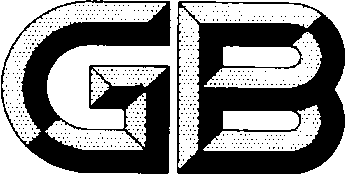
****

**中华人民共和国国家标准**

GB/T 25068.2—2018

|  |
| --- |
| 代替GB/T 25068.2—2010 |

信息技术　安全技术 网络安全

第2部分：网络安全设计和实现指南

Information technology — Security techniques — Network security —

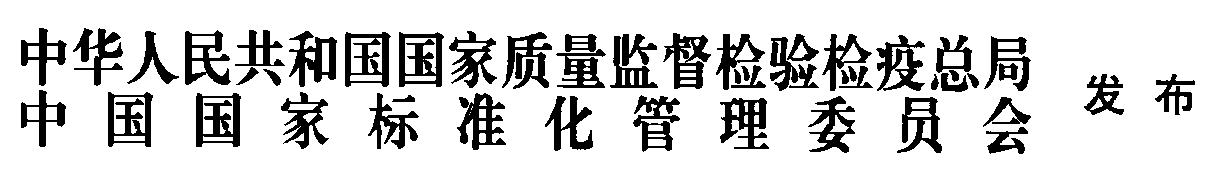
Part 2: Guidelines for the design and implementation of network security

（ISO/IEC 27033-2:2015，IDT）

|  |
| --- |
| （草案） |
| （本稿完成时间：2018年6月7日） |

1. XXXX-XX-XX发布

XXXX-XX-XX实施

****

目　　次

[前　　言](#_Toc27777_WPSOffice_Level1) [4](#_Toc27777_WPSOffice_Level1)

[1 范围](#_Toc393_WPSOffice_Level1) [1](#_Toc393_WPSOffice_Level1)

[2 规范性引用文件](#_Toc10637_WPSOffice_Level1) [1](#_Toc10637_WPSOffice_Level1)

[3 术语和定义](#_Toc3500_WPSOffice_Level1) [1](#_Toc3500_WPSOffice_Level1)

[4 缩写](#_Toc24574_WPSOffice_Level1) [1](#_Toc24574_WPSOffice_Level1)

[5 文档结构](#_Toc29546_WPSOffice_Level1) [1](#_Toc29546_WPSOffice_Level1)

[6 网络安全设计准备工作](#_Toc18092_WPSOffice_Level1) [2](#_Toc18092_WPSOffice_Level1)

[6.1 引言](#_Toc9645_WPSOffice_Level2) [2](#_Toc9645_WPSOffice_Level2)

[6.2 资产识别](#_Toc393_WPSOffice_Level2) [2](#_Toc393_WPSOffice_Level2)

[6.3 收集需求](#_Toc10637_WPSOffice_Level2) [3](#_Toc10637_WPSOffice_Level2)

[6.3.1法律和监管需求](#_Toc9645_WPSOffice_Level3) [3](#_Toc9645_WPSOffice_Level3)

[6.3.2业务需求](#_Toc393_WPSOffice_Level3) [3](#_Toc393_WPSOffice_Level3)

[6.3.3性能要求](#_Toc10637_WPSOffice_Level3) [3](#_Toc10637_WPSOffice_Level3)

[6.4 需求复审](#_Toc3500_WPSOffice_Level2) [3](#_Toc3500_WPSOffice_Level2)

[6.5 现有设计和实施的复审](#_Toc24574_WPSOffice_Level2) [3](#_Toc24574_WPSOffice_Level2)

[7 网络安全设计](#_Toc24132_WPSOffice_Level1) [4](#_Toc24132_WPSOffice_Level1)

[7.2 设计原理](#_Toc29546_WPSOffice_Level2) [4](#_Toc29546_WPSOffice_Level2)

[7.2.1引言](#_Toc3500_WPSOffice_Level3) [4](#_Toc3500_WPSOffice_Level3)

[7.2.2纵深防御](#_Toc24574_WPSOffice_Level3) [5](#_Toc24574_WPSOffice_Level3)

[7.2.3网络分区](#_Toc29546_WPSOffice_Level3) [5](#_Toc29546_WPSOffice_Level3)

[7.2.4弹性设计](#_Toc18092_WPSOffice_Level3) [6](#_Toc18092_WPSOffice_Level3)

[7.2.5场景](#_Toc24132_WPSOffice_Level3) [6](#_Toc24132_WPSOffice_Level3)

[7.2.6模型和框架](#_Toc30096_WPSOffice_Level3) [6](#_Toc30096_WPSOffice_Level3)

[7.3 设计验收](#_Toc18092_WPSOffice_Level2) [6](#_Toc18092_WPSOffice_Level2)

[8 网络安全实现](#_Toc30096_WPSOffice_Level1) [7](#_Toc30096_WPSOffice_Level1)

[8.1 引言](#_Toc24132_WPSOffice_Level2) [7](#_Toc24132_WPSOffice_Level2)

[8.2 网络组件选择标准](#_Toc30096_WPSOffice_Level2) [7](#_Toc30096_WPSOffice_Level2)

[8.3 产品或供应商的选择标准](#_Toc7905_WPSOffice_Level2) [7](#_Toc7905_WPSOffice_Level2)

[8.4 网络管理](#_Toc30975_WPSOffice_Level2) [8](#_Toc30975_WPSOffice_Level2)

[8.5 日志、监控和事故响应](#_Toc15716_WPSOffice_Level2) [9](#_Toc15716_WPSOffice_Level2)

[8.6 文档](#_Toc14632_WPSOffice_Level2) [9](#_Toc14632_WPSOffice_Level2)

[8.7 测试计划与测试实施](#_Toc26480_WPSOffice_Level2) [9](#_Toc26480_WPSOffice_Level2)

[8.8 验收](#_Toc17039_WPSOffice_Level2) [9](#_Toc17039_WPSOffice_Level2)

[附 录 A （规范性附录） 检查表描述](#_Toc7905_WPSOffice_Level1) [10](#_Toc7905_WPSOffice_Level1)

[附 录 B （资料性附录） 实例文档模板](#_Toc30975_WPSOffice_Level1) [11](#_Toc30975_WPSOffice_Level1)

[B.1 网络安全架构文档模板的一个例子](#_Toc24381_WPSOffice_Level2) [11](#_Toc24381_WPSOffice_Level2)

[B.1.1介绍](#_Toc8002_WPSOffice_Level2) [11](#_Toc8002_WPSOffice_Level2)

[B.1.2 业务相关的需求](#_Toc31856_WPSOffice_Level2) [11](#_Toc31856_WPSOffice_Level2)

[B.1.3技术构架](#_Toc12001_WPSOffice_Level2) [11](#_Toc12001_WPSOffice_Level2)

[B.1.4网络服务](#_Toc5266_WPSOffice_Level2) [12](#_Toc5266_WPSOffice_Level2)

[B.1.5硬件/物理布局](#_Toc7081_WPSOffice_Level2) [13](#_Toc7081_WPSOffice_Level2)

[B.1.6软件](#_Toc4182_WPSOffice_Level2) [13](#_Toc4182_WPSOffice_Level2)

[B.1.7性能](#_Toc15655_WPSOffice_Level2) [14](#_Toc15655_WPSOffice_Level2)

[B.1.8已知问题](#_Toc23576_WPSOffice_Level2) [14](#_Toc23576_WPSOffice_Level2)

[B.1.9参考资料](#_Toc32068_WPSOffice_Level2) [14](#_Toc32068_WPSOffice_Level2)

[B.1.10附录](#_Toc5428_WPSOffice_Level2) [14](#_Toc5428_WPSOffice_Level2)

[B.1.11注释词表](#_Toc15032_WPSOffice_Level2) [15](#_Toc15032_WPSOffice_Level2)

[B.2一个用于功能安全需求文档的示例模板](#_Toc8994_WPSOffice_Level2) [15](#_Toc8994_WPSOffice_Level2)

[B.2.1介绍](#_Toc15411_WPSOffice_Level2) [15](#_Toc15411_WPSOffice_Level2)

[B.2.2防火墙配置](#_Toc8835_WPSOffice_Level2) [15](#_Toc8835_WPSOffice_Level2)

[B.2.3安全风险](#_Toc8638_WPSOffice_Level2) [16](#_Toc8638_WPSOffice_Level2)

[B.2.4安全建设管理](#_Toc31101_WPSOffice_Level2) [16](#_Toc31101_WPSOffice_Level2)

[B.2.5安全行政管理](#_Toc28187_WPSOffice_Level2) [16](#_Toc28187_WPSOffice_Level2)

[B.2.6身份验证和访问控制](#_Toc26655_WPSOffice_Level2) [16](#_Toc26655_WPSOffice_Level2)

[B.2.7（审计）记录](#_Toc20526_WPSOffice_Level2) [16](#_Toc20526_WPSOffice_Level2)

[B.2.8信息安全事件管理](#_Toc15513_WPSOffice_Level2) [17](#_Toc15513_WPSOffice_Level2)

[B.2.9实体安全](#_Toc21693_WPSOffice_Level2) [17](#_Toc21693_WPSOffice_Level2)

[B.2.10人员安全](#_Toc21139_WPSOffice_Level2) [17](#_Toc21139_WPSOffice_Level2)

[B.2.11附录](#_Toc11006_WPSOffice_Level2) [17](#_Toc11006_WPSOffice_Level2)

[B.2.12注释词表](#_Toc32234_WPSOffice_Level2) [17](#_Toc32234_WPSOffice_Level2)

[附 录 C ITU-T X.805 框架和ISO/IEC 27001:2005 控制映射](#_Toc15716_WPSOffice_Level1) [18](#_Toc15716_WPSOffice_Level1)

前　　言

GB/T 25068《信息技术 安全技术 网络安全》分为以下5个部分：

——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：使用安全网关保护网络之间的通信

——第5部分：使用虚拟专用网络(VPN)保护跨网通信安全保护

——第6部分：无线IP网络访问安全保护

本部分为GB/T 25068的第2部分。

本部分按照GB/T 1.1-2009给出的规则起草。

本部分使用翻译法等同采用国际标准ISO/IEC 18028-2：2006《信息技术 安全技术 IT网络安全 第2部分：网络安全体系结构》。本部分代替了GB/T 25068：2011《信息技术 安全技术 IT网络安全 网络安全体系架构》。与GB/T 25068：2011相比，主要技术变化如下：

1. 删除了引言部分。
2. 原文CCITT X.800中的内容已在本部分引用的国家标准GB/T 9387.2-1995中体现，故本部分不再引用X.800。
3. 在原文正文里使用的缩略语没有全部反映在第4章中，本部分在其中做了增补，增加的缩略语在其右面页边用单竖线“|”指示。
4. 为避免干扰章节编号，第5章中几个问题的数字编号改为字母编号。
5. 由于我国尚未有隐私和数据保护的相关法律法规，故在6.8中删掉“依据国家隐私和数据保护的法律法规”。

本文件的某些内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任。

本部分由全国信息安全标准化技术委员会（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.

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

信息技术 安全技术 网络安全 网络安全设计和实现指南

1. 范围

本部分标准为组织提供了计划、设计、实施和记录网络安全的指南。

1. 规范性引用文件

下列引用文件对本文档的应用是必不可少的。凡是注日期的引用，只有引用的版本适用。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。

ISO/ IEC7498（所有部分），信息技术 - 开放系统互连 - 基本参考模型

GBT 29246-2012 信息技术 安全技术 信息安全管理体系 概述和词汇

GB/T 22080-2016 信息技术 安全技术 信息安全管理体系 要求

GB/T 22080-2016 信息技术 安全技术 信息安全管理体系 信息安全控制实践指南

ISO/ IEC 27005：2011 信息技术 - 安全技术 - 信息安全风险管理

GB/T 25068-1，信息技术 - 安全技术 - 网络安全 第1部分：综述和概念

1. 术语和定义

为施行本文件，ISO / IEC 7498（所有部分），GB/T 16264、GB/T 22080、GB/T 22081、ISO / IEC 27005和GB/T 25068-1中的术语和定义都适用。

1. 缩写

IPS 入侵防御系统（Intrusion Prevention System）

POC 概念证明（Proof of Concept）

RADIUS 远程身份验证拨入用户服务（Remote Authentication Dial-In User Service）

RAS 远程访问服务（Remote Access Service）

SMS 简单消息服务（Simple Message Service）

SMTP 简单邮件传输协议（Simple Mail Transfer Protocol）

TACACS 终端访问控制器访问控制系统（Terminal Access Controller Access-Control System）

TFTP 简单文件传输协议（Trivial File Transfer Protocol）

TLS 安全传输层协议（Transport Layer Security）

1. 文档结构

本部分标准的结构包括：

• 网络安全设计的准备

- 引言

- 资产识别

- 需求收集

- 需求复审

- 现有的设计和实施的复审

• 网络安全设计

- 引言

- 设计原则

- 设计验收

• 网络安全实现

- 引言

- 网络组件的选择准则

- 产品或供应商的选择准则

- 网络管理

- 日志记录、监控和事故响应

- 文档

- 测试计划和实施测试

- 验收

1. 网络安全设计准备工作
   1. 引言

网络安全的目标是促进那些能够提高组织业务流程的信息流，阻止那些降低组织业务流程的信息流。网络安全设计与实施的编制工作包括如下阶段：

--资产识别

--需求收集

--需求复审

--技术选择和技术约束的评估

--现有设计和实施的评估

这些阶段形成了早期的文档，该文档包括：后续设计与实施阶段的所有输入。

* 1. 资产识别

对任何网络来说，资产识别是应对信息安全风险的首要步骤。有些资产如果被不适当地泄露、修改或失效，将会延缓组织的业务流程，这样的资产都需要保护。需要保护的资产包括物理资产（服务器，交换机，路由器等）和逻辑资产（配置设置，可执行代码，数据等）。作为持续性计划/灾难恢复风险分析的一部分，资产登记应已执行。需要解决如下问题：

--需要保护的不同类型的网络设备和设施分组有哪些？

--需要保护的不同类型的网络活动有哪些？

--需要保护哪些信息资产和信息处理能力？

--信息资产存储于信息系统架构的哪个位置？

可识别的资产包括安全支持管理、控制和用户通信所需的资产，以及网络基础设施、服务和应用程序正常生效的功能。这就包括主机、路由器、防火墙等设备，接口（内部和外部），信息存储/处理和使用的协议。基础设施资产的保护仅是网络安全设计目标的一部分。原则目标是保护商业资产，例如信息和业务过程。

* 1. 收集需求

6.3.1法律和监管需求

应该收集和复审法律监管对网络定位与功能的要求，以保证这些需求在网络设计中得到满足。需要特别注意跨管辖或监管边界的信息流。在这种情况下，需要记录边界两侧的要求。

6.3.2业务需求

组织的业务流程和数据分类类型决定了其访问需求。网络应该配置成这样：对于适当授权的用户能够访问信息资产，并且阻止其他的访问。信息访问通常和一些服务相关，这些服务可以建立在开放端口（例如TCP端口80的HTTP服务）、特定主机（如www.example.org，IP地址为10.11.12.13），特定主机组（例如172.128.97.64/24子网）或特定的网络接口设备（如MAC地址为10:00:00:01:02:03的接口）。该组织需要识别哪些是向他人提供的服务、哪些是由他人提供的服务以及哪些是内部服务。

6.3.3性能要求

流量数据能够记录通信线路、服务器和安全网关/防火墙的配置，故而需要被收集，以便实现用户所期望的高水平服务—没有“过度配置”以及相关不必要的成本。收集的信息诸如现有通信连接的速度，任何第三方路由器的配置/容量，每个链接允许访问的用户数（并发访问和访问的用户数量），所需的最小、平均和最大用户连接时间，可访问的授权用户身份，网页点击次数，数据库访问的点击率，未来一年和三/五年的增长预期，以及是否需要窗口登录。可以使用电信表(排队)理论来确定所需端口、信道的数量，特别是拨号链路上的端口和信道。应对性能要求进行复审，排除疑问，性能标准要求应满足已经确认的技术架构和相关的技术安全架构。

* 1. 需求复审

当前的性能和任何计划的技术网络架构的变化都需要进行复审，并和开发中的技术安全架构进行比较以发现不兼容之处。这些不兼容之处都需要重新复审并且进行适当的架构修改。

在复审过程中收集到的信息应至少包括以下内容：

—正在使用的网络连接类型的识别；

—安全风险的确定；

—制定技术安全体系架构和安全控制的需求列表；

—使用的网络协议；

—在网络各个层面使用的网络应用。

信息的收集应考虑网络性能。应该获得相关网络体系结构的详细信息，并对此进行复审，以便为接下来的过程步骤提供必要的理解和上下文。尽早明确这些内容，确定相关的安全需求识别标准、识别控制区域、审查技术安全体系结构选项并决定哪些应被采纳，可获得更高效更可行的安全解决方案。例如，对于由于位置的关系，只能通过一个管道建立所有网络连接，那么对于选定的地点来说，针对多种不同通道，所设置的冗余连接的安全控制，就是无用无效的。其他控制也要如此考虑，才能找到保护网络连接的最优方式。

在早期阶段，如果当前架构下尚未实现能被接受的安全解决方案，则应为网络和应用架构预留出时间，以便对这些架构进行复审和必要的修改。

* 1. 现有设计和实施的复审

现有安全控制复审必须依据安全风险评估和管理复审的结果来进行。安全风险评价的结果可以指明被评估威胁相应的安全控制需求。应对当前网络安全架构进行差距分析，以确定现有的网络安全体系结构中还有哪些问题还未解决。

网络安全体系架构应该包含现有的网络控制措施以及任何遗漏和新的安全控制措施。

1. 网络安全设计
   1. 引言

网络安全体系架构限制了不同信任域之间的数据流。信任域之间最明显边界是一个组织内部网络和外部世界之间的接口。任何规模的组织，都会在可被识别和控制的内部信任域之间确立边界。网络安全体系结构包括：组织/行业内部网络与外部世界之间接口的描述，反映上述6.4节中提到的复审要求，并解决如何保护组织免受GB/T 25068-1中曾描述的常见威胁和漏洞的攻击。

7.2节提供了最佳实践设计指南，本系列标准第4部分及之后部分给出了针对当前和未来特定网络技术的网络安全体系架构指南，以及在特定场景下一个组织的设计指南。本系列标准第3部分给出了一个组织所需的特定网络场景的指南。

需求调研过程中形成的技术设定必须形成文档，例如：

—只允许有授权访问的IP通信（防火墙通常支持IP通信，如果允许并入协议，那么可能会造成管理困难）；

—如果需要引入非IP协议，则此类协议需在安全体系架构之外或利用隧道技术的协议来进行接入。

网络安全体系结构通常包含服务，包括但不限于：

—身份验证和授权（密码、令牌、智能卡、证书、RAS /RADIUS/终端访问控制系统（TACACS+），等）；

—逻辑访问控制（单点登录、基于访问控制的角色、可信数据库、应用程序控制、防火墙、代理设备等）；

—安全审计和核查（审计日志、审计日志分析设备、入侵检测设施、写一次读多次（WORM）设备等）；

—存储清理/安全删除（可控“擦除”设施）；

—安全测试（漏洞扫描、网络监听，渗透测试等）；

—安全的开发环境（独立开发和测试环境、免编译器等）；

—软件变更控制（配置管理软件、版本控制等）；

—安全软件部署（数字签名、SSL协议、传输层安全（TLS）（RFC 5246），等）；

—安全维护和可用性（良好的备份/恢复设施、恢复、聚类、数据仓库、多样性通信等）；

—传输安全（传输加密的使用、扩频技术、无线局域网（WLAN）、虚拟专用网/外联网）。

* 1. 设计原理

7.2.1引言

与网络安全体系架构相关的常见风险是设计失败，这是由于不好的设计和/或对业务连续计划缺少适当的考虑或设计无法对当前或未来威胁等级做出响应。设计安全体系架构的基本要素是已识别的安全控制措施和业务需求。通用的网络安全设计实践大多包括这些要素。本系列标准第4部分之后的部分详细介绍了网络技术安全体系架构最佳实践的设计与实现。关于最佳实践指南的其他细节可能在后续颁布的部分中有所体现。

当考虑网络安全体系架构时，下面几个部分提供了关于设计最佳实践的一般性指南。

7.2.2纵深防御

组织不仅仅应从一个角度来考量网络安全，而是应通过一种普适分层方法来进行综合考量。安全必须全面覆盖所有网络层。采用分层方法的网络安全体系架构就是纵深防御。安全组件是一个集策略、设计、管理和技术于一体的组合。每一个组织都需要确定需求，并设计一个基于这些需求的纵深防御。

许多移动设备有USB和网络连接，以及无线功能。这些设备可以通过ad-hoc方式连接到内部网络或系统。如果设备的无线连接开放和无担保，这些设备就可能通过绕过外围控制在内部网络上充当着一个流氓无线接入点。应采取严格措施，以限制不安全的移动设备连接到网络，并为检测流氓接入点而执行日常的无线信道扫描。

任一无线接入点应设计在非军事区。内部网络的无线接入点应该有严格的连接设置：最强的安全保护措施（在可能的情况下用WPA2），MAC地址过滤以限制有设备连接到已授权的设备。本标准的第3部分提供了更多关于移动通信技术和相关控制威胁的细节。

纵深防御原则体现了使用多个安全控制或安全技术来帮助减少风险，该风险是来自于被破坏或被规避的防御组件。举例来说，同一环境中已经具备病毒防护的防火墙和服务器时，个人工作站上也应安装防病毒软件。来自多个供应商的不同的安全产品可能被部署用来防御网络中的不同的潜在载体，帮助防止任何一个防御的短板，该短板可能导致一个更大范围的失效，这种防御方法被称为“分层方法”。

图1显示了边界安全、基础设施安全、主机安全 、应用程序安全和数据安全。所有的层都是为了保护数据。

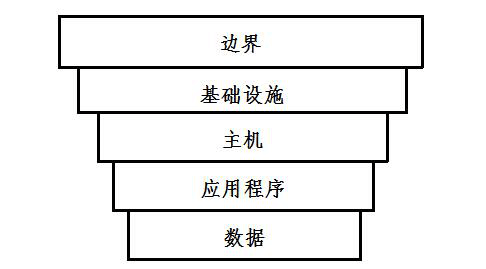


图1-纵深防御

基于分层方法的安全解决方案是灵活和可度量的，该解决方案适用于组织的安全需求。

7.2.3网络分区

网络分区指将不同敏感度等级（不同风险容忍度和敏感度）的系统资源置于不同的安全分区。在系统内创建了一种方法，即在系统的特定区域内，只使用执行任务所必需的数据。（例如，只有在互联网上提供服务的服务器才是在公共DNS上注册的）。

安全网关（专用防火墙设备、在IPS设置防火墙功能，以及在网络路由器和交换机中的访问控制列表）就是指保证所需的网络流量，限制不必要的网络流量。

有了适当的布局和配置，安全网关有助于创建安全架构，将网络基础设施进行安全区域划分并控制它们之间的通信。如何布局和配置安全网关详见在本系列标准的第4部分。

划分原则体现出以下网络安全设计原则：

–不同敏感度的网络应设在不同的安全区：

–为外部网络提供服务（例如互联网）设备和计算机系统应位于不同的区域（非军事区–DMZ）内部网络设备和计算机系统则无需进行分区；

–战略资产应设在专用安全区；

–低信任级别的设备和计算机系统，如远程访问服务器和无线网络接入点应设在专用安全区。

–不同类型的网络应位于不同的安全区：

–用户工作站应同服务器位于不同的安全区；

–网络和安全管理系统应设在专用安全区；

–在开发阶段的系统应同产品系统位于不同的区域。

7.2.4弹性设计

网络安全设计应包括多个层的冗余，以防备单点故障并最大限度地提高网络基础设施的可用性。这包括使用冗余接口、备份模块、备用设备和拓扑冗余路径。此外，设计还使用了一组富功能设置，以使网络对攻击和网络故障具有更强的抵抗力。

7.2.5场景

对网络环境的复审，通常围绕与已定义的网络威胁、设计考量和控制要素等特征相关的特定网络场景和相关的“技术”主题。对于审查技术安全架构/设计选项，选择和记录与首选技术安全架构/设计的相关安全控制来说，这些信息是非常有用的。这一系列标准的第3部分引用了此类场景，对每个场景的安全威胁和安全设计技术与控制要素提供了详细的指导，以应对这些威胁。

7.2.6模型和框架

安全系统工程组件包括安全模型或框架的选择、使用和制定。

安全模型是用来描述实体（受组织安全策略约束的主题）和定义策略中所述的必要访问规则。安全模型通常侧重于通过访问控制或信息完整性进行保密，其中一些是正式定义的，另一些是非正式定义的。

典型的安全模型聚焦于进入过程的保密性或信息的完整性，其中一些被正式定义和其他被非正式的定义。

安全框架通常为组织提供一种如何形成安全系统大纲的方法，一个框架的例子是ITU-T X.805。ITU-T X.800这一系列的首要框架是ITU-T X.805，其适用于终端到终端的网络安全机制。为此，X.805定义了安全维度的概念，这些维度包括工具容器、技术、标准、法规、程序等等。这些维度涵盖了安全的方方面面。X.805定义了一个避免冗余安全的机制，通过识别某一层（特指在X.805中的层）的能力来保护另一个层，从而降低了安全解决方案的整体成本。X.805是一个通用的安全框架且不提供任何特定信息系统或组件的规范。相反，它指定了安全规则和目标的安全功能，以促进终端到终端的网络安全。附件C中提供了ITU-T X.805如何在ISO / IEC 27001控制支持下进行应用。

* 1. 设计验收

网络安全设计的验收应在适当水平的管理下完成。

1. 网络安全实现
   1. 引言

第7章描述了网络安全的实现应基于网络安全设计。

网络安全的实现包括：

* 分区和分块；
* 网络组件选择标准；
* 产品或供应商选择标准；
* 网络管理；
* 记录、监控和事故响应；
* 文档；
* 测试计划与测试实施；
* 验收。
  1. 网络组件选择标准

对于任何安全网络设计而言，都会用到通用组件的组合。这些组件的组合将创建一个技术层面上的网络安全设计。第8章和ISO/IEC 27033-3之后的部分将讨论下列组件的细节。这些组件形成一定组合，以确保在6.4节中所反映的需求。

这些组件可能包括：

• 分区和分块；

* 安全管理系统（如监控和配置管理）；
* 基本安全技术，如身份管理、密码等；
* 网络准入控制设备；
* 威胁削减技术；
* 边界设备；
* 网络过滤器，如防火墙和远程访问设备的内容监测；
* 入侵检测系统/入侵防御系统；
* 端点保护；
* 路由器和交换机；

• 外网连接。

* 1. 产品或供应商的选择标准

产品选择不应该孤立的进行，应建立一个与网络安全体系架构设计相关联的迭代过程。

举例来说，产品选择应基于以下内容：

–产品的技术适用性和优点；

–性能；

–协议支持；

–弹性；

–兼容性；

–可扩展性；

–网络管理设施；

–审计能力；

–一致性；

–技术文档；

–维护性；

–远程诊断设备；

–逻辑安全；

–遵循类似ISO15408（信息安全评估准则）标准中定义的评估方法来保证安全功能的实现；

–供应商的特点（能力、跟踪记录、对质量的承诺、市场地位、规模、对产品定位、组织/财务稳定性、参考和培训设施的综合能力）；

–按交货时间表交货；

–成本。

* 1. 网络管理

网络管理是指网络系统操作、管理、维护和供给网络系统所属的活动、方法、程序和工具。

• 保持网络和网络提供的服务正常平稳运行的操作，包括监测网络，以便于在用户受到影响之前及时发现问题。

• 跟踪并合理分配网络资源的管理。包括所有处于网络控制下的“管家”服务。

• 执行维修和升级的维护。例如，当设备必须更换时、当路由器为操作系统镜像提供一个补丁时、当为网络添加一个新的交换机时。维护还包括纠错和防御方法以使得网络运行的更好，例如调整设备配置参数。

有意或故意地错误配置相关的网络组件，会产生重大风险，不仅关系到其可用性，也常常关系到完整性和保密性。

因此解决这些风险的控制是必要的。这种控制可以分为组织控制和技术控制。

组织控制包括适当任命管理人员、操作四眼原则、适当的职责分离，以及为避免出现默认或弱密码所采取的程序和策略。操作控制包括配置和版本控制，来解决或跟踪潜在的错误配置或设备配置变更。

技术控制包括使用管理接口和工具提供适当的身份验证、授权和数据保密。技术管理需要大量的与网络相关的组件。安全网关可以在本地或远程进行管理，但远程管理应该使用工具来完成，此类工具应保证具有强身份验证或双身份验证，或至少能够在技术上避免默认或弱密码，并且能够尽可能提供完整性和保密性的功能。例如对加密VPN通道使用时，适当地配置加密等级或SSH终端仿真。服务器也可以在本地或远程管理。服务器对敏感信息进行远程管理时，使用工具应保证具有强身份验证或双身份验证，或至少能够在技术上避免默认或弱密码，并且能够尽可能提供完整性和保密性的功能。

基础设施组件，如交换机和路由器，可以从控制台端口进行本地管理，也可从中央管理工作站进行远程管理，或使用远程终端仿真程序来管理远程计算机或分布式管理系统。然而，这些协议是不安全的,除非他们可以配置一个方法对连接进行完全的加密。安全的远程连接的一个例子就是完全加密并含有一个安全文件传输工具的SSH。此外，访问基础设施组件应由身份验证服务器控制。

外包给服务提供者的网络通常有自己的管理系统。他们应该通过一个使用安全远程管理方法的中央管理站进行管理，远程管理的方法应该包括使用公钥密码加密和认证。可以使用的安全方法例如Telnet、通过VPN隧道的TFTP或由一个认证服务器控制的SSH。

许多组织使用简单网络管理协议(SNMP)管理陷阱来直接监控网络。SNMP版本1和版本2有重大风险以致网络存在脆弱性或不安全。因此，如果一个组织决定使用SNMP，则应该使用版本3以实现完整的安全控制。

* 1. 日志、监控和事故响应

就如同用安全相关设备保护起来的DMZ一样，位于DMZ的审计服务器也是通过配置所有安全网关系统来实现内网和外网整体的安全。审计服务器不是内部网络域的一部分，应该只能被分配授权管理安全网关/防火墙系统的安全人员直接访问。然而，需要允许写入访问操作，以使得审计日志通过基础设施组件、服务器和防火墙内的安全协议上传(例如安全复制协议(SCP))。所有防火墙和指向审计服务器的审计日志都应经由安全检查人员通过专用于审计日志文件复审的审计分析软件进行事后检验。

安全信息管理包括信息的收集和标准化，以便于决策。收集的信息可能包括系统记录、SNMP信息、IDS/IPS警报和流信息。

在可能的情况下，应根据已检测到的异常活动优先级来配置审计服务器和/或IDS/IPS系统，通过电子邮件、短信等方式，向已任命的安全管理人员发出警报。任何一项异常活动应该为视为一次未遂攻击，被任命的安全管理人员应该按照警报优先级来对实施事故响应程序。

* 1. 文档

网络安全架构文档是关键技术安全文档之一，如前所述，应符合相关的安全风险评估和风险管理复审结果，且满足组织/行业网络和信息安全策略和相关的其他安全策略的有关要求。与其他文档一样，网络安全架构文档也应实施变更控制管理。附件B.1中给出了一个示例模板。它应该参考相关技术架构文档和其他技术安全文档。主要相关的文档包括：

–信息安全管理的所有网络组件的需求文档(如安全网关、防火墙、路由器等)。这些需求也包括功能安全需求如防火墙规则库的需求。——模板示例见附件B.2；

–审计日志分析软件需求文档；

–产品分析报告。

* 1. 测试计划与测试实施

安全测试策略文档用来描述用测试来验证网络技术安全体系架构的方法。它应该专注于关键技术安全控制应如何测试，以确保定义的需求得到满足，所设计的策略得以实施。为了验证这些观点，要执行系统测试和基于检查表的检查。

测试策略文档应该包括：

–识别和身份验证机制；

–弹性设计；

–授权机制；

–实施策略的控制；

–验证固化操作系统；

–验证审计日志解决方案。

测试策略还应该包括单元测试和可用性测试，以确保设计的适用性。

进行系统测试之前，测试计划之前应该做好准备。测试计划应包括测试数据和测试场景以留作证据。测试计划还应该包括一个适当的测试清单。应该精心准备测试数据以检验技术安全控制的功能。

* 1. 验收

完整的网络安全实施的验收应该在适当的管理水平下进行。

附 录 A  
（规范性附录）  
检查表描述

表1： ISO / IEC 27001:2005 / ISO / IEC 27002:2005网络安全相关控制和ISO / IEC 27033 - 2:2012条款的交叉引用表

|  |  |  |
| --- | --- | --- |
| ISO/IEC 27001:2005/  ISO/IEC 27002:2005  条款 |  | ISO/IEC 27033-2:2012 clause |
| 0.6.1- 网络控制 | 网络应该充分的管理和控制,从威胁,为了保护和维护安全系统和应用程序使用网络,包括在途信息。 | 见下文对ISO / IEC 27001/27002条10.6.1 IG a）到e） |
| 10.6.1 IG a) | 操作负责网络应该分开，在适当的地方操作  计算机 | 8.3网络管理 |
| 10.6.1 IG d) | 适当的日志应该应用于使记录的操作。 | 8.4 日志记录和监控 |
| 10.6.1 IG e) | 管理活动应密切协调优化服务组织和确保于各个控制信息处理基础设施应用一致。 | 8.3网络管理 |
| 10.6.2 –网络服务安全 | 安全特性、服务水平和管理需求的网络服务应该识别和包含在任何网络服务协议,这些服务是否提供内部或外包。 | 6.3 需求收集 |
| 10.8.1 信息交换政策和步骤 | 正式交流的政策、程序和控制应该在保护的信息交换通过使用所有类型的通信设施。 | 8.5文档 |
| 11.4.1 网络服务政策 | 用户只能提供访问服务,他们已经明确授权使用。 | 8.3网络管理 |
| 11.4.2 用户身份验证和外部链接 | 适当的身份验证方法应该用于控制由远程用户的访问。 | 8.3网络管理 |

附 录 B  
（资料性附录）  
实例文档模板

B.1 网络安全架构文档模板的一个例子

B.1.1介绍

包括部分如:

•目的/目标/范围,

•假设,技术,否则,

•文档状态,

•文档结构

B.1.2 业务相关的需求

包括部分如:

•介绍,

•上下文,

•网络和其他服务。

B.1.3技术构架

包括部分如:

•介绍,

•技术概述

——总结,

——主要领域1,

——主要领域2

——主要领域3,

——等等。

——服务器,

——工作站,

——日志记录,

——管理、

——身份验证和访问控制,

——服务覆盖和弹性,

•系统位置,

•系统组件,

•联系,

•组件1,

——概述

——配置,

——日志记录,

——管理、

•组件2,

——概述

——配置,

——日志记录,

——管理、

•组件3,

——概述

——配置,

——日志记录,

——管理、

•组件“x”等。

——服务器管理,

——介绍,

——监视服务,

——扩展系统管理(XSA),

——企业安全管理器(ESM),

——其他经理,

•防火墙、

——介绍,

——概述

——防火墙配置备份,

——设计标准和配置,

——规则基地,

•防火墙管理,

——配置,

——防火墙警报,

——远程访问,

•日志,

•备份系统,

——介绍,

——防火墙、

——服务器,

——应用程序,

•网络通信,

——局域网络,例如vlan,无线局域网,

——路由器,

——开关,

——IP寻址,

•管理责任,

——服务器,

——防火墙、

——基础设施,

——应用程序管理。

B.1.4网络服务

包括部分如:

•介绍,

•服务位置x,

•服务位置,

应该有一个列表的所有网络服务的位置,包括如:

•KiloStream服务,

•MegaStream服务,

•帧中继服务,

•自动取款机,

•IP / MPLS,

•宽带服务,

•wifi / WiMax,

•局域网连接服务,

•GSM、

•基本利率ISDN(30 64 Kbps通道交付MegaStream),

•ISDN基本速率接口(BRI),(2×64 Kbps通道),

•模拟直接交换线(del),

•内部网/外联网服务,

•互联网服务提供商,

•包括所有行和服务。

该泛用清单应列入附录，并在文件正文中提及时引用该清单。

B.1.5硬件/物理布局

包括部分,如:

•介绍,

•位置。

应该有一个列表的所有硬件,平面图和内阁布局——位置,包括的报道,例如,服务器、路由器、交换机、防火墙和其他通讯设备。所有的硬件应该贴上标签,标签计划至少应包括或引用。

表B.1显示了一个示例硬件列表。为每个类型的硬件应该有一个表,表的示例包括服务器组件。

**表 B.1 — 例如硬件列表**

|  |  |  |  |
| --- | --- | --- | --- |
| **服务器组件** | **硬件** | **软件** | **内容** |
| 名称和服务器生产 | 零件号码 | 软件和版本 | 具体评论的要求。垂直扩展,或集群 |

B.1.6软件

包括部分,如:

•介绍,

•软件列表,

——x -软件位置,

——y -软件位置,

——等等。

所有软件的列表,包括版本号,应该包括,例如:

•Windows软件,

•防火墙、

•RAS /半径,

•路由器软件,

•切换软件,

•代理,

•审计管理,

•邮件服务器,

• SMTP邮件中继，

• 内容管理，

• java / ActiveX筛选，

• 网络服务器，

• FTP服务器，

• 域控制器，

• 备份软件，

• 其他软件。

该清单应列入附录，并在文件正文中提及时引用该清单。

B.1.7性能

应包括包含“子系统”的预期的性能细节，如：

• 桌面，

• 服务器，

• 局域网，

• 广域网，

• 网关，

• 外部服务。

B.1.8已知问题

有关已知问题的详情，包括有关不符合规定的问题，应包括在技术、物理及环境等方面，包括部分如：

• 导言，

• 不符合的领域。

B.1.9参考资料

参考资料应包括在内的所有相关文件，包括：

• 安全风险评估和管理审查结果，

• 网络安全政策，

• 信息安全政策，

• 有关其他安全政策，

• 技术架构文件，

• 每一个防火墙系统的服务访问（安全）要求文件（包括防火墙规则库），

• （审计）日志分析软件需求文档，

• 产品分析报告，

• 通用测试策略和计划，

• 信息安全事件管理计划，

• SecOPs，

• 第三方安全连接的条件，

• 为第三方用户提供用户指南。

B.1.10附录

包括如下的细节：

• 硬件配置，

• 服务器/主机配置，

• 防火墙配置，

• 路由器配置，

• 软件配置，

• 数据库配置，

• 知识产权解决方案，

• SNMP配置，

• 系统陷阱，

• 应用陷阱，

• 标准。

B.1.11注释词表

B.2一个用于功能安全需求文档的示例模板

注意 每一个防火墙系统应该产生一个文档。

B.2.1介绍

包括部分如：

• 背景/范围/目标，

• 防火墙系统名称，

• 防火墙位置，

• 防火墙角色，

• 负责防火墙操作的人员名称，

• 对文件内容的修订记录，

• 参考文献。

B.2.2防火墙配置

包括部分如：

• 导言，

• 通过防火墙系统链接的身份，

• 防火墙架构概要，

• 防火墙系统详细信息：

–硬件，

–软件，

–防火墙体系结构，

–防火墙服务，

–防火墙管理，

–内部路由器，

–外部路由器，

–DMZ枢纽，

–反恶意代码服务器，

–SMTP邮件，

–网络页面，

–SMTP邮件服务器，

–（审计）记录服务器，

–UPS，

–其他组成部分，

–其他控制要求，

• 对链接，和其他系统的描述，

• 信息类型包括哪些和它们的敏感性，

• 用户类型和数字等。

B.2.3安全风险

包括部分如：

• 介绍，

• 潜在的不利业务影响（有时被称为资产估值），

• 威胁评估，

• 易损性评估，

• 风险评估，

• 在防火墙使用的上下文中。

B.2.4安全建设管理

包括有责任的部门，如：

• 安全干事/组，

• 网络人员，

• 防火墙支持人员，

• 网络管理，

• 其他管理，

• 用户。

B.2.5安全行政管理

包括部分如：

• SecOPs，

• 安全合规审查，

• 可用性，

• 维护，

• 配置控制，

• 容量管理，

• 问题管理，

• 服务水平管理，

• 本文件的有效期满。

B.2.6身份验证和访问控制

包括部分：

• 导言，

• 逻辑访问控制，如防火墙管理员、内部和远程用户，

• 外部访问控制措施，如网络防火墙规则库，安全平台和应用程序代理服务器，

• 网络级保护。

B.2.7（审计）记录

包括日志等部分：

• 信息被记录，

• 进行的分析，以及用了什么工具，

• 安全。

B.2.8信息安全事件管理

包括日志相关的部分：

• 导言，

• 事件报告，

• 事件处理，

• 等。

B.2.9实体安全

包括对访问控制的责任的部分，有：

• 防火墙系统，

• 综合布线。

B.2.10人员安全

包括适用于防火墙相关人员的部分：

• 招聘筛选/检查，

• 安全意识和培训。

B.2.11附录

包括服务和协议细节：

• 向内和向外的访问，

• 远程管理，

• 防火墙管理，

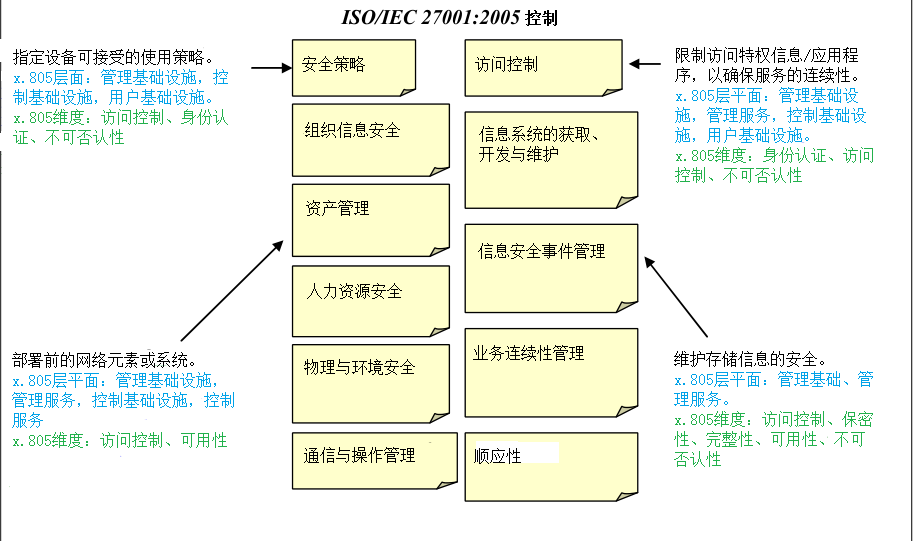
• DMZ服务器管理，

• 任何其他相关的服务和协议细节。

B.2.12注释词表

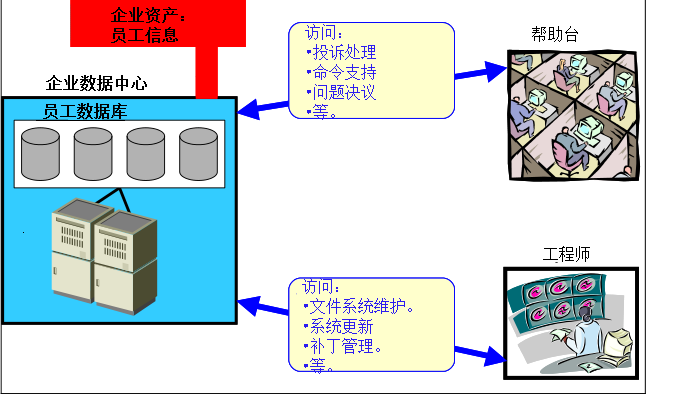
附 录 C  
ITU-T X.805 框架和ISO/IEC 27001:2005 控制映射

ITU-T x.805也可以用于在ISO / IEC 27001:2005标准下增强控制技术。特别是，如图C.1所描绘的，ITU-T x.805可以在安全政策，资产管理、访问控制、信息安全事件管理方面增强ISO / IEC 27001:2005。在具体的层，面，尺寸对ITU-T X.805的适用在图中有详细的描述。例如，随着访问控制和可用性维度成为最突出的问题，最适用于资产管理，基础设施和服务层，控制，和管理层。



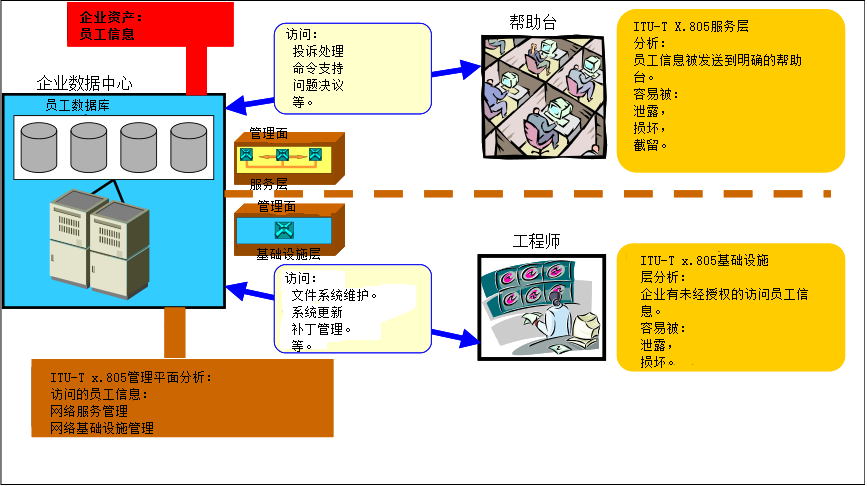
图C.1 -- ITU-T x.805增强ISO / IEC 27001控制

举例来说，为存储其雇员的信息，增强可用于系统地评估和设计的安全性，具体个人信息应仅限于授权用户。员工信息是由企业使用的几个支持组织访问的，其中之一是帮助服务台；此外，其中包含的数据中心和系统由企业组织维护。如图2，帮助台可以通过IT服务访问员工信息处理投诉的，支持新的IT服务订单，解决员工的问题（例如，远程访问）等。此外，作为维修活动的一部分，企业组织访问员工信息并进行文件系统维护，系统更新，补丁管理等行为。



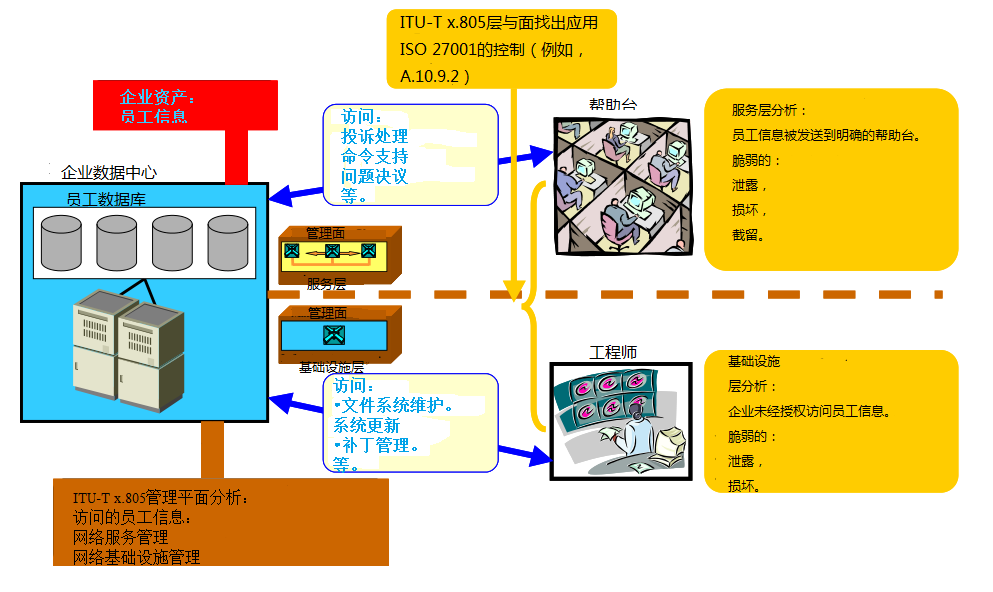
图C.2--企业资产的访问情况

ITU-T x.805威胁/脆弱性分析表明，企业IT组织的成员可以查看和修改员工信息，从而使其容易受到基础设施层的泄露和损坏的攻击（见图C.3）。此外，作为执行问题解决方案的一部分，员工信息在数据中心和帮助服务台之间传送，从而使它在服务层的拦截容易被泄露，损坏。因此，控制必须进行表示和选择，以保护员工的信息，以及基础设施和服务层的管理层中的漏洞。应该指出的是，本文并未对ITU-T x.805一步一步的进行分析。这样的结果仅被认为是假定的简单结果。



图C.3 - ITU-T x.805对企业资产的威胁和脆弱性的分析结果

在服务和基础设施层，由于安全漏洞和威胁，被ISO/IEC 27001:2005 Control A.10.9.2认定为被要求保护员工信息的管理由ITU-T x.805分析（图C.4）。ISO/IEC 27001 Control A.10.9.2规定对参与网上交易信息予以保护，以防止未经授权的信息不完整的传输，误传，变更，未经授权的披露，未经授权的消息复制或重播。



图C.4-- ISO/IEC 27001控制

ITU-T x.805尺寸对控制A.10.9.2的实施和操作提供细节的服务和基础设施层的员工信息。在服务层，通信安全维度提供VPN来防止错误使用。数据完整性维度提供IPSecAH防止完全传输使用，未经授权的信息变更、复制以及防止消息重放。数据保密性维度提供IPSec ESP防止未经授权的披露使用。在基础设施层、数据完整性校验和提供文件尺寸以防止未经授权的变更使用，数据保密性维度提供了文件加密，防止未经授权的披露，访问控制维度提供对文件系统的访问控制列表（ACL）的使用，以防止未经授权的复制。图C.5描绘了ITU-T x.805是如何保护员工信息资产和控制a.10.9.2操作。

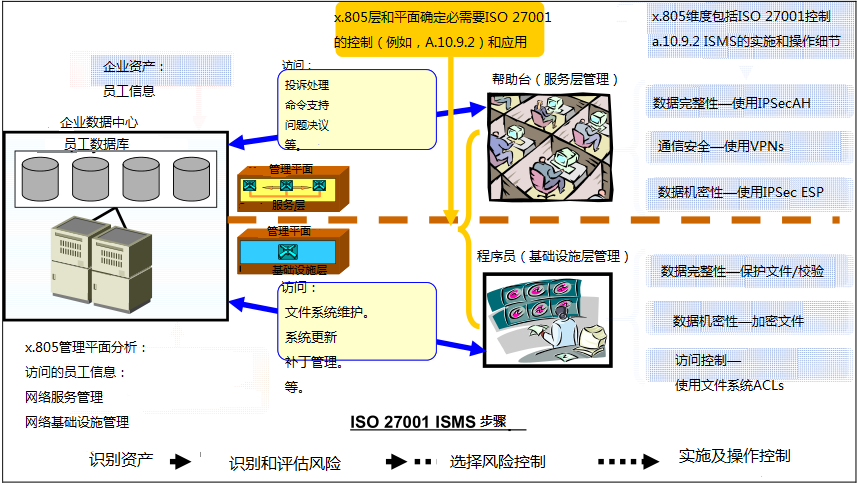


图5 -- ITU-T X.805为ISO / IEC 27001:2005的实施