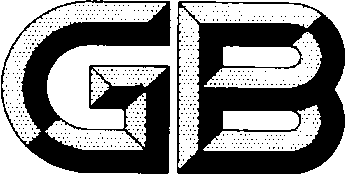
1. ICS 点击此处添加ICS号
2. 点击此处添加中国标准文献分类号



中华人民共和国国家标准

GB/T      —XXXX

|  |
| --- |
|  |

信息技术　安全技术 网络安全

综述和概念

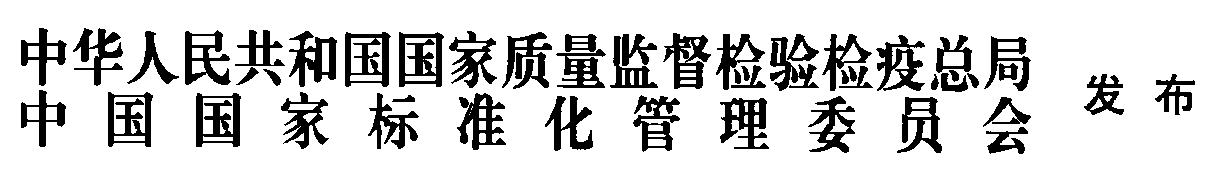
Information technology — Security techniques — Network security —Part 1:Overview and concepts

（ISO/IEC 27033-1:2015，IDT）

|  |
| --- |
| （草案） |
| （本稿完成时间：2017年7月11日） |

1. XXXX-XX-XX发布

XXXX-XX-XX实施



目　　次

[前　　言 3](#_Toc516365931)

[引　　言 4](#_Toc516365932)

[1. 范围 5](#_Toc516365933)

[2. 规范性引用文件 5](#_Toc516365934)

[3. 术语和定义 6](#_Toc516365935)

[4. 缩写 11](#_Toc516365936)

[5. 文档结构 13](#_Toc516365937)

[6. 概述 14](#_Toc516365938)

[6.1. 背景 14](#_Toc516365939)

[6.2. 网络安全规划和管理 15](#_Toc516365940)

[7. 识别安全风险和准备识别安全控制 17](#_Toc516365941)

[7.1. 简介 17](#_Toc516365942)

[7.2. 有关当前和/或规划网络的信息 17](#_Toc516365943)

[7.2.1 组织信息安全策略中的安全需求 17](#_Toc516365944)

[7.2.2.有关当前和/或规划网络的信息 17](#_Toc516365945)

[7.3. 信息安全风险和潜在的控制区域 20](#_Toc516365946)

[8. 支持控制措施 22](#_Toc516365947)

[8.1. 简介 22](#_Toc516365948)

[8.2. 网络安全管理 22](#_Toc516365949)

[8.2.1背景 22](#_Toc516365950)

[8.2.2网络安全管理行为 23](#_Toc516365951)

[8.2.4网络监测 25](#_Toc516365952)

[8.2.5网络安全评估 25](#_Toc516365953)

[8.3. 技术脆弱性管理 25](#_Toc516365954)

[8.4. 识别与认证 25](#_Toc516365955)

[8.5. 网络审计日志记录和监测 26](#_Toc516365956)

[8.6. 入侵检测和防御 27](#_Toc516365957)

[8.7. 恶意代码防御 27](#_Toc516365958)

[8.8. 基于加密的服务 28](#_Toc516365959)

[8.9. 业务连续性管理 29](#_Toc516365960)

[9. 网络安全设计和实现的指导原则 29](#_Toc516365961)

[9.1. 背景 29](#_Toc516365962)

[9.2. 网络技术安全架构/设计 29](#_Toc516365963)

[10. 参考网络场景—风险、设计、技术和控制问题 31](#_Toc516365964)

[10.1. 简介 31](#_Toc516365965)

[10.2. 员工互联网访问服务 31](#_Toc516365966)

[10.3. 增强性协作服务 31](#_Toc516365967)

[10.4. 企业对企业的服务 31](#_Toc516365968)

[10.5. 企业对客户的服务 32](#_Toc516365969)

[10.6. 外包服务 32](#_Toc516365970)

[10.7. 网络分段 32](#_Toc516365971)

[10.8. 移动通信 32](#_Toc516365972)

[10.9. 旅行用户的网络支持 33](#_Toc516365973)

[10.10. 支持家庭和小型企业的网络 33](#_Toc516365974)

[11. “技术”主题—风险、设计技术和控制要素 33](#_Toc516365975)

[12. 开发和测试安全解决方案 33](#_Toc516365976)

[13. 操作安全解决方案 34](#_Toc516365977)

[14. 监控和复审解决方案实施 34](#_Toc516365978)

**[附 录 A](#_Toc516365979)** [（资料性附录） ISO/IEC 27033本部分中安全控制部分同ISO/IEC 27001、ISO/IEC 27002标准中相关条款交叉引用 35](#_Toc516365979)

**[附 录 B](#_Toc516365980)** [（规范性附录） ISO/IEC 27033本部分中安全控制部分同ISO/IEC 27001、ISO/IEC 27002标准中相关条款对照表 39](#_Toc516365980)

[附 录 B （资料性附录） SecOPs文档示例模板 45](#_Toc516365981)

[参考文献 49](#_Toc516365982)

前　　言

新的标准体系替代原有标准体系的情况。

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、设计技术和控制问题；

——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

GB/T 25068-1取代了GB/T 25068-1:2010。

本部分按照GB/T 1.1-2009《标准化工作导则 第1部分：标准的结构和编写》给出的规则起草。

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：

本部分主要起草人：

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（见图1），其中，连接在一起的网络可能包括如下一个或多个：

——组织内部的网络；

——组织之间的网络；

——组织和公众之间的网络。

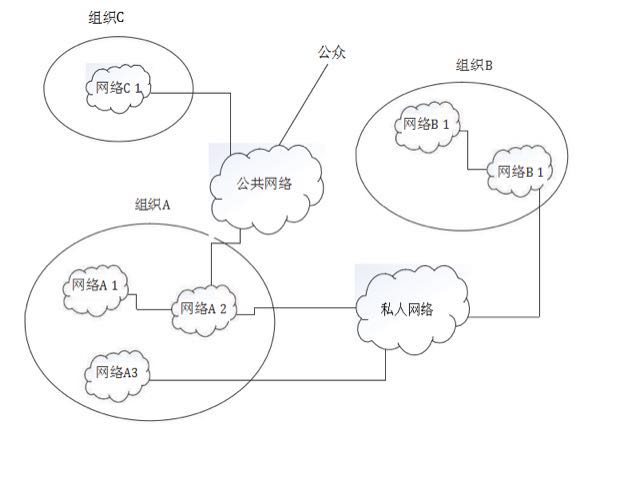


图1-典型的网络类型及连接方式

此外，快速发展的公共网络技术（特别是通过互联网发展起来公共网络技术）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，进而提供在线公共服务。这些商业机会从将互联网作为简单的连接媒介来提供低成本的数据通信到通过互联网服务提供商（ISP）提供更复杂的服务。这也就意味着，在电路的每一端使用相对低成本的本地连接，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。

这种环境既有利于获得重大商业利益，又存在新的安全风险。随着组织严重依赖于信息和相关网络，那么信息机密性、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。换句话说，实施和维护足够的网络安全对任何组织业务成功运行来说至关重要的。

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。适当时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，随着更多的产品组合起来以提供整体的解决方案，是否具备互操作性将决定解决方案成功与否。安全性不仅是每个产品或服务的关注点，还必须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。这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（ISO / IEC 27033其余部分详细介绍）。

——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（本文中，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，本部分标准也与参与到网络安全规划、设计和实施网络安全架构的人员有关（例如网络架构师和设计师，网络管理员和网络安全管理员）。

——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、设计人员、网络管理员和网络安全官有关。

——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，网络架构师和设计人员，网络管理员和网络安全人员）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，网络架构师和设计人员，网络管理员和网络安全人员）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，网络架构师和设计人员，网络管理员和网络安全人员）有关。

需要强调的是，本标准在国际标准ISO/ IEC 27002的基础上，对网络安全控制提供了进一步详细的实施指导。

信息技术 安全技术 网络安全 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南。（本文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）。

本标准的使用者包括拥有、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，对信息安全和/或网络安全、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，本标准的使用者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相关。

本部分还包括以下内容：

——提供了识别和分析网络安全风险，以及定义网络安全需求的指南（基于识别和分析的网络安全风险）；

——提供了支持网络技术安全体系结构的控制措施的概述，包括不仅仅适用于网络的非技术控制措施和技术措施；

——介绍了如何实现高质量的网络技术安全体系结构，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），简述了与实施和运营网络安全控制有关的问题，以及对其实施进行持续的监督和审查。

综上所述，它提供了GB/T 25068系列标准的概述和对所有其他部分的“路线图”。

1. 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 9387（所有部分）信息技术 开放系统互连 基本参考模型［ISO 7498（所有部分）］

GB/T 22080—2016信息技术 安全技术 信息安全管理体系要求 （ISO/IEC 27001:2013，IDT）

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

GB/T 31722—2015 信息技术 安全技术 信息安全风险管理 （ISO/IEC 27005:2008，IDT）

1. 术语和定义

为实现本文件的目的，在GB/T 16264、GB/T 22080、GB/T 22081、ISO / IEC 27005给出如下适用的术语和定义。



警报 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。



架构 architecture

一个系统的各组成部分、它们之间相互关系以及与环境的关系，以及指导其设计和演进原则的基本组织。

[GB 22032-2008，定义4.5]



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为目的的任何人。



审计日志 audit logging

复审、分析以及持续监控的有关信息安全事件的数据记录。



审计工具 audit tools

一种辅助分析审计日志内容的自动化工具。



认证机构（CA）certification authority

基于一个或多个用户信任来创建和分配公钥证书的机构。



信息安全总则 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。



非军事区域（DMZ） demilitarized zone

插在网络之间作为“中立区”的边界网络（也称为屏蔽子网）。



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降低的行为。



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。



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。



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。



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。



互联网 the Internet

公共域内互连网络的全球系统。



互联网络 internet

互连网络的集合成为一个互联网络或一个互联网。



内联网 intranet

组织成员利用互联网络协议和网络连接性安全地分享部分组织的信息和操作的私有计算机网络。



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。



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信息：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 27039，2.15



入侵检测系统（IDS）intrusion detection system

用于识别某一企图、正在发生或已经发生的入侵，并可能对信息系统和网络中的入侵做出响应的技术系统。



入侵防御 intrusion prevention

积极应对以防止入侵的正式过程。



入侵防御系统（IPS）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。



恶意软件 malware

被专门设计用于损坏或中断系统，攻击机密性、完整性和/或可用性的恶意软件。



多协议标记交换（MPLS） multi protocol label switching

一种为内部路由选择而开发的技术，这种路由选择是通过将标签分配给单个的数据路径或数据流来实现的。这种技术还可以用来在一般路由协议机制底层进行连接切换。



网络行政管理 network administration

日常操作和网络管理过程，以及使用网络的资产管理。



网络分析仪 network management

用于观察和分析网络中信息流的软件或设备。



网元 network element

与网络连接的信息系统。



网络管理 network monitoring

对网络进行规划、设计、实施、运行、监视和维护的过程。



网络监视 network monitoring

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



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、规划和实践，并指出如何通过以上策略保护网络基础设施和服务。



网络嗅探器 network sniffer

用于捕获在网络中流动的信息的软件或设备。



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。



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。



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。



路由器 router

用于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。

注1：网络自身能够基于不同的网络协议。

注2：路由信息保存在路由表内。



安全域 security domain

遵从于共同安全策略的资产和资源的集合。



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。



垃圾邮件 spam

非请求电子邮件，其可携带恶意内容和/或欺诈消息。



欺骗 spoofing

假冒成合法的资源或用户。



交换机 switch

通过内部交换机制在网络设备之间提供连接的设备，其中通常在OSI参考模型的第2层或第3层处实现的交换技术。



信道 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：信道可以通过使用协议封装、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。



虚拟本地网络

物理网络内从逻辑角度创建的独立网络。

1. 缩写

3G 第三代移动电话系统（third generation mobile telephone system）

AAA 身份验证、授权和计费（authentication，authorization and accounting）

ACL 认证、授权和核算（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）

BPL 宽带电源线（broadband 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 呼叫线路标识符（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（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 拒绝式服务（denial of service）

DSL 数字用户线（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 实施指导（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 制造资源规划（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 私人自动分支（电话）交换（private automated branch (telephone) exchange）

PC 个人电脑（personal computer）

PDA 个人数据助理（personal data assistant）

PIN 个人身份证号码（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 冗余阵列的廉价磁盘（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（symmetric digital subscriber line）

SecOPs 安全操作程序（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电话的垃圾邮件（spam over IP telephony）

SSH 安全外壳（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（terrestrial trunked radio）

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 不间断电源供应（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）

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（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保护访问（Wi-Fi protected access）

1. 文档结构

GB/T 25068系列标准的结构或者“路线图”，如下图2所示。

注意，在图2中，实线表示GB/T 25068中各部分的自然层次。虚线表示在（a）第1部分至第3、4、5、6部分之间可能存在引用了有关安全风险方面信息的关系，以及（b）第2部分至第3、4、5、6部分可能存在引用了有关设计技术和控制要素信息的关系。此外，第3部分内容中涉及到的有关内容在第4、5、6部分进行了详细叙述，因此在第3部分不做赘述。

因此，对于从零开始的任何组织或准备对现有网络进行重大审查的组织，应首先使用第1部分的内容，然后再使用第2部分的内容，但在必要时应参阅第3到6部分中涉及的安全风险、设计技术和控制要素。

例如，一个组织正在考虑实施一个新的网络环境，包括使用IP聚合、安全网关和无线网络，以及使用网络托管和互联网（例如针对电子邮件和输出在线访问）。

在使用第1部分中描述的过程来确定新网络环境的安全风险时，组织将考虑同GB/T 25068其他相关部分信息相关的风险。例如，这些部分定义了涉及IP聚合、安全网关和使用无线网络，以及使用网络托管和互联网（例如针对电子邮件和输出在线访问）的特殊安全风险（连同设计技术和控制问题）

在使用第2部分确定所需的网络技术安全架构时，组织将参考GB/T 25068其他相关部分的设计技术和控制要素的信息，即定义具体设计技术和控制要素的信息为安全风险的部分，涉及IP聚合、安全网关和使用无线网络，以及使用网络托管和互联网（例如针对电子邮件和输出在线访问）。

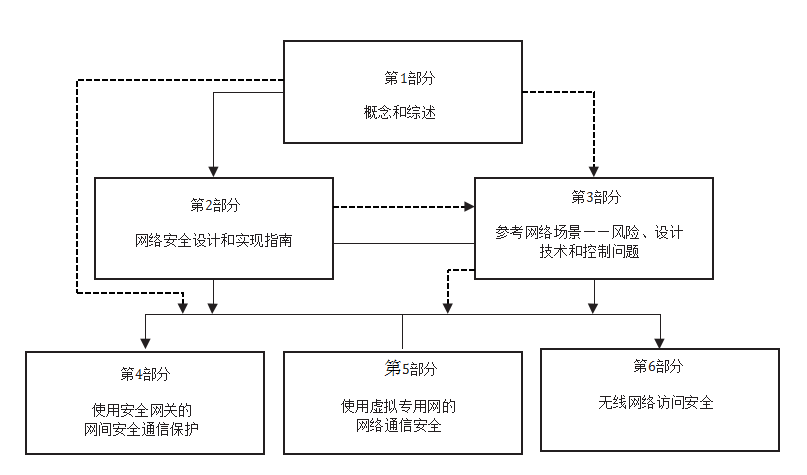


图2 GB/T 25068“路线图”

本部分标准的结构包括：

• 网络安全方法概述（详见第6条）；

• 识别网络相关风险和准备识别安全控制过程的总结，例如，建立网络安全要求（详见第7条）；

• 关于支持网络安全技术架构及其相关技术控制的概述，即不仅适用于网络的其他控制（非技术和技术）（详见第8条）；

• 介绍了如何通过使用一致性方法和辅助模型/框架规划和设计网络安全，从而实现高质量的技术安全架构，这将确保网络安全适用于组织的业务环境，（详见第9条）；

• 介绍了同参考网络场景相关的特定风险、设计、技术和控制要素（即对GB/T 25068-3内容的介绍）（见第10条）；

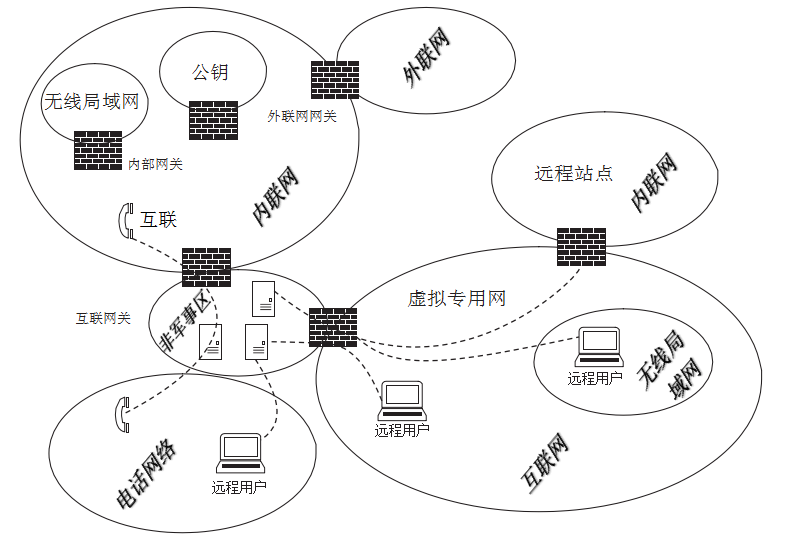
• 介绍了同网络技术主题相关的特定风险、设计技术和控制要素（即ISO / IEC 27033-4、27033-5、27033-6和其他可能的未来部分的介绍）（见第11条和附件A）；

• 介绍了与开发、实施和测试网络安全解决方案（详见第12条），操作网络安全解决方案（详见第13条）以及正在进行的网络安全实施监控和复审相关的问题（详见第14条）；

• 以表格形式表述了ISO / IEC 27001/27002中有关网络安全控制的条款和ISO / IEC 27033-1子条款之间交叉引用的表格，见附件A。

1. 概述
   1. 背景

目前，许多组织中常见的网络环境如图3所示。（图3仅仅是为了说明本概述的目的，并非用于任何其它用途。）



远程用户

IP语音

图 3 ―典型联网环境

内联网指的是组织内部依赖和维护的网络。通常情况下，只有组织的工作人员才有该网络的直接物理访问权。由于网络位于该组织拥有的场所内，因此可以轻易地实现一定程度的物理保护。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，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。这类基础设施，例如公开密钥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，例如公钥基础设施环境的基本部分，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认证，因为它们引入了额外的风险。对于这两种情况，内部安全网关可以用来进行逻辑隔离。

当今，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。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引入的风险。

公共网络，其中互联网是最常见的示例，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设施，并且提供内联网各种形式的扩展。由于在公共网络（特别是因特网）中的低信任级别，需要复杂的安全网关来帮助应对相关联的风险。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以及合作伙伴和客户对于网络连接需求。

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网络电话（VoIP）技术来实现内部电话网络时，通常还需要在电话网络中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，它们可以引起关注，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并不是天生安全的。全球环境中，大量人员具有访问底层机制和协议的能力、知识和倾向，并制造网络安全事件，包括未授权的访问，甚至于全面的破坏性拒绝服务。

* 1. 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/上下文，然后评估安全风险：

—收集关于当前和/或计划的网络环境的信息。

—复审公司信息安全策略。这些策略中的网络安全相关风险往往被过分关注，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策略。

—需知此策略还应包含组织对遵守法律法规的立场，这就包括：1.有关监管机构或立法机构（包括国家政府机构）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。

—收集和复审关于当前和/或计划的网络（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、威胁和漏洞（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审查，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条）。（1.评估潜在违反相关监管或立法机构（包括国家政府机构）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.使用默认潜在的负面业务影响，确保在网络上存储或传输的敏感./分类信息）。

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

c) 复审技术安全架构/设计选项，在考虑网络情景和“技术”主题的同时，选择和记录最优的技术安全架构/设计和相关的安全控制策略（见第9至11条）。（需要注意的是，这将包括相关监管机构或立法机构(包括国家政府机构)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条）。

e) 实施和操作安全控制（见第13条）。

f) 监测和复审实施情况（见第14条）。

—应定期进行复审，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。

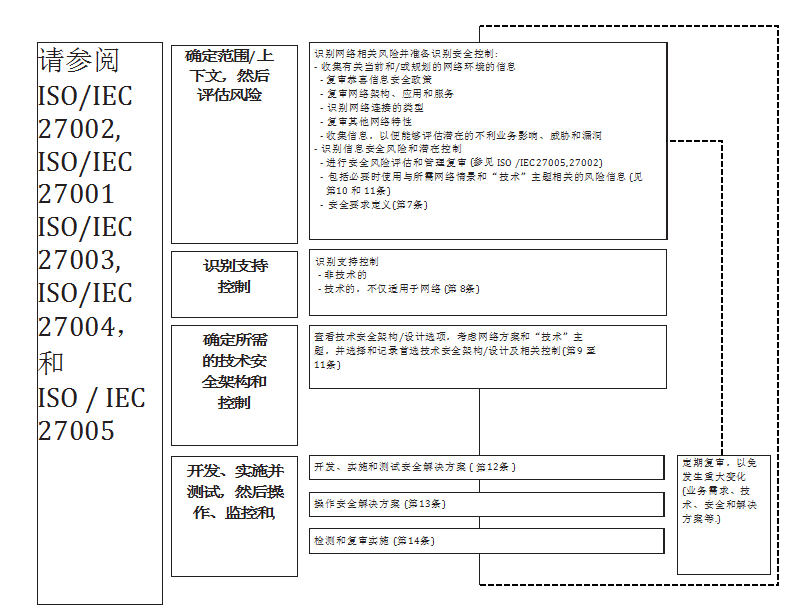


图 4 ― 网络安全规划和管理过程

应强调的是，在整个过程中，应适当参考ISO / IEC 27001、ISO / IEC 27002和ISO / IEC 27005，包括关于识别安全控制的一般建议。本标准是对这些标准的补充，并依据GB/T 25068-2到6的内容，介绍了如何识别适当的网络安全控制策略。

1. 识别安全风险和准备识别安全控制
   1. 简介

如上文第6条所述，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和/或规划的网络环境的信息，以下第7.2节为此提供了指导。下一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。以下第7.3节提供了这方面的有关指导。

* 1. 有关当前和/或规划网络的信息

7.2.1 组织信息安全策略中的安全需求

组织（或社区）的信息安全策略可以包括关于需要保密性、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，以及无论评估风险如何都需要实施的网络安全控制策略。因此，第一步应该是审查公司信息安全策略，以了解所有一直被视为高度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Internet的连接都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审查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。

关于信息安全政策的指导在ISO / IEC 27002和ISO / IEC 27005中给出。

7.2.2.有关当前和/或规划网络的信息

7.2.2.1简介

下一步应该是收集和审查关于当前和/或规划的网络—架构、应用、服务、连接类型和其他特性的信息—这将对识别和评估风险，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

应获取相关的当前和/或计划的网络架构、应用程序和服务的详细信息，并对其进行复审，以便为进行网络安全风险评估、管理复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和/或规划中实际环境的要求，那么在早期阶段应对网络架构、应用和服务进行复审和必要地修订。

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。

（一些资源也将属于城域网（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，存在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，关于技术安全的内容被分到ISO/IEC 27040 存储安全中介绍）。

不同的协议具有不同的安全特性，应该给予特殊考虑。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，示例为以太网；
* 为允许进入网络而设计的访问控制协议，示例为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；
* 许多运营商网络所基于的多协议标签交换（MPLS）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措施；
* 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认证。通常这是在应用框架本身内完成的，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，这些控制措施可能还不够。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。

还应在安全性的环境中考虑网络服务类型（例如，DNS、电子邮件和语音等）。

在复审网络架构、应用和服务时，还应考虑到已有的组织/社区内部或组织/社区内部与外部往来的网络连接，甚至是计划的网络连接。组织/社区的现有连接可以由于协议或合同的变更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，并且因此可能引入更高的风险，由此可能需要更强的和/或附加的控制。

7.2.2.3.网络连接类型

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（对其限制到已知团体的访问）实现，一些连接可以通过公共网络（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，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。

按照业务需求，将通用网络连接类型分类如下：

−在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。大多数（如果不是全部）用户能够访问可用的信息系统，但是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链路，而不是通过组织维护的网络链接；

−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，这种连接将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，包括连接组织的用户，都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访问数据库、网站和/或电子邮件设施（例如，通过因特网）的访问；

−从IP网向公共电话网的连接，其中从IP网络中的电话向PSTN发起接入。这种连接是不受控制的，因为从世界上的任何位置都接收此呼叫。

无论使用什么分类方法，都应当复审当前和/或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

复审当前和/或计划网络的其它特征。另外，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），这极其重要的。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（多协议标签交换）网络；

• 这与MPLS网络是否支持 QoS也有关系。（QoS能够提供稳定的性能，具有可靠性和可用性。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，还是需要之时再建立连接。

一旦确定当前和/或计划网络的特征，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复审投入。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：

－未知用户群，使用公共网络；

－封闭的业务群中的已知用户群，使用公共网络；

－组织内部唯一的已知用户群，使用公共网络；

－未知用户群，使用私人网络；

－封闭行业群中的已知用户群，使用专用网络；

－组织内部唯一的已知用户群，使用专用网络。

无论采用哪种复审方法，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，最终决定采用哪一种网络连接方法。

7.2.2.5其他信息

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，并能提高复审的重点和效果。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复审时应考虑的事情：

−信息类型；

−业务进程；

−实际的或可能的硬件组件、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条款结合起来，应用于网络安全风险评估和管理复审，其活动总结在7.3条款中，如下所示。

* 1. 信息安全风险和潜在的控制区域

正如之前预料的一样，现在大多数机构依赖于使用网络、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，对于每个机构所在地信息系统的访问以及对机构其他场所内网和外网的访问有着明确的业务需求边界，这种访问包括面向公众的和来自于公众的。当与第三方网络连接时，我们需要极其小心以确保连接机构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另一端的网络连接。

还有一些风险可能与遵守相关法律和法规的过程有关。（尤其要注意隐私和数据保护法律。一些国家对个人数据收集、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，根据各个国家法律，将对通过网络收集、处理和传播个人信息进行追责，甚至可能限制数据转移到特定国家，这些都会产生重大的安全隐患。对一些硬件和IP地址来说，这些不太明显的数据也适用于该法律。）

因此，面临的风险可能涉及对信息的未授权访问、未授权信息发送、引入恶意代码、拒绝接收或起源、拒绝服务连接和无法获得信息和服务。这些可能造成如下损失：

•（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）的抗抵赖性；

•网络交易的可核查性；

•信息（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，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，如下图5所示。

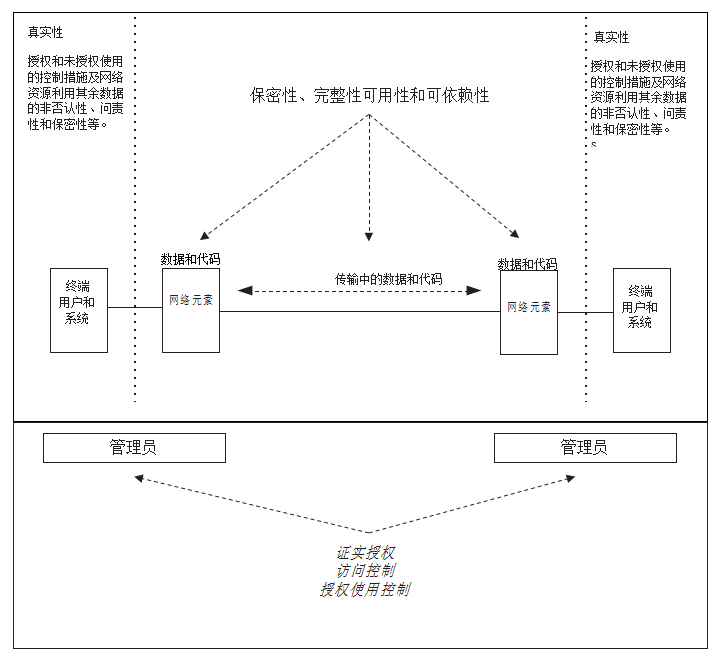


图 5 ― 网络安全风险区域的概念模型

因此，应根据ISO/IEC 27001、27002和27005提供的指导，进行网络安全风险评估和管理复审，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件所造成的负面影响。（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能够利用的漏洞的严重性或级别；

－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漏洞的等级进行制定；

－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。（这实际上是上图4“确定范围/情境并评估风险”及其相关图“确定网络相关风险和准备确定安全控制”的扩展图。）

图6的前两排方框名为“建立审查界限/范围”和“资产确认”，表明这是准备性活动。下两排方框是风险评估活动，最后两排是信息安全控制筛选和（其他）风险接受活动。

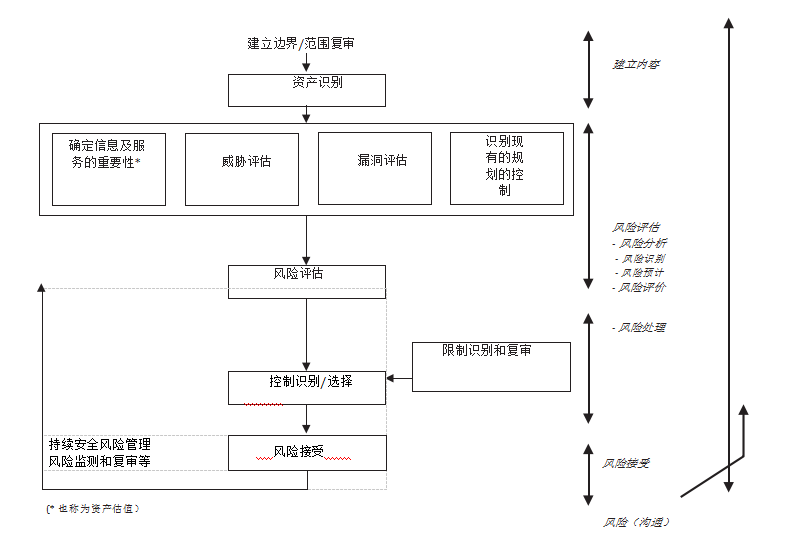


图6-网络安全风险评估和管理过程

ISO 27001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ISO/IEC 27001、ISO/IEC 27002及ISO/IEC 27005。应强调的是，在进行此类审查时，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(参见下文第10和11条，以及ISO / IEC27033第3至6部分)。

1. 支持控制措施
   1. 简介

本部分概述了支撑网络安全技术架构和其相关技术控制措施，这些相关的技术控制措施不仅仅适用于网络（非技术和技术方面）。GB/T 22080-2016、GB/T 22081-2016 和 ISO/IEC 27005上可以找到很多这类的控制措施信息。这些对网络使用来说至关重要的控制措施将在下述8.2至8.9中进行阐述，分别为网络安全管理（网络安全管理活动、网络安全角色和责任、网络监测和网络安全评估）、技术漏洞管理、识别和验证、网络审计日志记录和监测、入侵检测、恶意代码防护、密码加密服务和企业连续性管理。可以查阅GB/T 22080-2016、GB/T 22081-2016 和 ISO/IEC 27005中的相关内容。

* 1. 网络安全管理

8.2.1背景

总的来说，网络安全管理应在一个安全方式下开展，且在适当考虑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措施，其中大部分控制措施可以在GB/T 22081-2016和ISO/IEC 27005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网络安全管理行为

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行为的支持，包括对网络安全实现及运行的创建和控制。这些行为要确保组织/社区内的所有信息系统的安全。网络安全管理行为应包括：

－定义所有与网络安全有关的责任，并指定一名对网络安全负总责的管理者；

－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；

－网络安全事件管理方案；

－建档并测试业务连续性/灾难恢复计划；

可通过查阅 GB/T 22081-2016、 ISO/IEC 27005和 ISO/IEC 27035获取详细的专题信息。以上内容对于使用下述条款中深入指南来说尤为重要。

8.2.2.2网络安全策略

管理的职责在于易于接受并能支持机构的网络安全政策（正如GB/T 22081-2016所述）。网络安全政策应源于机构的信息安全政策并与之一致。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。）

网络安全的策略的内容通常应包括对网络安全风险评估和管理复审结果的概述（对控制措施的花费给以解释），包括选中的、与评估风险相当的所有安全控制措施的细节（参见上述7.3条款）。

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。附件C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措施中列出全面的检查清单：

－网络安全策略；

－相关的安全操作规程；

－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主要的新发布之前（与重要的业务或网络变更相关），否则每年进行一次。

这种检查应包括进行针对认可标准的安全性测试，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点扫描与渗透测试的组合。在任何检查开始之前，应检查测试计划以确保测试将以完全符合相关法律的方式进行。在执行这种检查时，不应忘记网络不可能仅限定于一个国家之内—它可能分布于具有不同法律的不同国家。该检查结束后，其报告应指出所遇到的脆弱性的细节和所需的修正及其优先级。

8.2.2.5多机构网络连接安全条件

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），可能就不受此法律约束。

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应生成该连接的安全条件文件，详述了B需提供的控制措施。这些控制措施应在B实施后，由组织签署绑定声明以确保安全性的效果。A将保留委托权或对B进行合规性检查。

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。该文件应说明用户所用硬件、软件、与网络有关的数据及其安全的责任。

8.2.2.7网络安全事件管理

使用网络的地方信息安全事件发生的可能性更大（与不使用网络的地方相比），对业务产生的不利影响也更严重。而且，尤其是与其它机构连接的网络发生安全事件时，很可能产生重大的法律后果。

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件时迅速做出反应，最大限度地减少其影响，并吸取教训，以防止再次发生。该方案应能够解决信息安全事件（识别系统、服务和网络状况中可能存在的违反信息安全政策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信息安全事件）。更详细的信息安全事件管理见ISO/IEC 27035。

8.2.3网络安全角色与责任

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；

－确保网络操作责任与电脑操作分开，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紧密跟踪威胁的演进（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，响应安全事件或警报等）。

网络用户：

－交流安全要求；

－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；

－针对网络安全效果提供反馈。

审计员（内部的和/或外部的）：

－复审和审计（例如，定期测试网络安全的效果）；

－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网络监测

网络监测是网络安全管理中非常重要的一个部分。下面8.5条中有论述。

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措施，包括安全测试-漏洞扫描等。安全应是评估新的网络技术和网络环境的主要考量。

* 1. 技术脆弱性管理

网络环境，与其它复杂的系统一样，不可能没有错误。具有已知的或已经被公开的技术脆弱性的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机密性。因此，技术漏洞管理目前应涵盖所有的网络组件并应包括：

－及时获取技术脆弱性的信息；

－评估此类漏洞的曝光；

－制定恰当的安全控制措施解决相关风险；

－执行和核验预定的安全控制措施；

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、固件或软件还有机构信息，例如负责管理人。

如果组织已成立了总体技术漏洞管理项目，把技术网络漏洞管理项目并入到总体任务中是优先方案。（关于技术漏洞管理更详细的信息，包括实施指南，可以在ISO/IEC 27002中找到。）

* 1. 识别与认证

限制授权人员通过连接进行访问非常重要（无论是组织内还是组织外的）。例如，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是策略的普遍要求。对这些连接的要求并不专指网络连接，因此可以通过使用GB/T 22081-2016 和 ISO/IEC 27005获得网络使用的适当细节。

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另外的安全控制措施合理的解决网络本身固有的问题，例如，不允许使用远程访问账户直接访问系统和网络软件，除非有提供附加的验证（如下）——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。

－加强验证。使用用户身份/密码匹配是验证用户的简便方法，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验证用户，尤其是远程访问用户和/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，通过手提电脑）。最简单的方法是使用主叫线路识别（CLID）（但由于其易被冒用，因此CLID在无法进一步验证的情况下不会被用于验证ID），通过调制解调器在不使用时断开连接，仅在调用者身份验证后才进行连接。更复杂但更安全的方法，尤其是在远程访问情境下，使用其它的识别方式支持用户验证，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验证账户时起作用（最好，用户的电脑和位置/访问点标识），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验证。

－安全单点登录——涉及用户的网络很可能遇到多次识别和验证核查。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验证数据。安全单点登录可以通过减少用户牢记密码个数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帮助台工作负载。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有风险并打开了入侵的大门（有时候，称为“打开王国的钥匙”风险）。它比一般的识别和验证机制更强，因此很有必要，且通过安全单点登录可以让识别和验证系统达到更高的安全级别（系统级别）。

* 1. 网络审计日志记录和监测

通过审计日志记录和持续监测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故不会发生。

充分的记录错误审计日志信息以及有效的事件以确保对可疑或实际发生的网络安全事故进行彻底地复审。然而，要识别如此多的审计记录相关的信息，不仅分析起来很困难，而且会影响性能，因此我们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：

－远程失败登录尝试的日期和次数；

－重验证失败（或标识使用）事件；

－安全网关通信流违规；

－远程尝试访问审计日志；

－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进行预警。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。

需要强调的是，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（包括标识和身份验证以及访问控制）。持续监测涵盖的范围包括：

－防火墙、路由器、服务器等的审计日志；

－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；

－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不可抵赖性。因此，所有的审计日志应恰当保护，包括对指定日期的存档CD进行销毁。根据公司要求和国家法律，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，实施网络监测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，在实施任何监测之前应通知所有的用户）。总之，监测应本着负责的态度，而不是利用某国隐私法的不健全去查看员工的行为。显然，采取的网络监测行为应与所在组织/机构的安全和隐私策略相一致，处理相关责任时，程序恰当。如果犯罪或民事诉讼中使用审计日志证据，实施网络日志记录和监测时还应更加谨慎。

关于网络使用的大多数审查记录和监测控制以及相关的信息系统可以根据ISO/IEC 27002 和 ISO/IEC 27005的使用而定。

* 1. 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，这些攻击者变得更加狡猾，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识别和验证能力、逻辑访问控制能力、计算审查控制能力以及入侵监测和防御能力得以解决。这种能力能够预测入侵、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，以及后续的整合并分析，就如同分析组织正常信息系统行为/使用模式一样。

IDS监听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：监测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：通过监测安全事件日志或检查系统变化实现监测主机（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。

* 1. 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、信息破坏和/或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，要确保扫描软件总是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，要求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链接时，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护请参见GB/T 22081 和 ISO/IEC 27005。

* 1. 基于加密的服务

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措施以保护网络连接上的信息。数字签名控件可以为消息认证控件提供类似的保护，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（不可抵赖），应该考虑如下控制措施：

－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的顺序的协议。

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）。信息的发送方，在要求源证据时，应使用数字签名把信息封装到普通标准中，在要求交付证据时，发送方应请求使用数字签名封装的答复。

ISO/IEC 18033对加密机制进行了标准化。一种常用的，被称为块密码的加密技术，ISO/IEC 10016标准化了使用块密码进行加密保护的方式(称为操作模式)。在ISO / IEC 9797中对被称为消息认证码(或mac)的消息完整性控制进行了标准化。ISO /IEC 9796和GB/T 17902对数字签名技术进行了标准化。更多与不可抵赖性有关的信息请参见ISO/IEC 14516和ISO/IEC 13888。

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。对于密钥管理信息以及相关话题，诸如PKI或身份管理、查阅的更多话题应制定其它文件和标准，参见下列标准：

− GB/T 17901：密钥管理；

− GB/T 16264.8 ：目录 公匙与属性证书框架；

− 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。

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。

* 1. 业务连续性管理

重要的是要制定控制措施，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被中断业务的各个部分的能力。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——业务影响分析复审、风险评估复审、业务恢复需求确立、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；

－被识别的推荐业务连续性策略选项与优先级和时间安排匹配；

－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、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。虽然互联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。

1. 网络安全设计和实现的指导原则
   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条为网络场景提供了风险、设计技术和安全控制区域提供了参考。第11条为当前组织关注的特定技术热点提供有关风险、设计技术和安全控制问题的参考。第10条和第11条介绍了一种特别的网络安全解决方案，包括多样的主题和控制区域。附录B中有关于 ISO/IEC 27001/27002网络安全相关控制措施和ISO/IEC 27033-1条款交叉引用的表格。

依据第8条到第11条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措施列表进行详细复审。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（详见第12条）。一旦技术安全架构和安全控制措施生效，就应开始实施实时的的持续监测和执行审查（详见第14条）。

* 1. 网络技术安全架构/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，账户应满足组织所有的安全策略要求（见条款7.2.1如上），包括相关网络架构、应用服务、连接类型、其它特征（见7.2.2条）和安全风险评估与管理审查确认的潜在控制清单（详见7.3条）。账户必须满足现有的技术安全架构/设计才能实现。一旦选项被选中并复审，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/行业标准化的服务要求；

－所有现存或计划的架构、设计和执行文件；

－当前的网络安全政策（信息系统安全相关政策），在安全风险评估和管理复审结果基础上优先选择；

－定义受保护资产；

－当前和规划性能要求包括相关流量要求；

－当前的产品信息；

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，ISO/IEC 27033-2中有详述，其中附录D也包含服务访问要求文件模板（ISO/IEC 27033-2）。其它文件的更详细的信息参见上面8.2.2条款和ISO/IEC 27033-2。

（接下来，一旦要求的网络技术安全架构/设计已被记录和执行，那么安全测试规划和安全测试也应运而生。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（详见第12条））

下面每个活动的信息都记录于 ISO/IEC 27033-2 ：

－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/行业广义上的网络需求；

－复审现有的和/或计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/行业的功能需求相一致）

－资产识别/确认；

－确认安全风险评估和管理结果，并依据结果复审现有以及计划的网络安全控制措施，选择潜在的安全控制措施；

－复审网络性能要求并确认基准（复审性能需求、消除疑虑以及性能基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ISO/IEC 27001:2007中的条款相对应）；

－使用场景和技术指导（ISO/IEC 27033-3到 27033-6有叙述）（同样，详见第10条和第11条）；

－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、扩展性、管理设施、逻辑安全，当然还有供应商的能力、业绩记录等）；

－概念验证（在网络技术安全架构和相关产品集还未就位前，和/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措施应如何测试。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ISO/IEC 27033-2中有描述。而且，可参考27033-2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措施列表之前，应完全记录并批准所有项目的技术安全架构/设计。

1. 参考网络场景—风险、设计、技术和控制问题
   1. 简介

这一系列标准的第三部分描述了与参考网络场景有关的风险、设计技术和控制问题。下面10. 2 到 10.10节中介绍了一些场景的例子。第三部分不仅提供了详细的安全风险和安全设计技术指导并提供了减少所有特定场景下要求的控制措施。第三部分包括第四部分到第六部分的引述，以避免文档内容重复。

* 1. 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，因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，是如 www（http和https）之类的基本服务？是只允许信息检索和员工参与的聊天频道、论坛？还是允许增强协作服务？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。即使有限制政策，员工访问网络还是会带来大量的安全风险。

* 1. 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；

−将其作为内部服务和组织外部的服务使用。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，或者只是作为服务从第三方购买。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。针对内部以及内外部同时使用，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。

* 1. 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。

当使用因特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。

* 1. 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）、认证（当下可能使用的方法，例如两个因素，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的环境；

−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）。

* 1. 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，和/或使用其他外包服务。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，特别是在事件管理场景中。

* 1. 网络分段

对许多国家，特别是联邦或组织型国家而言，特定的立法对信息安全要求有很大的影响。国际组织通常在许多不同国家开展业务，因此有义务遵守各个国家的特定立法，这可能进一步要求组织需满足每个国家的信息安全要求。例如，特定国家的立法可能需要对客户数据进行特定保护，且不允许将此类数据传输到另一个国家。这通常需要采取额外的信息安全控制，以确保遵守此类立法。

为了满足某个国际组织在不同国家开展业务的信息安全要求，实施与国家边界一致的网络分段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。

* 1. 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ISO /IEC 27033-6关于IP无线网络安全通信安全中有所阐述）。

消费市场上个人移动通信设备的快速发展催生出一些也可以用于商业环境新特点。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业务机会，原有专属于商业市场的设备也被引入消费市场。这类设备可用的新功能中，设备存储器能力的增长、公共开放因特网的永久在线连接，以及人们出于私人和商业目的使用相同设备的情况，意味着面临更大的安全风险。

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。

* 1. 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了新的风险，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策略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。

* 1. 支持家庭和小型企业的网络

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的成本有限，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。

1. “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。

1. 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”测试应该率先进行，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。

合规性审查应在日常运营之前完成。当所有缺陷已被确定、修复并由高级管理层签署后，审查即已完成。

应强调的是，这应包括对相关公认的国家、政府、行业标准（在没有国际标准的情况下）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。这应包括漏洞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和法规完全兼容。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（包括高级管理层）并接受执行。

1. 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执行日常运营，安全测试已经得到实施，并预先完成相关的必要操作。换句话说，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复审（见下文第14条）。

1. 监控和复审解决方案实施

在日常运营实施后，应根据相关公认的国家、政府和社区的标准（在没有国际标准的情况下）开展持续监测和合规性复审。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条所述的模式。

附 录 A   
（资料性附录）  
ISO/IEC 27033本部分中安全控制部分同ISO/IEC 27001、ISO/IEC 27002标准中相关条款交叉引用

|  |  |  |  |
| --- | --- | --- | --- |
| 27001/27002 分条款 | | 27033-1 分条款 | |
| 12.2.1.控制恶意软件 | 1. 应适当结合用户的意识，并实现检测、预防和恢复，去控制、防止恶意软件的出现。 | 1. 8.7 | 1. 防范恶意代码 |
| 12.2.1 a) | 1. 制定禁止使用未经授权软件的正式政策（策略？） | 1. 8.2.2.2 | 1. 网络安全策略 |
| 12.2.1 b) | 1. 实施控制以防止或发现未经授权的软件的使用（例：应用白名单） | 1. 8.6 | 1. 入侵检测和预防 |
| 12.2.1 c) | 1. 实施控制以防止或发现已知或可疑的恶意网站的使用（例：黑名单） |  |  |
| 12.2.1 d) | 1. 制定一项正式x策略，说明应采取何种保护措施以防范从外部网络或其他媒介获取文件和软件的风险 | 1. 8.2.2.2 | 1. 网络安全策略 |
| 12.2.1 e) | 1. 减少恶意软件可以利用的漏洞，例，通过技术脆弱性管理 | 1. 8.3 | 1. 技术脆弱性管理 |
| 12.2.1 f) | 1. 对支持关键业务流程的系统软件和数据内容进行定期审查；任何未经批准的文件或未经授权的修改均应收到正式调查 | 1. 9.2 | 1. 网络安全技术架构/设计 |
| 12.2.1 g) | 1. 安装并定期更新恶意软件的检测和修理软件，将扫描计算机及媒体作为预防管理，或例行基础，进行的扫描应包括： 2. 1）在使用前，扫描任何通过网络或任何形式的中转介质接受到的文件是否含有恶意软件 3. 2）在使用前，扫描电子邮件，附件及下载的文件是否含有恶意软件，以上扫描应在不同的地方（分区？），例，在电子邮件服务，计算机桌面和进入组织网络时 4. 3）扫描网页是否含有恶意软件 | 1. 8.5 | 1. 网络审计日志记录和监测 |
| 12.2.1 h) | 1. 定义处理系统中的恶意软件保护程序和责任，对其使用和培训、报告和从恶意软件攻击中恢复 |  |  |
| 12.2.1 i) | 1. 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和恢复安排，以从恶意软件攻击中恢复 |  | 1. 8.9业务连续性管理 |
| 12.2.1 j) | 1. 程序实现定期手机信息，入订阅邮件列表，或验证关于新的恶意软件网站的信息 |  |  |
| 12.2.1k) | 1. 实现程序可验证与恶意软件相关的信息，并确保警示公告是准确并充足的；管理者应确保源头质量，例，著名期刊，可靠的互联网站点或供应商生产的软件可防止恶意软件，用于区分恶作剧软件和真正的恶意软件；所有用户都应意识到恶作剧软件的问题，以及在收到他们时应该怎么做； |  |  |
| 12.2.1 l) | 1. 隔离的环境，可能导致灾难性的影响。 |  |  |
| 13.1.1网络控制 | 1. 应该对网络进行管理和控制，以保护系统和应用程序中的信息 |  |  |
| 13.1.1a) | 1. 建立网络设备管理的责任和流程； |  | 1. 8.2网络安全管理 |
| 13.1.1b) | 1. 在适当的情况下，网络的操作责任应与计算机操作分开； |  | 1. 8.2网络安全管理 |
| 13.1.1c) | 1. 应设立特别管制措施，以保障通过公共网络或无线网络的数据的机密性和完整性，并保护联网系统和应用程序（详见10和13.2）；还可能需要进行特殊控制，以维持网络服务和计算机联网的可用性； |  | 1. 所有的控制在11.技术主题—风险，技术设计和控制问题 |
| 13.1.1d) | 1. 适当的日志和监控应该用于能够记录或检测可能影响或与网络安全相关的行为 |  | 1. 8.5网络审计日志和监控 |
| 13.1.1e) | 1. 管理活动应协调密切，以优化对组织的服务，并确保在信息处理基础设施中一致的应用控制 |  | 1. 8.2网络安全管理 |
| 13.1.1f) | 1. 网络系统应进行身份验证 |  | 1. 8.4识别和身份验证 |
| 13.1.1g) | 1. 联网系统应被限制 |  |  |

表A.2

|  |  |  |  |
| --- | --- | --- | --- |
| 27033-1 | | 27002 | |
| 6 | 14.1 综述 |  |  |
| 6.2 | 14.2 网络安全规划与管理 | 13.2.1 | 网络传输策略与规程 |
| 7 | 14.3 风险识别与准备识别安全控制 |  |  |
| 7.2 | 14.4 有关当前和/或规划网络的信息 |  |  |
| 7.2.1 | 14.5 组织信息安全策略中的安全需求 |  |  |
| 7.2.2 | 14.6 有关当前/规划网络的信息 |  |  |
| 7.2.2.2 | 14.7 网络架构、应用及服务 |  |  |
| 7.2.2.3 | 14.8 网络连接类型 |  |  |
| 7.2.2.4 | 14.9 其他网络特征 |  |  |
| 7.2.2.5 | 14.10 其他信息 |  |  |
| 7.3 | 14.11 信息安全风险和潜在的控制区域 |  |  |
| 8.2 | 14.12 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 | 访问网络和网络服务 |
| 8.2.2.3 | 网络安全操作规程 |  |  |
| 8.2.2.4 | 网络安全合规性检查 |  |  |
| 8.2.2.5 | 网络连接安全条件 |  |  |
| 8.2.2.6 | 远程网络用户安全条件文件 |  |  |
| 8.2.2.7 | 网络安全事件管理 | 16 | 信息安全事件管理 |
| 8.2.3 | 网络安全角色与责任 | 7.2.1 | 管理责任 |
| 8.2.4 | 网络监测 | 12.4 | 日志记录与监测 |
| 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 | 识别与认证 | 9.2.4 | 用户私密认证信息管理 |
| 9.3.1 | 私密认证信息用户 |
| 8.5 | 网络审计日志记录和监测 | 12.4 | 日志记录与监测 |
| 12.7 | 信息系统审计考量 |
| 8.6 | 入侵检测和防御 | 13.1.2 | 网络服务安全 |
| 8.7 | 恶意代码防御 | 12.2 | 恶意软件防护 |
| 8.8 | 基于加密的服务 | 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 |
| 9 | 网络安全设计和实现的指导原则 |  |  |
| 9.2 | 网络技术安全架构/设计 |  |  |
| 10 | 参考网络场景—风险、设计、技术和控制问题 |  |  |
| 10.2 | 员工互联网访问服务 |  |  |
| 10.3 | 增强性协作服务 |  |  |
| 10.4 | 企业的业务服务 | 13.2.1 | 信息传输策略和规程 |
| 10.5 | 企业的客户服务 | 13.2.1 | 信息传输策略和规程 |
| 14.1.2 | 公共网络上的安全应用服务 |
|  |  | 14.1.3 | 交易中的保护应用服务 |
| 10.6 | 外包服务 |  |  |
| 10.7 | 网络分段 |  |  |
| 10.8 | 移动通信 |  |  |
| 10.9 | 旅行用户的网络支持 |  |  |
| 10.10 | 支持家庭和小型企业办公室的网络 |  |  |
| 11 | “技术”主题 - 风险、设计技术和控制问题 | 13.1.1 | 网络控制 |
| 12 | 开发和测试安全解决方案 | 13.1.2 | 网络服务安全 |
| 13 | 操作安全解决方案 |  |  |
| 14 | 监控和审查解决方案实施 |  |  |

附 录 B  
（规范性附录）  
ISO/IEC 27033本部分中安全控制部分同ISO/IEC 27001、ISO/IEC 27002标准中相关条款对照表

表B.1 - ISO / IEC 27001和ISO / IEC 27002之间的相互参照，以及ISO / IEC 27033本部分中的条款

|  |  |  |  |
| --- | --- | --- | --- |
| ISO/IEC 27001 及ISO/IEC 27002 条款 | 规定 | ISO/IEC 27033-1 条款 | |
| 10.4.1针对恶意代码的控件 | 检测、预防和恢复控制，以防止恶意代码  并应实施适当的用户意识程序。 | 8.7防恶意代码 | |
| 10.4.2 针对移动代码的控件 | 在授权使用移动代码的情况下，配置应确保授权的移动代码根据明确定义的安全策略操作，并且应防止执行未经授权的移动代码。 | 7.2.2.2网络架构、应用和服务 | |
| 10.6.1-网络控件 | 应对网络进行充分管理和控制以免受威胁，并保持使用网络的系统和应用程序的安全性，包括传输中的信息。 | 参见ISO / IEC 27001/27002条款10.6.1 IG a至e）。 | |
| 10.6.1 IG a) | 在适当的情况下，网络的操作责任应与计算机操作分开。 | 8.2 网络安全管理。 | |
| 10.6.1 IG b) | 应建立远程设备管理职责和程序，包括用户区域的设备。 | 11.7远程访问服务。（更多详细信息，请参见ISO / IEC 27033-5。） | |
| 10.6.1 IG c) | 应建立特殊控制措施，以保护通过公共网络或通过无线网络传递的数据的机密性和完整性，并保护所连接的系统和应用程序（见11.4和12.3）。还可能需要特殊控制来维持网络服务和连接的计算机的可用性。 | 所有11中的控件，.技术主题——风险、设计技术和控制问题。 | |
| 10.6.1 IG d) | 应采用适当的记录和监测，以便记录安全相关的行动。 | 8.5网络审计日志和监控。 | |
| 10.6.1 IG e) | 管理活动应密切协调，以优化对组织的服务，并确保在信息处理基础设施中持续应用控制。 | 8.2网络安全管理。 | |
| 10.6.2 –网络服务安全 | 应确定所有网络服务的安全功能、服务级别和管理要求，并将其适用于所有网络服务协议，无论这些服务由内部提供还是外包。 | 8.2网络安全管理（以及第8条其他子条款和第9至11条）。 | |
| 10.8.1信息交换政策和程序 | 应建立正式的交换政策、程序和控制措施，以通过使用各种类型的通信设施来保护信息交流。 | 6.2网络安全计划和管理 | |
| 10.8.4电子信息 | 应当适当保护电子通讯中涉及的信息。 | A.11互联网电子邮件 | |
| 10.9.1电子商业 | 应该保护通过公共网络传递的电子商务中涉及的信息免受欺诈活动、合同纠纷以及未经授权的披露和修改。 | 10.4业务对业务服务  10.5业务到客户服务 | |
| 10.9.2线上交易 | 应当保护在线交易中涉及的信息，以防止不完全传输、错误路由、未授权的消息变更、未经授权的披露、未授权的消息复制或重发。 | 10.5业务到客户服务 | |
| 10.9.3公开信息 | 在公共可用系统上提供信息的完整性应该受到保护，以防止未经授权的修改。 | A.10 网络托管 | |
| 11.4.1网络服务使用政策 | 用户只能获得他们特别授权使用的服务访问权限。 | 8.2.2.2网络安全策略 | |
| 11.4.2外部连接的用户验证 | 应使用适当的身份验证方法来控制远程用户的访问。 | 8.4识别和认证 | |
| 11.4.3网络设备识别 | 自动设备识别应被视为认证来自特定位置和设备的连接手段。 |  | |
| 11.4.4远程诊断和配置端口保护 | 应控制对诊断和配置端口的物理和逻辑访问。 |  | |
| 11.4.5  网络隔离 | 信息服务、用户和信息系统组应在网络上隔离。 |  | |
| 11.4.6网络连接控制 | 对于共享网络，特别是跨越组织边界的那些共享网络，用户连接到网络的能力应当根据访问控制策略和业务应用的要求进行限制。 | 11. “技术”主题——风险、设计技术和控制问题 |
| 11.4.7网络路由控制 | 应该为网络实施路由控制，以确保计算机连接和信息流不会违反业务应用程序的访问控制策略。 | A.6安全网关 |

表 B.2 —ISO / IEC 27033和ISO / IEC 27001和ISO / IEC 27002本部分条款之间的交叉引用

|  |  |  |
| --- | --- | --- |
| ISO/IEC 27033-1条款 | 规定 | ISO/IEC 27001和 ISO/IEC 27002 条款 |
| 6 | 概述 |  |
| 6.2 | 网络安全计划和管理 | 10.8.1 信息交流政策和程序 |
| 7 | 识别风险并准备识别安全控制 |  |
| 7.2 | 有关当前/计划网络的信息 |  |
| 7.2.1 | 公司信息安全策略中的安全要求 |  |
| 7.2.2 | 有关当前/计划网络的信息 |  |
| 7.2.2.2 | 网络架构、应用和服务 | 10.4.2针对移动代码的控件 |
| 7.2.2.3 | 网络连接类型 |  |
| 7.2.2.4 | 其他网络特性 |  |
| 7.2.2.5 | Other Information 其他信息 |  |
| 7.3 | 信息安全风险和潜在控制区 |  |
| 8.2 | 网络安全管理 | 10.6.1 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 | 5.1 信息安全策略 |
|  |  | 11.4.1 网络服务使用政策 |
| 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 | 网络连接的安全条件 |  |
| 8.2.2.6 | 远程网络用户的文档化安全条件 |  |
| 8.2.2.7 | 网络安全事件管理 | 13信息安全事件管理 |
| 8.2.3 | 网络安全角色和职责 | 8.1.1角色和职责 |
| 8.2.4 | 网络监控 | 10.10监测 |
| 8.2.5 | 评估网络安全 |  |
| 8.3 | 技术脆弱性管理 | 12.6技术脆弱性管理 |
| 8.4 | 识别和验证 | 11.4.2外部连接的用户验证 |
|  |  | 11.5.2用户身份验证 |
| 8.5 | 网络审计日志和监控 | 10.6.1网络控制 |
|  |  | 10.10.1审核日志 |
| 8.6 | 入侵检测和预防 |  |
| 8.7 | 防恶意代码 | 10.4防范恶意和移动代码 |
| 8.8 | 基于密码的服务 | 12.3加密控制 |
| 8.9 | 业务持续性管理 | 14业务连续性管理 |
| 9 | 设计指南和网络安全的实现 |  |
| 9.2 | 网络技术安全架构/设计 |  |
| 10 | 参考网络方案——风险、设计技术与控制问题 |  |
| 10.2 | 员工互联网服务 |  |
| 10.3 | 增强协作服务 |  |
| 10.4 | 业务对业务服务 | 10.9.1电子商务 |
| 10.5 | 业务到客户服务 | 10.9.1电子商务 |
|  |  | 10.9.2 在线交易 |
| 10.6 | 外包服务 |  |
| 10.7 | 网络分段 |  |
| 10.8 | 移动通信 |  |
| 10.9 | 网络支持旅行用户 |  |
| 10.10 | 网络支持家庭和小型企业办公室 |  |
| 11 | “技术”主题——风险、设计技术与控制问题 | 10.6.1 网络控制 |
|  |  | 11.4.6网络连接控制 |
| 12 | 开发和测试安全解决方案 |  |
| 13 | 操作安全解决方案 |  |
| 14 | 监控和审查解决方案实施 |  |
| 附件 A | “技术”主题 - 风险、设计技术与控制问题 |  |
| A.1 | 局域网 |  |
| A.2 | 广域网 |  |
| A.3 | 无线网络 |  |
| A.4 | 无线电网络 |  |
| A.5 | 宽带网络 |  |
| A.6 | 安全网关 | 11.4.7网络路由控制 |
| A.7 | 虚拟专用网络 |  |
| A.8 | 语音网络 |  |
| A.9 | IP聚合 |  |
| A.10 | 网络托管 | 10.9.3公开信息 |
| A.11 | 互联网电子邮件 | 10.8.4电子信息 |
| A.12 | 路由访问第三方组织 |  |

附 录 B   
（资料性附录）  
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

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 与外部缔约方有关的风险评估

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，包括清关、要求

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 终止雇佣

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

7.1 物理和环境安全控制实施

7.2 物理安全边界

7.3 物理入口控制

7.4主要工作区

7.5 设备选址

7.6 密钥和组合

7.7 入侵检测报警

7.8 防盗设备防护

7.9 设备拆卸

7.10 硬件访问控制

7.11 篡改检测

7.12 维护和修复

7.13 供电安全

7.14 防火安全

7.15 水/液体安全

7.16 安全警报

7.17 PC安全

8. 通信和运营管理

8.1 操作规程和职责

8.1.1 变更控制程序

8.1.2 职责划分和责任领域

8.2 系统规划和验收

8.2.1 能力规划

8.2.2 系统验收

8.3 恶意代码和移动代码防范

8.3.1 防御

8.3.2 检测

8.3.3 修复

8.3.4 移动代码

8.4 备份和恢复

8.5 IT组件（包括网络）启动和关闭

8.6 媒体（包括文件）安全

8.6.1 可移动介质的管理

8.6.2 打印输出

8.6.3重复利用或介质处理安全

8.7 信息交换

8.8 监测

8.8.1 计费和审计

8.8.2 手动计费日志

8.8.3 时钟同步

8.9 操作日志

8.10 故障日志

8.11 IT和通信计划

9. 访问控制

9.1 用户账户管理

9.1.1用户账户请求

9.1.2 用户账户创建

9.1.3 审查、禁用和删除用户账户

9.2 访问控制配置

9.3 密码管理

9.3.1 控制和实施

9.3.2 密码生成

9.3.3 密码存储和传输

9.3.4 更改密码

9.3.5 密码审查

9.3.6 密码维护

9.3.7特权用户/系统管理监控密码

9.4 访问安全令牌

9.5 网络访问控制

9.5.1 概述

9.5.2 外部连接

9.6 连接的安全条件

9.7 远程访问

9.8 操作系统、应用和信息、访问控制

9.9 移动计算和远程工作

9.9.1 概述

9.9.2 笔记本电脑安全

9.9.3 掌上电脑安全

10. 信息系统采购、开发和维护

10.1 系统文档安全

10.1.1 操作软件控制

10.1.2 系统测试数据保护

10.1.3 源代码保护

10.2 开发和技术支持过程中的安全

10.2.1 系统和应用软件完整性

10.2.2分包/外包软件开发

10.3 软件维护

10.4 软件故障日志

10.5 技术脆弱性管理

11. 信息安全事件管理

11.1信息安全事件管理和漏洞

11.2 IT（包括网络）故障

12. 业务连续性管理

12.1 业务连续性计划

12.2 备份程序

12.3 紧急情况和故障

12.3.1 硬件故障

12.3.2 软件故障

12.3.3 消防/建筑疏散

13. 合规

13.1 遵守法律要求

13.2 遵守信息安全政策和标准以及技术合规性

13.3 系统审计工具的保护

14. 文档配置

14.1 反馈

14.2 Secop的变更

附录A - 参考文献

参考文献

1. ISO/IEC 7498-1:1994, *Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model*[S].
2. ISO/IEC 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Security Architecture*[S].
3. ISO/IEC 7498-3:1997, *Information technology — Open Systems Interconnection — Basic Reference Model: Naming and Addressing*[S].
4. ISO/IEC 7498-4:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Management Framework*[S].
5. ISO/IEC 9595-8, *Information technology — Open Systems Interconnection — The Directory: Publickey and attribute certificate frameworks*[S].
6. ISO/IEC 10181-1: 1996, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Overview*[S].
7. ISO 11166-2, *Banking — Key management by means of asymmetric algorithms — Part 2: Approved algorithms using the RSA cryptosystem*[S].
8. ISO 11568 (all parts), *Banking — Key management (retail)* [S].
9. ISO 11649, *Financial services — Core banking — Structured creditor reference to remittance information*[S].
10. ISO/IEC 11770 (all parts), *Information technology — Security techniques — Key management*[S].
11. ISO/IEC 11889-1, *Information technology — Trusted Platform Module — Part 1: Overview*[S].
12. ISO/IEC 11889-2, *Information technology — Trusted Platform Module — Part 2: Design principles*[S].
13. ISO/IEC 11889-3, *Information technology — Trusted Platform Module — Part 3: Structures*[S].
14. ISO/IEC 11889-4, *Information technology — Trusted Platform Module — Part 4: Commands*[S].
15. ISO 13492, *Financial services — Key management related data element — Application and usage of ISO 8583 data elements 53 and 96*[S].
16. ISO/IEC 13888:2004 (all parts), *Information technology — Security techniques — Non-repudiation*[S].
17. ISO/IEC 14516:1999, *Information technology — Security techniques — Guidelines for the use and Management of Trusted Third Party services*[S].
18. ISO/IEC 15288:2008, *Systems and software engineering — System life cycle processes*[S].
19. ISO/IEC 18043:2006, *Information technology — Security techniques — Selection, deployment and operations of intrusion detection systems (IDS)* [S].
20. ISO/IEC TR 18044:2004[[1]](#footnote-0)), *Information technology — Security techniques — Information security incident management*[S].
21. ISO 21118, *Information to be included in specification sheets — Data projectors*[S].
22. ISO/PAS 22399:2007, *Societal security — Guidelines for incident preparedness and operational continuity management*[S].
23. ISO/IEC 27003, *Information technology — Security techniques — Information security management systems implementation guidance*[S].
24. ISO/IEC 27004, *Information technology — Security techniques — Information security management — Measurement*[S].
25. IETF *Site Security Handbook* (RFC 2196), September 1997
26. IETF *IP Security Document Roadmap* (RFC 2411), November 1998
27. IETF *Security Architecture for the Internet Protocol* (RFC 2401), November 1998
28. IETF *Address Allocation for Private Internets* (RFC 1918), February 1996
29. IETF *SNMP Security Protocols* (RFC 1352), July 1992
30. IETF *Internet Security Glossary* (RFC 2828), May 2000
31. IETF *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing* (RFC 2827), May 2000
32. NIST Special Publications (800 series) on *Computer Security，*NIST Special Publication 800-10: *Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls,* December 1994.

1. ) ISO/IEC TR 18044 will be canceled and replaced following the publication of ISO/IEC 27035. [↑](#footnote-ref-0)