信息技术
安全技术
信息技术安全管理指南

第 5 部分：网络安全管理指南

注：本文件为个人自行翻译，因译者水平有限，其中错误再所难免，希望大家能够多扔板砖，西红柿亦可以考虑，臭鸡蛋的不要，鲜花尤佳，孔方兄最棒，美女那是我的最爱^_^。

偶，刘青，ID 易水寒江雪，半路出家搞安全管理，希望和大家能够多多交流，也希望各位大虾多多指正。Email:liuq1217@163.com；MSN：liuq1217@msn.com。

目录

1 范围

ISO/IEC TR 13335 的第 5 部分为负责管理 IT 安全的人员提供了关于网络和通讯方面的指南。这一指南支持在建立网络安全要求时需要考虑的通讯相关因素的识别和评估。ISO/IEC TR 13335 这一部分是基于这一技术报告的第 4 部分。第 4 部分介绍了如何识别与连接通讯网络相关的安全相关的适当的防护措施领域。

2 引用标准

ISO/IEC 13335-1:1997 IT 安全管理指南－第 1 部分：概念和一般模型

ISO/IEC 13335-2:1997 IT 安全管理指南－第 2 部分：IT 安全的管理和策划

ISO/IEC 13335-3:1997 IT 安全管理指南－第 1 部分：IT 安全管理技术

ISO/IEC 13335-4:1999 IT 安全管理指南－第 4 部分：选择防护措施

ISO/IEC DTR 14516:1999 关于可信第三方的使用和管理指南

ISO/IEC IS 13888-1997 信息技术－安全技术－抗抵赖性

ISO/IEC WD 15947-1999 IT 入侵检测框架

ISO/IEC IS 7498:第一部分-1995 IT 开放系统互联基本参考模型－基本模型

ISO/IEC IS 7498:第二部分-1989 IT 开放系统互联基本参考模型－安全架构

ISO/IEC IS 7498:第三部分-1997 IT 开放系统互联基本参考模型－命名和地址

ISO/IEC IS 7498:第四部分-1989 IT 开放系统互联基本参考模型－管理框架

（其他非 ISO/IEC 的相关引用标准在附录 A 中表示）

3 定义

ISO/IEC TR 13335 第 1 部分的定义适用于第 5 部分。第 5 部分使用下列术语：可审计性、资产、鉴权、可用性、基线控制方法、保密性、数据完整、影响、完整性、IT 安全、IT 安全策略、可靠性、残余风险、风险、风险分析、风险管理、防护措施、系统完整性、威胁和脆弱点。

4 缩略语

EDI	－	电子数据交换
IP	－	互相网协议
IT	－	信息技术
PC	－	个人电脑
PIN	－	个人识别码
SecOPs	－	安全操作程序
TR	－	技术报告

5 结构

ISO/IEC TR 13335 的第 5 部分采用的方法是：首先，总结了在建立网络安全要求时要考虑的通讯相关的因素的识别和分析的全部过程。然后，为潜在的防护措施领域提供了指示（在此过程中可以使用 TR 13335 其他部分的内容）。

这一文件阐述了三个简单的准则以帮助负责 IT 安全的人员来识别潜在的防护措施领域。这些著作那识别（1）网络连接的不同类型，（2）不同的网络特性和相互的信任关系，以及（3）与网络连接有个的潜在安全风险的类型（以及使用通过这些连接提供的服务）。然后将综合这些准则的结果用于指示潜在的防护措施领域。因此，提供了了关于潜在的防护措施领域以及更多细节来源的指示的简单的介绍性描述。

6 目的

这一文档的目的是为当建立网络安全要求时要考虑的通讯相关要素的识别和分析提供指南，并为潜在的防护措施领域提供指导。

7 概述

7.1 背景

政府和商业组织严重的依赖于信息的使用以开展他们的业务活动。信息和服务的保密性、完整性、可用性、抗抵赖性、可审计性、鉴权和可靠性的丧失可能对组织的业务运作造成负面影响。因此，在组织内保护信息并管理 IT 系统的安全需求就非常迫切。

保护信息的迫切需求在今天的环境里显得尤为重要。因为许多组织的 IT 系统都与网络相连。这些网络连接可以是组织内部的连接，组织之间的连接，有时是组织与公共网之间的连接。政府和商业组织都在全球范围内开展业务。因此他们依赖于从计算机的到传统方式的所有形式的连接。必须满足他们的网络需求。随之，网络安全就扮演者越来越重要的角色。

条款 7.2 总结了当建立网络安全要求时要考虑的通讯相关要素的识别和分析的推荐过程，并为潜在的防护措施领域提供指导。下面的章节将提供这一过程更多的详细信息。

7.2 识别过程

当考虑网络连接时，组织内所有与连接有关的责任人员都应清楚业务要求与益处。此外，他们和所有其他的连接用户应了解这种连接的安全风险及相关的防护措施领域。业务要求和益处可能影响在考虑网络连接、识别潜在的防护措施领域和最终选择、设计、实施和保持安全防护措施的过程中作出的决策和采取的行动。因此在整个过程中都需牢记这些业务要求和益处。为了识别适当的网络相关的安全要求和防护措施领域，需完成下列任务：

- 评审在组织的公司 IT 安全策略中列出的网络连接的通用安全要求（见第 8 条款）；
- 评审与网络连接有关的网络结构和应用程序，以为进行后续活动提供所需的背景信息（见第 9 条款）；

- 识别类型或应考虑的网络连接的类型（见第 10 条款）；
- 评审建议的网络特性（需要时可通过关于网络的可用信息和应用结构），以及相关的信任关系（见第 11 条款）；
- 确定有个的安全风险类型，可能时应借助于风险分析和管理评审的帮助——包括考虑通过连接传输的信息对于业务运作的价值，以及通过这些连接以未授权的方式对任何其他信息的潜在访问（见第 12 条款）；
- 在网络连接类型、网络特性和相关的信任关系的基础上，识别潜在防护措施领域适宜的参考，并确定安全风险的类型（见第 13 条款）；
- 文件和评审安全结构选项（见第 14 条款）；
- 通过使用识别的潜在防护措施领域的参考，准备分配详细防护措施选择、设计、实施和保持的任务，以及达成一致的安全结构（见第 15 条款）。

需要注意的是，在 TR 13335 的第 4 部分中包含了关于防护措施识别的通用性建议。TR 13335 的第 5 部分作为第 4 部分的补充，并介绍了如何识别适当的与通讯网络连接有关的安全相关的防护措施领域。

下图 1 解释了当建立网络安全要求时要考虑的通讯相关要素的识别和分析提供指南，并为潜在的防护措施领域提供指导。这一过程的每一步骤将在图 1 后续的条款中详细介绍。

需要注意的是，在图 1 中，实线代表了过程的主要路径，虚线代表了可以在安全风险分析和管理评审的结构的帮助下确定安全风险的类型。

除了主要路径之外，在一些特定的步骤为了确保一致性，可能需要对前面步骤的结果进行重新审视，尤其是在“ 评审公司 IT 安全策略 ”和“ 评审网络结构和应用程序 ”步骤。例如：

- 在确定完安全风险的类型之后，可能需要评审公司的 IT 安全策略，因为事实上已经出现了某些事情而这些事情没有在这一策略水平上被涵盖；
- 在识别潜在的防护措施领域时，应考虑公司的 IT 安全策略，因为公司的 IT 安全策略可能，例如，规定了必须在组织内实施特定的防护措施而不管风险；
- 在评审安全结构选项时，为了确保一致性，可能需要考虑网络结构和应用程序。

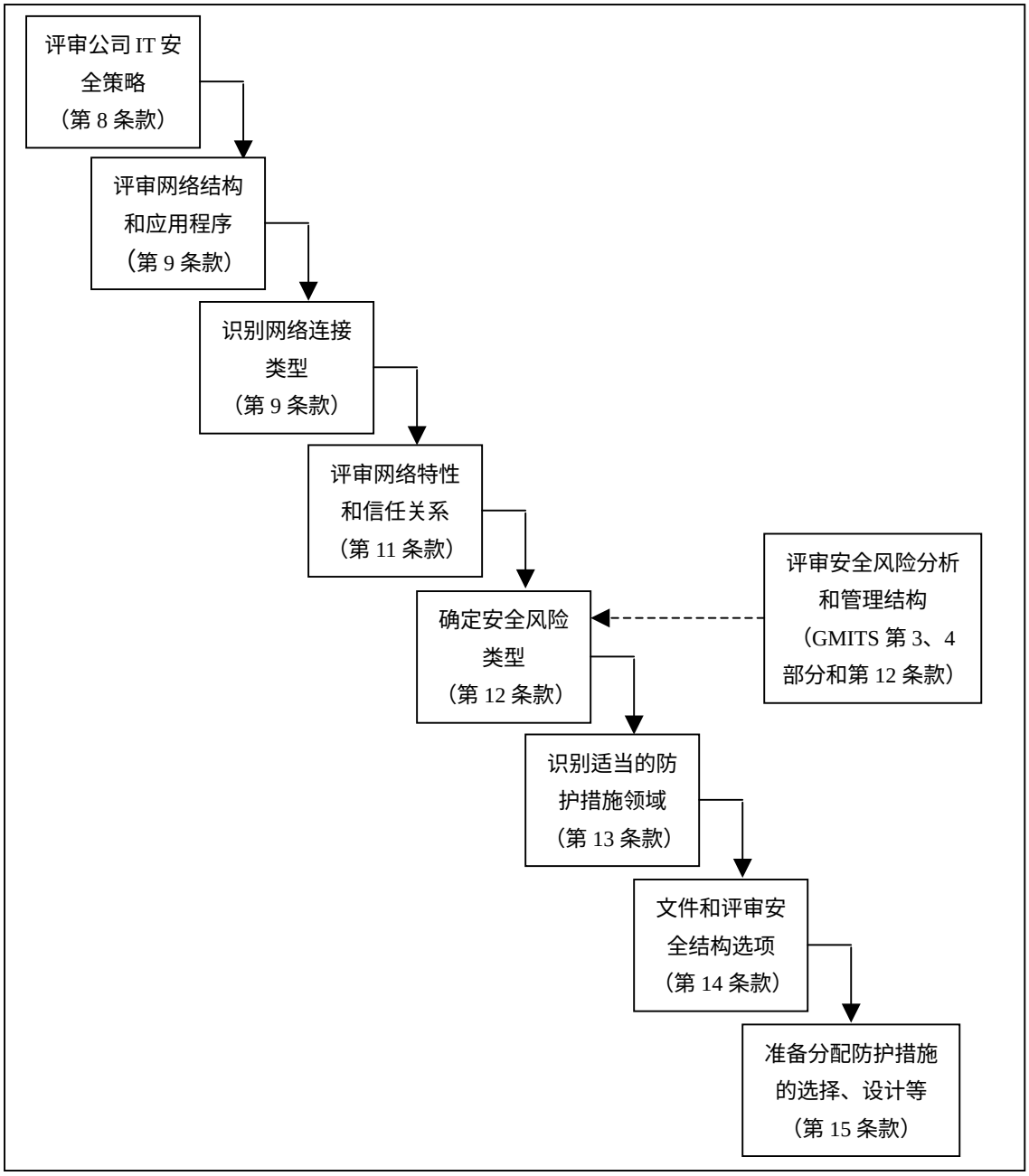

图 1：导致网络安全要求的建立的通讯相关因素的识别和分析过程

8 评审公司的 IT 安全策略要求

组织的公司 IT 安全策略可能包括关于以下方面的声明：对保密性、完整性、可用性、抗抵赖性、可审计性、鉴权和可靠性的需要，以及与网络连接直接相关的威胁类型和防护措施要求的观点。

例如，该策略应陈述：

- 特定类型的信息或服务的可用性是主要的关注点；
- 不允许通过拨号线路进行连接；

- 所有与互联网的连接必须通过安全网关；
- 必须使用特定类型的安全网关；
- 没有数字签名的付款指令是无效的。

必须陈述适用于组织范围的类似的声明、观点和要求，以确定安全风险的类型（见下文的第 12 条款）和识别网络连接的潜在防护措施领域（见第 13 条款）。如果存在类似的安全要求，那么这些安全要求应在潜在防护措施领域的起草列表中予以文件化，并且需要时应反映在安全结构选项中。在 TR 13335 的第 2 部分和第 3 部分中提供了关于在组织对待 IT 安全的态度之内的公司 IT 安全策略文件的定位及其内容和与其他安全文件的关系的指南。

9 评审网络结构和应用程序

努力加固潜在的防护措施领域的过程的后续步骤，即识别下列因素：

- 将使用的网络连接的类型；
- 网络特性和涉及的相关信任关系；
- 安全风险的类型。

确实应该在已存在的或计划的网络结构和应用程序的情况下来开发潜在防护措施领域的列表（随后就是为了保证特定连接安全的相关设计）。

应获得并评审相关的网络结构和应用程序的详细信息，以提供需要的理解和遵循的过程步骤的前后关系。

通过在越早的阶段澄清这些方面，识别相关的安全要求的识别准则、识别潜在的防护措施领域并优化安全结果的过程就变得越有效并最终产生更加切实有效的安全解决方案。

同时，在早期阶段对网络和应用程序结构方面的考虑运行评审这些结构的时间，如果一个可接受的安全解决方案在目前的结构下无法实际地完成，那么可能还包括修改的时间。

需要考虑的关于网络结构和应用程序的不同领域包括：

- 网络类型；
- 网络协议；
- 网络应用程序。

在下文的 9.2 到 9.4 条款中将讨论为这些领域中的每一个评审的部分问题。其他的考虑将在 9.5 条款中介绍。

（关于网络和应用程序结构的通用指南可参见）

9.2 网络类型

根据网络覆盖区域的不同，将网络分为以下几类：

- 局域网，用于局域系统的内部互联；
- 城域网，用于城市范围的系统的内部互联；
- 广域网，用于在比城域网更大的区域乃至全球范围内系统的内部互联。

9.3 网络协议

不同的协议具有不同的安全特性，并需要进行特殊的考虑。例如：

- 分享介质协议主要应用于局域网（有时候也应用于城域网），并提供管理在连接的系统之间的共享介质的使用。因为使用了共享介质，所以可以通过所有的连接系统对网络上的所有信息进行物理性访问。
- 路由协议被用于定义通过不同节点的路径。信息通过该路径在广域网和城域网内传送。沿着路径的所有系统都可以对信息进行物理访问，并且可以变更路由，无论是蓄意的还是无意的。

9.4 网络应用程序

需要在安全的情况下考虑通过网络使用的应用程序的类型。类型可以包括：

- 基于应用系统的终结竞争；
- 基于应用程序的存储和向前或线圈；
- 客户服务器应用程序。

9.5 其他的考虑