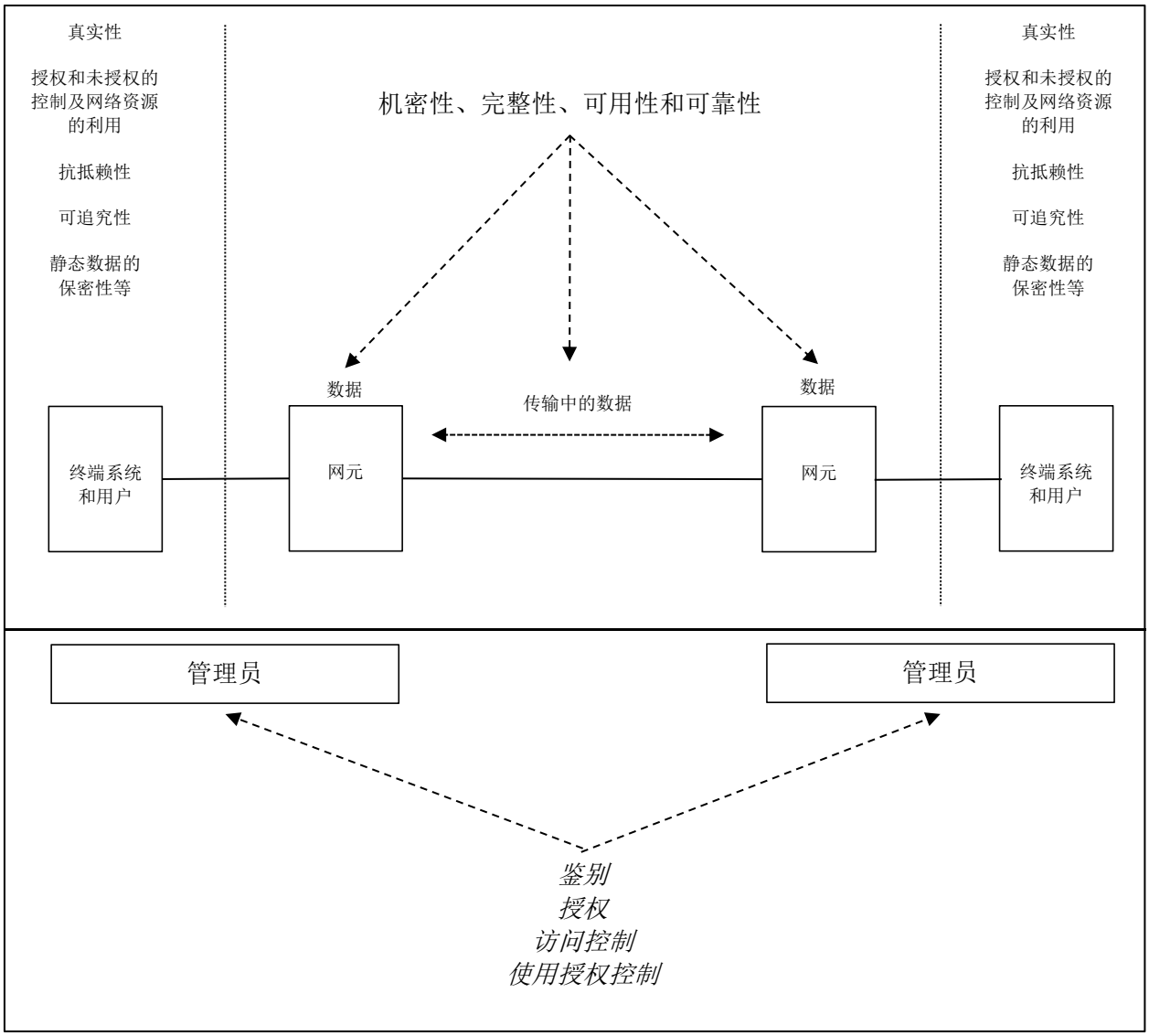

图5　网络安全风险区域的概念模型

因此，应根据 GB/T 22080、GB/T 22081 及 GB/T 31722 提供的指导，进行网络安全风险评估和管理评审，以识别并确认技术安全控制和技术安全体系结构、设计方面，支持非技术安全控制，符合公认的良好安全实践。这主要涉及五个方面：

——信息和服务的重要性，取决于由于商业操作引起的意外事故所造成的负面影响（有时亦称为资产评估）。这包括对网络中传输的业务运营信息的评估，以及其他任何可能通过网络未经授权访问的信息及其提供服务的评估；

——确定和评估对信息和服务产生威胁的可能性或级别；

——确定和评估已识别威胁或可利用脆弱性的严重性或级别；

——评估风险的措施，应根据企业经营可能造成的潜在负面影响以及威胁和脆弱性等级进行制定；

——通过识别技术安全架构、设计层面和潜在的安全控制域，以确保风险评估是可控的。

网络安全风险评估和管理的主要进程如图 6 所示。（这实际上是图 4 中的“判定范围及情境并评估

风险”及“识别网络相关风险并准备识别安全控制”的扩展图。）

图 6 的前两排为“确立评审的边界范围”和“资产识别”，表明这是准备性活动。下两排是风险评估活动，最后两排是信息安全控制筛选和（其他）风险接受活动。

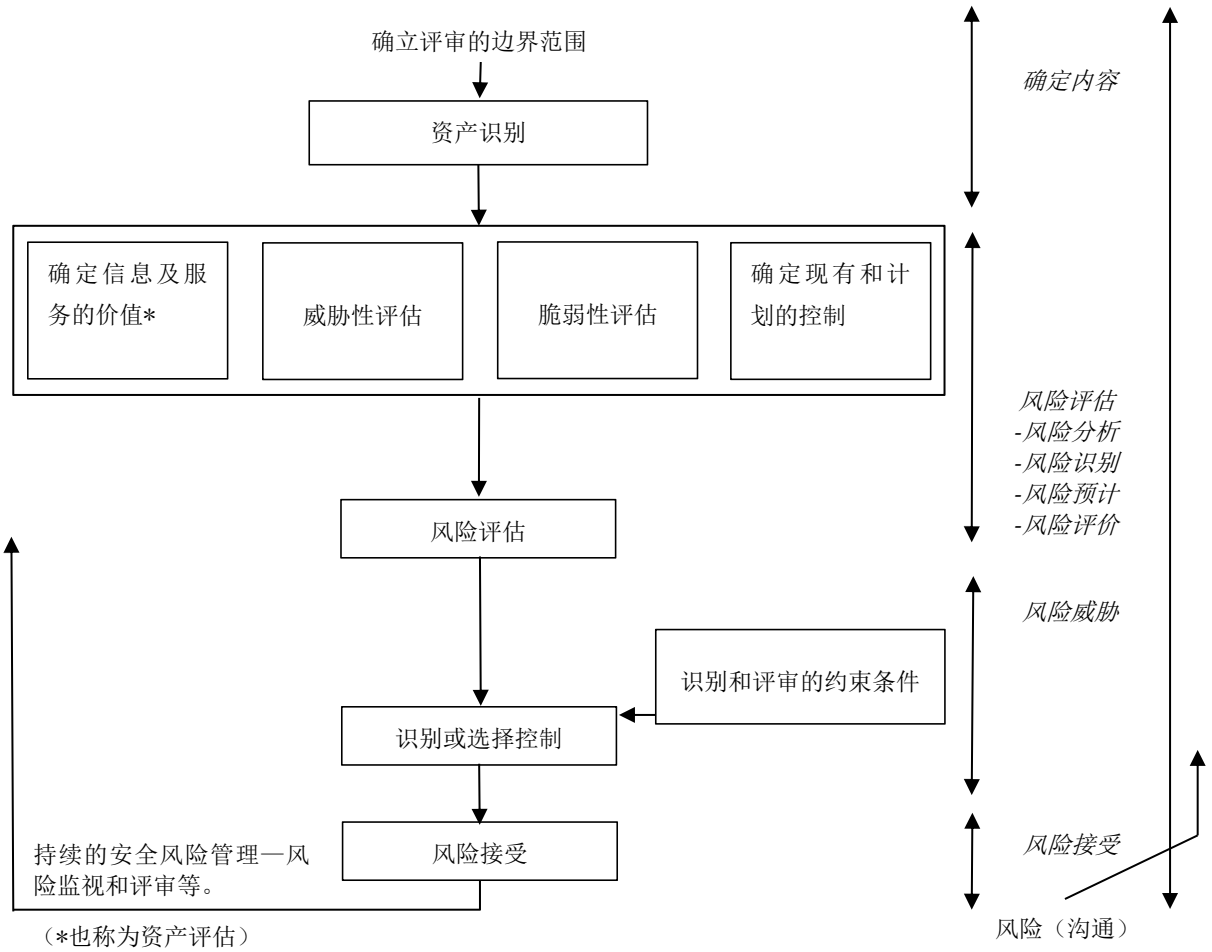

图 6 网络安全风险评估和管理过程

GB/T 22080 和相关标准中使用的术语以斜体显示。有关网络安全风险评估及管理评审的详细资料，请参阅 GB/T 22080、GB/T 22081 及 GB/T 31722。需强调的是，在进行此类评审时，应使用与所需网络方案和“技术”主题相关的风险(和安全控制)信息(见第 10 和 11 章，以及 GB/T 25068.3-GB/T 25068.6)。

8 支持控制

8.1 简介

本部分概述了支持网络安全技术架构的控制及和其相关的技术控制，即不仅仅适用于网络的其他控制（技术和非技术方面）。GB/T 22080、GB/T 22081 和 GB/T 31722 中可以找到很多这类的控制信息。这些对网络使用来说至关重要的控制将在下述 8.2 至 8.9 章节中进行阐述，分别是网络安全管理（网络安全管理活动、网络安全角色和职责、网络监视和网络安全评估）、技术脆弱性管理、鉴别和身份认证、网络审计日志记录和监视、入侵检测、恶意代码防护、基于密码的服务和业务连续性管理。如有需要，请参考 GB/T 22080、GB/T 22081 和 GB/T 31722 中的相关内容。

8.2 网络安全管理

8.2.1 背景

网络安全的全面管理应在一个安全方式下开展，且应充分考虑可用的不同网络协议和相关安全服务后实施。此外，组织还应考虑一系列的网络安全控制，其中大部分控制在GB/T 22081和GB/T 31722等标准中有所体现。这些将在8.2.2至8.2.5中所描述的网络安全背景中进一步展开。

8.2.2 网络安全管理活动

8.2.2.1 简介

对于任何网络来说，关键需求应得到安全管理活动的支持，包括对网络安全实现及运行的创建和控制。这些活动要确保组织、社区内所有信息系统的安全。网络安全管理活动应包括：

——定义所有与网络安全有关的职责，并指定一名对网络安全负全责的管理者；

——应对网络安全策略及相关技术安全架构进行建档；

——安全操作规程归档（SecOP）；

——实施安全合规性检查（包括安全测试），以确保维持相应的安全等级；

——在内部和外部组织或人员建立许可连接之前，应将网络安全连接条件进行建档；

——远程网络用户的安全条件建档；

——网络安全事故管理方案；

——建档并测试业务连续性、灾难性恢复计划；

可通过查阅 GB/T 22081、GB/T 31722和GB/T 20985（所有部分）获取详细的专题信息。上述对于网络的使用特别重要的专题将在下述章节中提供进一步指导。

8.2.2.2 网络安全策略

管理者有责任明确地接受和支持组织的网络安全策略（如GB/T 22081所述）。网络安全策略应源于组织的信息安全策略并与之一致。此策略应该能够得到实施，并容易被组织中得到授权的成员使用，且包含以下相关方面的清晰陈述：

——组织对可接受网络使用方面的立场；

——安全使用特定网络资源、服务和应用的明确规则；

——不遵守安全规则的后果；

——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。

——（在某些情况下，如果这些清晰的表述对机构更为方便，对机构人员更为清晰，可以并入到信息安全策略中。）

网络安全策略的内容通常应包括对网络安全风险评估和管理评审结果的概述（对控制的花费予以解释），包括与评估风险相当的所有安全控制的细节（见7.3）。

8.2.2.3 网络安全操作程序

为支持网络安全策略，应开发和维护SecOP文件。它们应包含与安全相关的日常操作规程的细节，以及负责其使用和管理的人员。附录B中有样板。

8.2.2.4 网络安全合规性检查

对于所有的网络连接，其安全合规性检查应从规定的控制中列出全面的检查清单：

——网络安全策略；

——相关的 SecOPs；
——技术安全体系结构；
——安全网关服务访问（安全）策略；
——业务连续性计划；
——相关的安全连接条件。

网络安全合规性检查应在任何网络连接的实际操作和重要版本更新之前（与重要业务或网络变更相关），或者每年进行一次。

这种检查应包括对公认标准的安全性测试，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。通常它应该包含脆弱性扫描与渗透测试的组合。在任何此类测试开始之前，应检查测试计划以确保测试将以完全符合相关法律法规的方式进行。在执行这种检查时，需注意网络不可能仅限定于一个地区之内——它可能分布于具有不同政策性法规的不同地区。该测试结束后，其报告应指出所遇到的漏洞细节和所需的修正及其优先级。

8.2.2.5 多组织网络连接的安全条件

除非连接的安全条件适当并且被正式许可，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，即用于隐私数据交换的网络连接的一端或两端遵从本地法律的约束，但若连接的一端位于另一个国家（在组织的域之外），则法律可能有所不同。

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 应为其连接中涉及的系统维护和演示确定特定安全级别。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 应生成该连接的安全条件文件，详述 B 需提供的控制。这些控制应在 B 实施后，由组织签署绑定声明以确保安全性。A 将保留对 B 进行委托或合规性检查的权利。

在某些情况下，社区中的组织彼此认可一个“连接安全条件”文件，该文件记录所有各方的义务和责任，包括相互的合规性检查。

8.2.2.6 远程网络用户安全条件文档

授权远程工作的用户应配有远程网络用户安全条件的文件。该文件应说明用户对网络的硬件、软件、和数据的责任以及它的安全性。

8.2.2.7 网络安全事件管理

使用网络时信息安全事件发生的可能性更大（与不使用网络的情况相比），对业务产生的不利影响也更严重。此外，与其它组织连接的网络很可能发生具有重大法律后果的安全事故。

因此，有网络连接的组织应具备一个便于文件化和实施的信息安全事件管理方案以及相关的基础设施，以便能够在识别安全事故时迅速做出反应，最大限度地减少其影响，并吸取教训，以防止再次发生。该方案应能解决信息安全事态（识别系统、服务和网络状况中可能存在的违反信息安全策略或防护失效或与之前未知的安全相关的情况）和信息安全事件（很可能入侵企业经营和威胁信息安全的，独立或一系列有害的或未预料的信息安全事态）。更详细的信息安全事件管理见 GB/T 20985（所有部分）。

8.2.3 网络安全角色与职责

与网络安全管理有关的角色与责任如下（注意，根据机构的规模这些角色可以合并）。

高级管理：
——明确组织的安全目标；
——创立、审批、发布和实施组织的安全策略、规程和规则；
——创立、审批、发布和实施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。

（注意高级管理包括企业负责人）

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；

——确保网络操作职责与电脑操作分开，安排合理。

网络安全团队：

——获得、开发、测试、检查和维护网络安全组件与工具；

——维护网络安全工具和组件以密切关注威胁的演变（例如，更新恶意代码（包括病毒）标签文件）；

——根据业务需要的变化，更新与网络安全相关的配置。

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确保有效的安全策略所要求的安全规范、规则和参数得到应用；

——采取适当措施以确保网络安全组件有效运行（例如备份、检测网络活动，响应安全事故或警报等）。

网络用户：

——传达其安全要求；

——遵守机构安全策略；

——遵守机构网络资源使用策略；

——报告网络安全事件和事故；

——提供网络安全有效性反馈。

审计员（内部和外部）：

——评审和审计（例如，定期测试网络安全的有效性）；

——检查系统是否符合网络安全策略；

——检查和测试操作安全规则中当前业务要求和法律限制的兼容性（例如网络访问的许可列表）。

8.2.4 网络监视

网络监视是网络安全管理中非常重要的一个部分。下面 8.5 章节中有论述。

8.2.5 网络安全评估

网络安全是一个动态概念。安全人员应始终跟进该领域的发展，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新来进行连续工作。对于建立的基准，应定期审计现有的安全控制，包括安全测试、脆弱性扫描等。安全应是评估新的网络技术和网络环境的主要考量。

8.3 技术脆弱性管理

与其他复杂系统一样，网络环境也存在错误。有些已知的或已经被公开的技术脆弱性组件仍在网络中被频繁使用。利用这些技术脆弱性对网络安全可能产生严重的影响，最常见于信息的可用性和保密性。因此，技术脆弱性管理目前应涵盖所有的网络组件并应包括：

——及时获取技术漏洞的信息；

——评估此类漏洞的曝光程度；

——制定恰当的安全控制解决相关风险；

——执行和核验预定的安全控制。

技术脆弱性管理的先决条件是能获取当前所有网络组件的完整清单，提供必要的技术信息，例如设备型号、供应商、硬件版本号、固件或软件以及机构信息，例如负责管理人员。

如果组织已成立了综合技术脆弱性管理项目，优先方案是把技术网络脆弱性管理项目并入到综合任务中。（关于技术脆弱性管理更详细的信息，包括实施指南，可以在 GB/T 22081 中找到。）

8.4 鉴别和身份认证

对授权人员的访问进行限制是非常重要的（无论是组织内还是组织外的）。例如，策略普遍要求对授权人员访问特定的网络服务和相关的信息进行严格限定。对这些连接的要求并不仅限于网络连接，因此可以通过参考 GB/T 22081 和 GB/T 31722 获得适用于网络使用的细节。

可能与网络的使用和相关的信息系统有关的三个安全控制域如下：

——远程登录。无论是来自远离组织工作的授权人员、远程维护工程师还是来自其它组织的人员，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。必要时，组织可以通过内部系统或合作伙伴利用公共网络建立网络连接。每种类型的远程登录应有适合相关网络性质的附加安全控制，例如，不允许使用远程访问帐户直接访问系统和网络软件，除非有提供附加的鉴别（见下文）——端对端加密以及对远离办公场所人员在未经授权的情况下，访问存储在电脑上的邮件软件和根目录数据进行保护。

——加强鉴别。使用用户 ID 或口令匹配是认证用户的简便方法，但可能遭到入侵或被猜出密码。因此，我们应考虑其它更多的安全方式认证用户，尤其是远程访问用户或未授权人员很可能获取受保护的重要系统权限，这是因为访问可能是使用公共网络发起的，或者访问系统可能不在组织的直接控制之下（例如，通过笔记本电脑）。最简单的方法是使用用户呼叫识别器（CLID）（但由于其易被冒用，因此 CLID 在无法进一步鉴别的情况下不会被用于认证 ID），通过调制解调器在不使用时断开连接，但仅在调用者身份认证后才进行连接。使用其它的认证方式支持用户鉴别是更复杂但也更安全的方法，尤其是在远程访问情境下，例如，远程验证标识和智能卡，并确保标识或智能卡只在授权用户鉴别帐户时起作用（最好是用户的电脑和位置或接入点），例如任何相关的 PIN 码或生物识别信息。这就是强大的双因素鉴别。

——安全单点登录。用户网络很可能遇到多次鉴别和身份认证核查。在这种情况下，用户可能冒险采用不安全的登录方式，例如，写下密码或再次使用相同的鉴别数据。安全单点登录可通过减少用户必须记住的密码数量从而减少与此类行为相关的风险。除了降低风险之外，用户的生产力也可以得到提高，并且可以减少与密码重置相关的服务台工作负载。然而，安全单点登录失败的后果是致命的，因为很多系统和应用可能处于风险之中，并且会受到损害（有时被称为“打开王国的钥匙”风险）。因此，比常规的鉴别和身份认证机制更强大的机制是必要的，并且从安全单点登录机制中排除对高级特权(系统级别)功能的鉴别和身份认证可能是更可取的。

8.5 网络审计日志和监视

通过审计日志记和持续监视对安全事件和安全事故进行快速的检测、调查、报告、响应，对确保网络安全的有效性来说非常重要。没有这些活动，就不可能保证网络安全控制始终有效，也不可能保证不发生对业务运行产生不利影响的安全事故。

应记录足够的错误状况和有效事件的审计日志信息，以确保对可疑或实际发生的网络安全事故进行彻底地评审。然而，分析如此大量的审计信息是十分困难的，而且会影响性能，因此更应该关注实际记录的信息是什么。对网络来说，审计日志维护应包括以下事件类型：

——远程登录失败的日期和次数；

——失败的重新鉴别（或标识使用）事件；

——安全网关通信量违规；

——尝试远程访问审计日志；

——系统中与安全相关的警报/预警（例如，IP 地址复制，电路中断）。

在联网环境中，审计日志应从多个渠道获取，例如路由器、防火墙、入侵检测系统（IDS）并发送到中央审计服务器上进行全局分析。所有的审计日志应进行实时和离线检查。在实时检查时，日志通过滚屏显示并对潜在的攻击发出预警。离线分析必不可少，因为这样可以从大局进行确定的趋势分析。一个攻击的最初迹象可能是在防火墙日志中出现大量的流量,这表明是针对潜在目标进行的探测活动。IDS 也能根据攻击特征码对其实时检测。

需强调的是，为了便于分析和调查，必须使用适当的经批准的审计日志管理和分析软件进行日志存储、检索、溯源（针对特定用户、应用程序和信息类型以及时间段，特别是在出于调查目的时）和报告，以快速的得到重点突出和容易理解的结果。审计日志分析报告必须保存在安全的地方，并按规定时间存档。必须在 UDP 中进一步保护审计日志（包括鉴别和身份认证以及访问控制）。持续监视涵盖的范围包括：

——防火墙、路由器、服务器等审计日志；

——预先配置的审计日志发出警报通知特定事件类型，例如防火墙、路由器、服务器等；

——入侵检测系统的结果；

——网络安全扫描活动结果；

——由用户和支持人员报告的安全事件和事故信息。

根据组织的需要，审计痕迹应在线保存一段时间。所有的审计痕迹都需要备份并存档以确保信息的完整性和可用性，例如，使用 CD 等 WORM 媒体。此外，审计日志还包含敏感信息以及可能被攻击者利用网络连接进行攻击的信息。在发生网络纠纷时，审计日志能够提供在信息网络中传输的证据，特别是能够确保其完整和抗抵赖性。因此，所有的审计日志应适当保护，包括在指定日期对存档 CD 进行销毁。根据企业要求和国家法律，审计痕迹应安全保留一段时间。另外，审计痕迹和相关服务器的时间同步也非常重要，例如，网络时间协议（NTP）经常用于取证和诉讼。

值得强调的是，实施网络监视应完全遵守国际和国家相关法律法规，这包括数据保护法和调查权规范法（根据法律，在实施任何监视之前应通知所有的用户）。总之，监视应本着负责的态度，而不是利用某国隐私法的不健全去查看员工的行为。显然，采取的网络监视行为应与所在组织、社区的安全和隐私策略相一致，处理相关责任时，程序恰当。如果刑事或民事诉讼中使用审计日志证据，实施网络审计记录和监视时还应更加谨慎。

关于网络使用的大多数评审记录和监视控制以及相关的信息系统可以根据 GB/T 22081 及 GB/T 31722 的使用而定。

8.6 入侵检测和防御

随着网络使用量的增加，入侵者可以更容易地找到多种方法来隐藏其初始访问点，以渗透到组织或社区的信息系统和网络中，建立网络连接并瞄准内部信息系统。而且，这些入侵者变得更加狡猾，使用的攻击手段也更加复杂，因为他们所使用的工具可以在网上或公开文献中获得。实际上，他们使用的很多工具都是自动的、高效的，就算是对初级入侵者来说也很容易。

对大多数组织来说，预防所有的潜在渗透从经济上说几乎不可能实现。因此，入侵行为很可能会发生。大多数渗透的相关风险应通过提高鉴别和身份认证能力、逻辑访问控制能力、计算评审控制能力以及入侵监视和防御能力得以解决。这些能力能够预测入侵、识别入侵、提高告警级别并防御入侵。它还能本地收集入侵信息，随后进行整合和分析，以及分析组织正常信息系统行为、使用模式。

IDS 监视所有内部网络的流量情况，以确定入侵是否尝试发生、正在发生或已经发生，对入侵做出响应，并向适当的人员发出警报。有两种类型的 IDS：

——NIDS：监视网络数据包并试图把攻击者的攻击模式与已知攻击模式数据库进行匹配来发现入侵者。

——HIDS：通过监视安全事件日志或检查系统变化实现监视主机（服务器）的活动，例如，系统重要文件的变化或系统注册表的变化。

入侵防御系统（IPS）会对进入内部网络的所有流量进行检查并自动拦截所有可识别的攻击。换言之，IPS 是专门为提供主动响应而设计的。

ISO/IEC 27039 中提供了详细的入侵检测和防御指南。

8.7 恶意代码防御

恶意代码（病毒，蠕虫，木马，间谍软件等——通常统称为“恶意软件”）通过网络连接传播。恶意代码能够造成计算机执行未授权的功能（例如在特定日期和时间用消息轰炸特定的目标），或者一旦复制就试图找到其他易受攻击的主机，同时破坏重要的资源（例如删除文件）。除非实施合适的控制，否则在损坏完成之前无法检测到恶意代码。恶意代码可能导致安全控制入侵（例如获取和泄露密码）、信息意外泄露、信息意外改变、信息破坏及未经授权使用系统资源。

通过特殊的扫描软件可以检测并删除某些类型的恶意代码。该扫描软件可用于扫描防火墙、文件服务器、邮件服务器和某些类型恶意代码的个人电脑、工作站。而且，要确保扫描软件始终更新到最新版本非常重要，最好每日更新一次，这样才能够检测到新的恶意代码。然而，用户和管理员应意识到不能完全依赖扫描设备检测所有的恶意代码（甚至特定类型的所有恶意代码），因为新形式的恶意代码不断出现。通常情况下，需要其他形式的控制来增强由扫描程序提供的（当扫描软件生效时）保护。

总的来说，反恶意代码软件的工作是扫描数据和程序，以识别与恶意软件相关的可疑模式。扫描的模式库被称为特征码，应每隔一段时间更新一次，或者在获取高风险恶意软件警报时更新特征库。在远程接入的情况下，防御病毒的软件应在远程系统上运行，也应在中心系统的服务器上，特别是在 Windows 系统和电子邮件服务器上运行。

网络用户和管理员应意识到在处理与恶意软件相关的外部连接时，风险更大。用户和管理员应通过制定细致的规程和实践从而尽可能减少恶意代码的产生。

用户和管理员应特别关注与网络连接有关的系统和应用配置，关闭不必要的功能（例如，PC 应用可以配置为宏被默认关闭，或在执行宏之前要求用户确认）。

更详细的恶意代码防御请参见 GB/T 22081 和 GB/T 31722。

8.8 基于密码的服务

在保密性要求高的环境中，应考虑对网络上的信息进行加密控制。在完整性要求高的环境中，应考虑数字签名和信息完整性控制以保护网络连接上的信息。数字签名控件可以为消息鉴别控制提供类似的保护，同时也具备抗抵赖性。

网络上传输的信息在要求提供实质性证据时（抗抵赖性），应该考虑如下控制：

——提供确认提交的通信协议；

——要求提供发件人地址或标识符并检查此信息存在与否的应用协议；

——检查发件人和收件人地址格式中语法的有效性及与相关目录中信息一致性的网关；

——确认网络发送以及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，并通过使用标准数字签名方法来提供保证（这也是一种抗抵赖的形式）。在需要来源证明的情况下，信息发送方应使用通用标准的数字签名密封信息。如需提供交付证明，发送方应要求使用数字签名封装回复。

决定使用加密、数字签名、消息完整性或其他基于加密的控制时应考虑相关法律法规，并视情况考虑适当的公钥基础设施、密钥管理要求、使用的机制是否适合所涉及的网络类型和所需保护程度，以及

与数字签名协议中使用的密钥(相关认证)相关联的用户或实体的可靠可信注册。

ISO/IEC 18033（所有部分）对加密机制进行了标准化。ISO/IEC 10116 标准化了使用分组密码进行加密保护的方式(操作模式)，这是一种常用的，被称为分组密码的加密技术。在 ISO / IEC 9797（所有部分）中对被称为消息认证码(或 MACs)的消息完整性控制进行了标准化。ISO /IEC 9796（所有部分）和 GB/T 17902（所有部分）（ISO/IEC 14888，IDT）对数字签名技术进行了标准化。更多与抗抵赖性有关的信息请参见 ISO/IEC 14516 和 GB/T 17903（所有部分）（ISO/IEC 13888，IDT）。

作为其它所有加密服务的基本服务，密钥管理保证了其生命周期期间的密钥安全管理和使用。有关密钥管理以及相关主题（PKI 或身份管理的更多主题），应参考其它文件和标准，如下：

—— GB/T 17901（所有部分）：信息技术 安全技术 密钥管理（ISO/IEC 11770，IDT）；

—— GB/T 16264.8 ：目录 公钥与属性证书框架（ISO/IEC 9597-8，IDT）；

—— ISO 11166—2：银行业务，借助非对称算法的密钥管理；

—— GB/T 27909（所有部分）：银行业务 零售密钥管理（ISO 11568，MOD）；

—— ISO 11649：银行业务 多中心密钥管理；

—— GB/T 21081：银行业务 密钥管理相关数据元（零售）（ISO 13492，IDT）；

—— ISO 21118：银行公钥基础设施。

注意，加密也应用于网络设备的管理。此外，访问和网络管理日志应以安全加密会话的形式传输，以保护敏感数据。

8.9 业务连续性管理

重要的是要制定控制，以便在发生灾难时确保业务的持续运作，并且在适当的时间范围内提供业务被中断后恢复每个部分的能力。因此，组织应适当安排业务持续性管理计划，其过程涵盖所有业务连续性阶段——业务影响分析评审、风险评估评审、建立业务恢复要求、业务连续性策略制定、业务连续性计划制定、企业连续性计划测试、全体员工企业连续性意识提升、业务连续性计划持续维护以及风险降低措施。只有遵循所有的阶段才能确保实现：

——所需的业务优先级和时间尺度符合业务需求；

——被识别的推荐业务连续性策略选项与优先级和时间尺度匹配；

——正确且必要的计划与设施得到妥当安排及测试，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。

业务连续性管理指南作为一个整体，包括业务连续性策略和相关计划制定，以及后续测试，都可以在 ISO/PAS 22399:2007 中得到。

从网络的角度看，网络连接的维护、实现具有足够容量的替代连接，以及在网络安全事件之后的恢复连接等问题，都必须予以解决。这些方面和要求应充分考虑随着时间的推移，连接对业务功能重要程度以及发生损害时对业务产生的不利影响。虽然连通性可以给组织带来许多好处，但如果发生中断，就灵活性和使用创造性方法的能力而言，它们也会成为脆弱点和“单点故障”，这可能对组织造成破坏性影响。

9 网络安全设计和实现指南

9.1 背景

本章节阐明了各种网络技术安全架构、设计层面和相关潜在控制区域的问题。第 10 章为网络场景的风险、设计技术和安全控制区域提供了参考。第 11 章为当前组织关注的特定技术主题提供有关风险、设计技术和安全控制要素的参考。第 10 章和第 11 章介绍了一种特定的网络安全解决方案，包括许多主

题和控制区域。附录 B 中有关于 GB/T 22080、GB/T 22081 网络安全相关控制和 GB/T 25068.1 交叉引用的表格。

依据第 8 至 11 章中所提到的相关网络架构，应用所涉及的技术安全架构、设计以及明确的控制列表进行详细评审。架构和控制清单应根据需要调整，然后用于作为制定、执行和测试技术安全方案的基础（见第 12 章）。一旦技术安全架构和安全控制生效，就应开始实施实时的持续监视和执行评审（见第 14 章）。

9.2 网络技术安全体系架构、设计

可行的技术安全架构、设计文件和执行选项为不同解决方案提供了协调分析方法的基础，这也有利于解决企业需求和安全需求之间经常出现的技术限制和争论问题。

记录选项时，帐户应满足组织所有的安全策略要求（见 7.2.1），包括相关网络架构、应用、服务、连接类型、其它特征（见 7.2.2）和安全风险评估与管理评审确认的潜在控制清单（见 7.3）。帐户必须满足现有的技术安全架构、设计才能实现。一旦选项被选中并评审，作为技术架构设计进程的一部分，它会被批准并记录于技术安全架构、设计控制规格文件中（无论与技术架构设计兼容与否）。形成最终的网络架构、应用和服务（确保与优先技术安全架构、设计一致）和潜在的控制列表（例如，因为技术架构、设计默认只能以特定的技术方式执行，必须替换确认的控制）。

GB/T 25068.2 阐述了组织应如何利用一致的方案来进行规划、设计并执行网络安全来实现高质量的技术安全架构、设计，以确保网络安全适合业务环境。

网络安全结构、设计开发进程的输入包括：

——组织、社区的文件化服务要求；

——所有现存或计划的架构、设计及执行的文件；

——当前的网络安全策略（信息系统安全相关策略），在安全风险评估和管理评审结果基础上优先选择；

——定义受保护资产；

——当前及规划性能要求包括相关流量要求；

——当前产品信息。

设计过程输出包括：

——网络技术安全架构、设计文档；

——每个安全网关、防火墙系统（包括防火墙规则库）的服务访问需求文档；

——安全操作规程；

——第三方安全网络连接相关条件；

——第三方用户相关使用指南。

网络技术安全架构、设计文件，在 GB/T 25068.2 中有详述，GB/T 25068.2 附录 D 也包含服务访问（安全）要求文件模板。其它文件的更详细的信息见 8.2.2 和 GB/T 25068.2。

（此外，一旦所需的网络技术安全架构、设计已被记录和执行，那么应当生成安全测试规划并进行安全测试。如果测试结果满意，根据测试期间发现的问题进行适当调整后，网络技术安全架构、设计和执行正式完成（见第 12 章））

下面每个活动的信息都记录于 GB/T 25068.2 ：

——网络安全技术设计和执行准备；

——网络安全项目启动；

——确定组织、社区广义上的网络需求；

——评审现有的及规划的技术架构并执行（要详述所有现存以及计划的技术架构和执行方案，检查是否与组织、社区的功能需求相一致）；

——资产识别并确认；
——确认安全风险评估和管理结果，并依据结果评审现有以及计划的网络安全控制，选择潜在的安全控制；
——评审网络性能要求并确认标准（评审性能需求、消除疑虑以及性能标准需要满足已正式确认的技术架构和相关技术安全架构、设计。因此，要识别通讯线路、服务器和安全网关等的配置数据，以确保达到服务需求）；
——网络技术安全设计应包括所有应用技术主题(这些主题与GB/T 22080—2016中的章节相对应)；
——使用场景和技术指导（GB/T 25068.3-GB/T 25068.6有叙述）（同样，见第10章和第11章）；
——使用模型框架（包括 ITU-T X.805）；
——产品选型是一个同网络技术安全架构设计有关的迭代过程，不能孤立的来看，要考虑到多个因素（这些因素包括技术适用性、性能、可扩展性、管理设施、逻辑安全性，当然还有供应商的能力、跟踪记录等）；
——概念验证（在网络技术安全架构和相关产品集还未就位前，=或产品服务审视之前（因为服务提供商往往夸大了产品的性能），进行概念验证）；
——网络技术安全架构、设计实现和存档；
——准备测试（制定安全测试策略，描述测试使用的方法证明网络技术安全架构，重点是关键的技术安全控制应如何测试。然后制定网络技术安全架构测试计划，包含实施测试的很多细节，包括何时何地由何人实施）；
——正式签署网络技术安全架构。

总体设计原则（使用最多的原则）在GB/T 25068.2中有描述。而且，可参考GB/T 25068.2附录——网络安全、模型框架案例学习和示例文档模板中的示例模型框架（参考架构）。

在最终确定执行安全控制列表之前，应完全记录并批准所有项目的技术安全架构、设计。

10 参考网络场景—威胁、设计技术和控制要素

10.1 简介

GB/T 25068.3描述了与参考网络场景有关的威胁、设计技术和控制要素。下文10. 2至 10.10章节中介绍了一些场景的例子。GB/T 25068.3不仅提供了详细的安全风险和安全设计技术指导，还提供了在所有特定场景下减轻风险所需要的控制。GB/T 25068.3包括GB/T 25068.4-GB/T 25068.6的引述，以避免文档内容重复。

10.2 员工互联网访问服务

目前，几乎所有的组织都为员工提供互联网访问服务，提供此类服务时应考虑访问目的是否明确且经过授权，而不是一般开放访问。其提供的服务应制定具体的策略，并明确使用目的。正常情况下，商业原因可以进行网络访问，需遵守组织的策略。因私也可访问（通常形式受限）。另外，还需考虑允许使用哪种服务——它是否是类似 www（http和https）的基本服务，是否只允许信息检索还是包括员工参与的聊天频道、论坛等，是否允许增强协作服务——如果是这样，组织可以引入一系列特定场景下处理风险的机制。

基本原则是企业只在需要服务时允许访问，但业务运行需求使用的服务将带来更多相关安全风险。即使有限制策略，员工访问网络还是会带来大量的安全风险。

10.3 增强性协作服务

包含各种通信和文档共享的可能性的增强性协作服务（例如即时消息——聊天、视频会议和文档共

享环境）在当今的商业环境中越来越重要。这样的协作服务通常包括视频电话、通过聊天信道的语音通信、电子邮件系统，以及文档共享和在线联合办公环境。组织利用两种基本方法来使用这种服务：

——仅将其用作内部服务使用，但缺点是该服务不能与外部合作伙伴一起使用等；

——将其作为组织内部服务和外部的服务使用。使用这种服务可以带来更多益处，但同时会带来更多相关安全风险。

在实施方面，该服务可以在内部实施，或者只是从第三方购买作为服务。在许多仅使用内部服务的情况下，最可能在内部实施。如果该服务要在内部和外部使用，从第三方购买协作服务则是更合适的解决方案。内部以及内外部同时使用的情况下，该服务提供了用于减轻这些风险的关于安全设计技术和控制的安全风险和建议。

10.4 企业对企业的服务

传统上讲，企业对企业的服务已经能够通过租用专用线路或网络段来实现。互联网和相关技术确实提供了更多的选择，但也引入了与实施这些服务相关的新安全风险。通常，企业对企业的服务有自己的要求。例如，可用性和可靠性是非常重要的要求，因为组织依赖于企业对企业的服务。

当使用互联网作为基本网络连接来实现企业对企业的服务时，可用性和可靠性等需求需要与之前区别对待。使用租用线路来衡量服务质量的方式已不再适用，需要通过适当的设计技术和控制来降低新的安全风险。

10.5 企业对客户的服务

企业对客户的服务包括电子商务和电子银行。需求包括保密性（特别是电子银行）、鉴别（当下可能使用的方法，例如双因素，基于证书等等；实施成本之间的关系也很重要，通常是因为客户数量大以及财务损失、商业声誉、信誉损失等风险的减少）、完整性和抵抗复杂性攻击（例如“中间人”或“浏览器中间者”攻击）等要求。

特征包含以下内容：

——安全通常只在组织控制下的终端平台上得以“保证”，为实施控制和维持平台安全提供良好环境；

——客户平台，特别是 PC 的安全性通常很差。在这种环境中实现控制更加困难，因此在这种情况下，客户平台将面临更多的风险（在这种环境下很难实施合同中无“安全连接条件”等系列要求）。

10.6 外包服务

由于现在 IT 环境的复杂性，许多组织使用外部提供的 IT 支持服务，或者完全或部分外包其 IT 基础设施的支持，及使用其他外包服务。许多供应商还要求直接访问其客户使用的产品，以便能够适当地处理网络安全事故或支持管理。

许多外包服务需要永久的访问权限，例如，支持访问的基础设施的权限，其他人可能只需要临时访问权限。在某些情况下，外包服务需要较高的访问权限，以便完成所需的任务，特别是在事故管理场景中。

10.7 网络划分

对许多地区，特别是港澳台地区而言，特定的地方性法规或政策性法规对信息安全要求有很大的影响。组织通常在许多不同地区开展业务，因此有义务遵守各个地区的特定政策法规，这可能进一步导致组织需满足每个地区的信息安全要求。这通常需要采取额外的信息安全控制，以确保遵守此类政策法规。

为了满足某个组织在不同地区开展业务的信息安全要求，实施网络划分是一个有效的泛解决方案。

在许多情况下，这种泛解决方案除了可以用于应用程序级访问控制外，还可用于建立单独的防御屏障。

10.8 移动通信

该参考网络场景涉及个人移动通信设备，例如，流行的智能手机或掌上电脑（PDA）（关于网络上设备通信的安全指南在GB/T 25068.6关于IP无线网络安全通信安全中有所阐述）。

虽然个人移动通信设备新特性的快速开发的主要驱动力来自于消费市场，但这些特性也可用于商业环境中。如“个人”一词引申为这种设备被个人所有，且可用于商业和私人目的。由于供应商希望在竞争性市场中获得更多的商机，原有专属于商业市场的设备也被引入消费市场。这类设备所具备的新功能中，设备存储器能力的增长、开放公共互联网的永久在线连接，以及人们出于私人和商业目的使用相同设备等情况，意味着更大的安全风险。

此外，随着个人移动通信设备的高度流行以及它们作为“私人物件”的身份，在许多情况下，仅使用有限特征集或仅允许有限数量设备连接的限制性策略可能无效或被绕过，从而意味着信息安全有效性的降低。

10.9 旅行用户的网络支持

当前，旅行用户期望旅行过程中的网络连接同在固定位置（例如其办公室）的连接一样有效。这样的解决方案和产品通常侧重于功能方面。从信息安全的角度来看，这样的功能往往带来新的风险，使得预设的信息安全策略受到影响甚至无效。例如，如果未使用适当的控制来实现旅行用户对内联网的访问，那么维持良好控制和（从外部）受保护的内联网的假设可能被质疑。

10.10 家庭和小型企业的网络支持

家庭和小型企业通常需要将组织的内部网络扩展到家庭或小型办公场所。扩展成本是一个关键问题，因为成本、效益通常不需要很高的实施成本，这意味着用于保护这种网络扩展的安全控制成本有限，并且通常阻止使用用于连接较大内联网段的已建立的网络互联安全控制。

在许多家庭或小型企业场景中，基础设施也可用于私人和商业目的，这可能导致额外的信息安全风险。定义安全风险，并提出有关安全设计技术和控制以缓解这些风险的建议。

11 “技术”主题—风险、设计技术和控制要素

与“技术”主题相关的安全风险、设计技术和控制要素包括如下内容：

——局域网；
——广域网；
——无线网；
——无线电网络；
——宽带网；
——安全网关；
——虚拟专用网；
——语音网络；
——IP 聚合；
——虚拟主机；
——电子邮件；
——路由访问第三方组织；
——数据中心。

12 开发和测试安全解决方案

一旦技术安全架构已完全记录并获得一致认可（包括高级管理层），则应制定解决方案，以“试用模式”实施，并进行全面测试和合规性检查。

一般来说，“适用性”测试应率先进行，通过测试策略文件所描述的方法，从而验证解决方案并制定测试计划。由于执行此类测试检验出某些不足，可能需要对测试策略进行更改，如有必要还需重新进行测试。

一旦“适用”测试已成功完成并做出了更改，应检查该实施是否符合文档化的技术安全体系结构和以下文档中规定的所需安全控制：

——技术安全体系结构；

——安全策略；

——相关安全操作规程（SecOPs）；

——安全网关服务访问(安全)的策略；

——业务连续性计划；

——相关安全连接条件。

合规性评审应在现场运行之前完成。当所有缺陷已被确定、修复并由高级管理层签署后，评审即已完成。

应强调的是，这应包括对相关公认的行业、地方标准（在没有国家标准的情况下）进行安全测试，在明确何时何地要进行哪些测试后，应制定安全测试策略和相关的安全测试计划。这应包括脆弱性扫描和渗透测试的组合。在开始任何此类测试之前，应检查测试计划，以确保该测试与相关法律法规完全兼容。在进行这项检查时，不应忘记，网络不仅限于一个国家——它分布在具有不同立法的不同国家。在测试结束后，报告应指出所遇到的漏洞并进行必要的修复，并以优先级标明，在附录中确认所有需要的修复已完成。此类报告应由高级管理层签署。

最后，当一切完毕时，应当签署并接受执行——包括高级管理层。

13 操作安全解决方案

“操作”是指使用达成一致的安全解决方案运营实时（日常）网络，并已经进行了安全测试，预先完成了相关的必要操作。换言之，一旦签署技术安全架构以及安全控制实施，则应开始执行日常运营。随着时间的推移，如果发生重大变化，则应进行进一步的实施测试和评审（见第 14 章）。

14 监视和评审解决方案的实施

在日常运营实施后，应根据相关公认的行业、地方标准（在没有国家标准的情况下）开展持续监视和合规性评审。此类活动应在与业务需求、技术、安全解决方案等相关的重大变化发布之前进行，否则每年进行一次。这里的活动应遵循上文第 12 章所述的模式。

附 录 A
（资料性附录）
GB/T 25068 本部分中安全控制部分同 GB/T 22080、GB/T 22081 标准中相关章节交叉引用

表 A.1 根据 GB/T 22080、GB/T 22081 章节

GB/T 22080/22081 章节		GB/T 25068.1 章节
12.2.1 恶意软件的控制	宜实现检测、预防和回复控制以防范恶意软件，并结合适当的用户意识教育。	8.7 恶意代码防范
12.2.1 a)	建立禁止使用未授权软件的正式策略	8.2.2.2 网络安全策略
12.2.1 b)	实现控制（如应用程序白名单），以防止或发现未授权软件的使用；	8.6 入侵检测和预防
12.2.1 c)	实现控制（如黑名单），以防止或发现已知或可疑的恶意网站的访问；	
12.2.1 d)	建立防范风险的正式策略，该风险与来自或经由外部网络或在其他介质获取的文件和软件相关，该策略宜说明需采取的保护措施；	8.2.2.2 网络安全策略
12.2.1 e)	减少可能被恶意软件利用的脆弱性，如通过技术脆弱性管理；	8.3 技术脆弱性管理
12.2.1 f)	定期评审支持关键业务过程的系统软件和数据内容；宜正式调查存在的任何未批准的文件或未授权的修改；	9.2 网络技术安全架构及设计
12.2.1 g)	作为一项预防措施，或例行程序，宜安装和定期更新恶意软件检测和修复软件扫描计算机和介质，执行的扫描宜包括： 1）在使用通过网络或任何形式的存储介质得到的文件前，要扫描恶意软件； 2）在使用电子邮件和附件下载前，要扫描恶意软件；该扫描宜在不同的位置进行实施，例如，在电子邮件服务上、在台式机上以及进入组织网络时； 3）扫描网页的恶意软件；	8.5 网络审计日志和监视
12.2.1 h)	就系统上恶意软件的防护，定义规程和责任，并就恶意软件攻击，培训它们的使用、报告和恢复；	

表 A.1 根据 GB/T 22080、GB/T 22081 章节（续）

12.2.1 i)	为从恶意软件攻击中恢复，宜准备适当的业务连续性计划，包括所有必要的数据和软件备份以及恢复安排；	8.9 业务连续性管理
12.2.1 j)	实现定期收集信息的规程，例如订阅邮件列表或验证提供新恶意软件的 web 站点；	
12.2.1 k)	实现规程以验证与恶意软件相关的信息，并确保报警公告是准确的和有价值的；管理者宜确保可靠的来源（例如，声誉好的期刊、可信的互联网站或防范恶意软件的软件供应商）被用于区分虚假的和真实的恶意软件；所有用户宜了解欺骗问题，以及收到后如何处理；	
12.2.1 l)	隔离可能导致灾难性影响的环境。	
13.1.1 网络控制	宜管理和控制网络以保护系统和应用中的信息。	
13.1.1 a)	宜建立网络设备管理的责任和规程；	8.2 网络安全管理
13.1.1 b)	在合适的地方，网络的运行责任宜与计算机运行责任予以分离；	8.2 网络安全管理
13.1.1 c)	宜建立专门的控制，以保护在共用网络上或无线网络上流经数据的保密性和完整性，并且保护已连接的系统及应用（见第 10 章和第 13.2 章节）；为维护所连接的网络服务和计算机的可用性，还可能需要专门的控制；	所有控制在 11.技术主题—风险、技术设计和控制要素
13.1.1 d)	宜应用合适的日志生成和监视，以便能记录或检测到一些可能影响信息安全或与信息安全相关的活动；	8.5 网络审计日志和监视
13.1.1 e)	为优化对组织的服务和确保在信息处理基础设施中诸多控制的一致应用，宜紧密协调相应的管理活动；	8.2 网络安全管理
13.1.1 f)	宜鉴别网络上的系统；	8.4 鉴别和身份认证
13.1.1 g)	宜限制与网络的系统连接。	

表 A.2 GB/T 25068.1 章节

GB/T 25068.1		GB/T22081	
6	概述		
6.2	网络安全规划和管理	13.2.1	信息传输策略和规程
7.2	有关当前及规划网络的信息		

表 A.2 GB/T25068.1 章节（续）

7	识别安全风险和准备确定安全控制		
7.2.1	组织信息安全策略中的安全需求		
7.2.2	有关当前及规划网络的信息		
7.2.2.2	网络架构、应用及服务		
7.2.2.3	网络连接类型		
7.2.2.4	其他网络特征		
7.2.2.5	其他信息		
7.3	信息安全风险和潜在的控制区域		
8.2	网络安全管理	13.1.1	网络控制
8.2.2	网络安全管理活动		
8.2.2.2	网络安全策略	5	信息安全策略
		9.1.2	网络和网络服务的访问
8.2.2.3	网络安全操作程序		
8.2.2.4	网络安全合规性检查		
8.2.2.5	多组织网络连接安全条件		
8.2.2.6	远程网络用户安全条件文档		
8.2.2.7	网络安全事故管理	16	信息安全事件管理
8.2.3	网络安全角色与职责	7.2.1	管理责任
8.2.4	网络监视	12.4	日志和监视
8.2.5	网络安全评估		
8.3	技术脆弱性管理	12.6	技术脆弱性管理
8.4	鉴别和身份认证	9.2.4	用户的秘密鉴别信息管理
		9.3.1	秘密鉴别信息的使用
8.5	网络审计日志和监视	12.4	日志和监视
		12.7	信息系统审计的考虑
8.6	入侵检测和防御	13.1.2	网络服务的安全
8.7	恶意代码防御	12.2	恶意软件防范
8.8	基于密码的服务	10.1	密码控制
8.9	业务连续性管理	17	业务连续性管理的信息安全方面
9	网络安全设计和实现的指南		
9.2	网络技术安全体系架构、设计		
10	参考网络场景—威胁、设计技术和控制要素		
10.2	员工互联网访问服务		
10.3	增强性协作服务		
10.4	企业对企业的服务	13.2.1	信息传输策略和规程
10.5	企业对客户的服务	13.2.1	信息传输策略和规程
		14.1.2	公共网络上应用服务的安全保护
		14.1.3	应用服务事物的保护
10.6	外包服务		

表 A.2 GB/T 25068.1 分条款（续）

10.7	网络划分		
10.8	移动通信		
10.9	旅行用户的网络支持		
10.10	家庭和小型企业的网络支持		
11	“技术”主题 – 风险、设计技术和控制要素	13.1.1	网络控制
12	开发和测试安全解决方案	13.1.2	网络服务的安全
13	操作安全解决方案		
14	监视和评审解决方案的实施		

附 录 B
（资料性附录）
（安全管理）SecOPs 文档示例模板

1. 概述
   1.1 背景
   1.2 文档结构
2. 范围
   2.1 场所
   2.2 技术设施
      2.2.1 IT 环境
      2.2.2 网络架构
      2.2.3 场所 1
      2.2.4 场所 2
      2.2.5 场所 3
      2.2.6 外部连接
3. 安全策略
4. 组织信息安全
   4.1 概述
   4.2 安全管理架构和职责
      4.2.1 组织安全官
      4.2.2 副组织安全官
      4.2.3 组织信息安全官
      4.2.4 IT 支持团队（相关的）
      4.2.5 业务区域管理
      4.2.6 工作人员
      4.2.7 组织管理委员会
   4.3 信息安全事件和脆弱性报告
   4.4 SecOP 分布
   4.5 与外部合作团队有关的风险评估
   4.6 对外（第三方）访问的协议
   4.7 外包
5. 资产管理
   5.1 资产清单
   5.2 信息和其他资产的可接受使用
   5.3 信息分类
6. 人力资源安全
   6.1 最低人员安全，包括许可、需求
   6.2 条款和条件
   6.3 信息安全意识和培训
   6.4 纪律处分
   6.5 人员监督
   6.6 终雇佣止
   6.7 安全门禁卡/通行证
   6.8 对 IT 系统和网络环境的物理访问
7. 物理和环境安全

参考文献

[1] ISO/IEC 9595-8, Information technology — Open Systems Interconnection — The Directory: Publickey and attribute certificate frameworks

[2] GB/T 18794.1-2002，信息技术 开放系统互联 开放系统安全框架 第1部分：概述（ISO/IEC 10181-1: 1996，IDT）

[3] ISO 11166-2, Banking — Key management by means of asymmetric algorithms — Part 2: Approved algorithms using the RSA cryptosystem.

[4] GB/T 27909（所有部分），银行业务 密钥管理（零售）（ISO 11568 (all parts) ，MOD）

[5] ISO 11649, Financial services — Core banking — Structured creditor reference to remittance information

[6] GB/T 17901（所有部分），信息技术 安全技术 密钥管理（ISO/IEC 11770(all parts) ，IDT）

[7] GB/T 21081，银行业务 密钥管理相关数据元（零售）（ISO 13492,IDT）

[8] GB/T 17903-2008（所有部分），信息技术 安全技术 抗抵赖（ISO/IEC 13888 (all parts):2004，IDT）

[9] ISO/IEC 14516:1999, Information technology — Security techniques — Guidelines for the use and Management of Trusted Third Party services

[10] ISO/IEC 15288:2008, Systems and software engineering — System life cycle processes.

[11] GB/T 28454-2012，信息技术 安全技术 入侵检测系统给的选择、部署和操作（ISO/IEC 18043:2006,MOD）

[12] ISO/IEC TR 18044:2004, Information technology — Security techniques — Information security incident management

[13] ISO 21118, Information to be included in specification sheets — Data projectors

[14] ISO/PAS 22399:2007, Societal security — Guidelines for incident preparedness and operational continuity management

[15] GB/T 31496，信息技术 安全技术 信息安全管理体系实施指南（ISO/IEC 27003, IDT）

[16] GB/T 31497，信息技术 安全技术 信息安全管理 测量（ISO/IEC 27004,IDT）

[17] ISO/IEC 27039, Information technology — Security techniques — Selection, deployment and operations of intrusion detection systems (IDPS)

[18] ISO/IEC 27040, Information technology — Security techniques — Storage security

[19] IETF Site Security Handbook (RFC 2196), September 1997

[20] IETF IP Security Document Roadmap (RFC 2411), November 1998

[21] IETF Security Architecture for the Internet Protocol (RFC 2401), November 1998

[22] IETF Address Allocation for Private Internets (RFC 1918), February 1996

[23] IETF SNMP Security Protocols (RFC 1352), July 1992

[24] IETF Internet Security Glossary (RFC 2828), May 2000

[25] IETF Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing (RFC 2827), May 2000

[26] Special Publications NIST (800 series) on Computer Security

[27] NIST Special Publications (800-10) : Keeping Your Site Comfortably Secure: An Introduction to

Internet Firewalls, December 1994.