ICS 25.040
N 10

中华人民共和国国家标准

GB/T 30976.1—2014

工业控制系统信息安全
第1部分：评估规范

Industrial control system security—Part 1: Assessment specification

2014-07-24 发布　　2015-02-01 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 30976《工业控制系统信息安全》分为两个部分：

——第1部分：评估规范；

——第2部分：验收规范。

本部分为GB/T 30976的第1部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分由中国机械工业联合会提出。

本部分由全国工业过程测量和控制标准化技术委员会(SAC/TC 124)和全国信息安全标准化技术委员会(SAC/TC 260)归口。

本部分起草单位：机械工业仪器仪表综合技术经济研究所、中国电子技术标准化研究院、北京和利时系统工程有限公司、中国核电工程有限公司、上海自动化仪表股份有限公司、东土科技股份有限公司、中国电力科学研究院、清华大学、西门子(中国)有限公司、浙江大学、西南大学、重庆邮电大学、施耐德电气(中国)有限公司、北京钢铁设计研究总院、华中科技大学、北京奥斯汀科技有限公司、罗克韦尔自动化(中国)有限公司、中国仪器仪表学会、中国科学院沈阳自动化研究所、无线网络安全技术国家工程实验室、西安西电捷通无线网络通信股份有限公司、中央办公厅电子科技学院、北京海泰方圆科技有限公司、青岛多芬诺信息安全技术有限公司、北京国电智深控制技术有限公司、北京力控华康科技有限公司、广东航宇卫星科技有限公司、华北电力设计院工程有限公司、华为技术有限公司、三菱电机自动化(中国)有限公司、中标软件有限公司、横河电机(中国)有限公司北京研发中心。

本部分主要起草人：王玉敏、唐一鸿、隋爱芬、罗安、吕冬宝、张建军、薛百华、陈小淙、高昆仑、王雪、冯冬芹、刘枫、王浩、周纯杰、陈小枫、华镕、张莉、宋岩、李琴、夏德海、胡亚楠、王雄、胡伯良、梅恪、刘安正、田雨聪、方亮、马欣欣、张建勋、杨应良、丁露、王勇、杜佳琳、王亦君、陈日罡、张涛、王玉裴、刘利民、丁青芝、刘文龙、钱晓斌、朱镜灵、张智、龚明、何佳、杨磊。

工业控制系统信息安全
第1部分:评估规范

1 范围

GB/T 30976的本部分规定了工业控制系统(SCADA,DCS,PLC,PCS等)信息安全评估的目标、评估的内容、实施过程等。

本部分适用于系统设计方、设备生产商、系统集成商、工程公司、用户、资产所有人以及评估认证机构等对工业控制系统的信息安全进行评估时使用。

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(包括所有的修改单)适用于本文件。

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

IEC 62443-3-3—2013 工业过程测量和控制安全-网络和系统安全 第3-3系统安全要求和安全等级(SL)

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

脆弱性 vulnerability

系统设计、实现或操作和管理中存在的缺陷或弱点,可被利用来危害系统的完整性或安保策略。

3.1.2

识别 identify

对某一评估要素进行标识与辨别的过程。

3.1.3

评估目标 assessment target

评估活动所要达到的最终目的。

3.1.4

验收 acceptance

风险评估活动中用于结束项目实施的一种方法,主要由被评估方组织机构,对评估活动进行逐项检验,以是否达到评估目标为接受标准。

3.1.5

风险处置 risk treatment

选择并且执行措施来更改风险的过程。

3.1.6

残余风险　residual risk

经过风险处置后遗留的风险。

3.1.7

风险接受　risk acceptance

接受风险的决定。

3.1.8

风险分析　risk analysis

系统地使用信息来识别风险来源和估计风险。

3.1.9

风险评估　risk assessment

风险分析和风险评价的整个过程。

3.1.10

风险管理　risk management

指导和控制一个组织机构相关风险的协调活动。

3.1.11

风险处置　risk treatment

选择并且执行措施来更改风险的过程。

3.1.12

工业控制系统　industrial control system；ICS

对工业生产过程安全(safety)、信息安全(security)和可靠运行产生作用和影响的人员、硬件和软件的集合。

注：系统包括，但不限于：

1) 工业控制系统包括分布式控制系统(DCS)、可编程逻辑控制器(PLC)、智能电子设备(IED)、监视控制与数据采集(SCADA)系统，运动控制(MC)系统、网络电子传感和控制，监视和诊断系统[在本标准中，不论物理上是分开的还是集成的，过程控制系统(PCS)包括基本过程控制系统和安全仪表系统(SIS)]。

2) 相关的信息系统，例如先进控制或者多变量控制、在线优化器、专用设备监视器、图形界面、过程历史记录、制造执行系统(MES)和企业资源计划(ERP)管理系统。

3) 相关的部门、人员、网络或机器接口，为连续的、批处理、离散的和其他过程提供控制、安全和制造操作功能。

3.1.13

安全　safety

免于不可接受的风险。

3.1.14

信息安全　security

a) 保护系统所采取的措施；

b) 由建立和维护保护系统的措施而产生的系统状态；

c) 能够免于非授权访问和非授权或意外的变更、破坏或者损失的系统资源的状态；

d) 基于计算机系统的能力，能够提供充分的把握使非授权人员和系统既无法修改软件及其数据也无法访问系统功能，却保证授权人员和系统不被阻止；

e) 防止对工业自动化和控制系统的非法或有害的入侵，或者干扰其正确和计划的操作。

注：措施可以是与物理信息安全(控制物理访问计算机的资产)或者逻辑信息安全(登录给定系统和应用的能力)相关的控制手段。

3.2 缩略语

下列缩略语适用于本文件。

CL	能力等级	(Capability level)
DCS	分布式控制系统	(Distributed Control System)
ERP	企业资源计划	(Enterprise Resource Planning)
FR	基本要求	(Foundational requirement)
HES	健康、环境和安全	(Health, enviroment and security)
ICS	工业控制系统	(Industrial control system)
IED	智能电子设备	(Intelligent Electronic Device)
MES	制造执行系统	(Manufacturing Execution System)
ML	管理等级	(Management level)
PCS	过程控制系统	(Process Control System)
RE	增强要求	(Requirement enhancement)
SLC	可编程序控制器	(Programmalbe Logic Controller)
SCADA	监视控制与数据采集系统	(Supervisory Control And Data Acquisition)
SIS	安全仪表系统	(Safety Instrumented System)
SL	信息安全等级	(Security level)
SR	系统要求	(System requirement)
VPN	虚拟专用网	(Virtual private network)

4 工业控制系统信息安全概述

4.1 总则

工业控制系统的信息安全特性取决于其设计、管理、健壮性和环境条件等各种因素。系统信息安全的评估应包括在系统生命周期内的设计开发、安装、运行维护、退出使用等各阶段与系统相关的所有活动。必须认识到系统面临的风险在整个生命周期内会发生变化。

评估系统信息安全特性时，应考虑以下各方面：

a) 危险引入点；
b) 危险后果的受体及其影响；
c) 传播途径；
d) 降低风险的措施；
e) 环境条件；
f) 组织机构管理。

注：在系统生命周期的不同阶段，由于某些新危险条件的出现，系统的安全等级会发生变化。

4.2 危险引入点

危险引入点是工业控制系统与非安全设备、系统和网络的接入点。危险源可能来自于工业控制系统的系统外部，也可能来自于工业控制系统的系统内部。安全威胁通过危险引入点并利用传播途径可能对受体造成伤害。危险引入点归结为以下几类，但不限于：

a) 网络和通信的连接点：例如，远程技术支持和访问点、无线接入点、调制解调器网络连接、因特网或物联网连接、遥测网络连接、开放的工业控制系统网络连接、与工业控制系统专网互联的其他网络连接、配置不当的防火墙等；

b) 移动媒体：例如，USB 设备、光盘、移动硬盘等；
c) 不当操作：例如，恶意攻击、无意误操作等；
d) 受感染的现场设备等。

4.3 传播途径

危险源可能通过传播途径对受体造成伤害。通常，可识别单一的传播途径，但在多数情况下，一个完整的传播途径是由若干单一类型的传播途径组合而成。传播途径一般分为以下几类，但不限于：

a) 外部公共网络，如因特网；
b) 内部信息网络；
c) 工控专网(点对点、无线)；
d) 移动存储装置。

4.4 危险后果的受体及其影响

危险后果的受体是指受到破坏时所侵害的客体，包括以下三个方面：

a) 人员；
b) 环境；
c) 资产。

对客体造成的侵害的程度归结为三种，分别对应于：

a) 造成特别严重的损害，A 级；
b) 造成严重损害，B 级；
c) 造成一般损害，C 级。

注：表 1 给出了后果造成侵害的级别。

表 1 后果造成的侵害等级

级别	风险区域								
	业务连续		信息安全			工业操作安全		环境安全	国家经济影响
	一个站点生产中断	多个站点生产中断	直接经济损失(亿元人民币)	刑事责任	社会影响	现场人员	非现场人员	环境	基础设施和服务
A(高)	＞7 d	＞1 d	＞30	重罪刑事罪行	品牌形象损失	死亡	死亡或重大社会事件	大面积长期过度的重大损害	影响多个业务部门或扰乱社区服务
B(中)	＞2 d	＞1 d	＞3	轻罪刑事罪行	失去客户的信任	损失工作日或重大伤害	投诉或当地社区的影响	受地方机构通报	在超越一个公司的水平可能影响到业务部门，社区服务
C(低)	＜1 d	＜1 d	＜3	无	无	急救	无投诉	可释放的极限	几乎无影响

4.5 工业控制系统信息安全评估的内容概述

4.5.1 组织机构管理评估

组织机构管理通常对构成管理体系的基本要素提出相应的要求和为满足这些要求需要实现或解决哪些方面的内容，而不提供如何去开发管理体系。工业控制系统管理机构(资产所有者)面对具有挑战性的新问题时，应当把信息安全作为一个关键内容融合到整个安全运行体系中。那么常见的工程方法是将问题分解成更小的子问题，按照分治方式解决每个子问题。这是解决 ICS 信息安全风险的合理途径。然而，在解决信息安全方面常犯的错误是，试图用一套系统一次解决所有的 ICS 信息安全问题。ICS 信息安全是一个更大的挑战，需要考虑整个 ICS 以及环绕和利用 ICS 的政策、规程、实践和人员等各个方面。实施这样大范围的管理可能需要组织机构内部的文化变革。

在整个组织机构管理范围的基础上解决 ICS 信息安全管理是一项艰巨的任务。因为没有适合所有情况的工业控制系统信息安全实践。信息安全实际上是一个风险和成本的平衡。行业不同面对的情况有所不同。在某些情况下，风险可能与健康、安全、环境(HSE)因素有关而不是单纯的经济影响。风险可能带来不可恢复的后果而不仅仅是暂时性的财务损失。

组织机构管理评估基于 GB/T 22081—2008 第 5 章～第 15 章标准制定，但是引入一个重要的概念，工业控制系统的信息安全风险对 HSE 影响，应与现有风险管理实践结合来应对这些风险。具体的评估内容见第 5 章和附录 A。

4.5.2 工业控制系统能力(技术)评估

系统能力(技术)评估目的是保证系统能够在技术上免受攻击。对于一个运行很好的系统，他应该满足操作和安全两个要求。要提前决定的是什么时候开发项目测试以及供应商和集成商对于网络安全设备或系统的要求保证什么级别。对特殊设备或系统的保证的级别将决定系统能力实现的要求。供应商可能推荐测试方法对于特殊的设备和系统，但是用户将需要确定这些技术是否满足安全要求。

理想情况下，将系统所有状态都进行能力评估，以保证每个安全措施能够满足或可以知道其剩余的风险。尽管完整的系统评估理论上是可能的，但是由于财务和人为约束而不能获得大多数的认证。因此，现在面临的问题是决定可接受的风险等级，执行可接受风险的评估。本部分的内容主要见 IEC 62443-3-3:2013 的第 4 章～第 10 章，分别对应于本部分的第 6 章和附录 B。

4.5.3 与其他安全措施的关联

在工业控制系统环境下，评估人员应该完全理解企业计算机安全政策、规程、与特定设施和/或工业操作相关的健康、安全、环境风险。应小心确保评估不会干扰由工业控制系统设备提供的控制功能，在评估实施前，可能需要使系统离线。

信息安全、物理安全和功能安全可能是密切相关的。在某些情况下，其他安全措施有可能为信息安全提供独立保护层，而附加的信息安全措施也有可能破坏其他安全措施的完整性。因此，在具体的风险评估活动中，应考虑三者潜在的相互作用及其影响后果。

4.5.4 过程环境制约因素

在评估工业控制系统信息安全特性时，应考虑过程环境条件的制约因素，特别是针对在用工业自化控制系统，应考虑现场测试和引入安全技术措施对正常生产过程的影响。在实施现场测试和引入安全技术措施之前，必须分析下列过程环境条件，以确保行动不会影响正常生产过程。

a) 工业控制系统或其子系统承担的任务；

b) 操作人员的能力；

c) 工业控制系统所连接的工业过程的特性；

d) 附加工具或系统对工业控制正常逻辑的影响；

e) 与工业控制系统连接的公用设施(气、电等)。

4.6 评估结果

4.6.1 风险可接受程度

信息安全采取的管理和技术措施建议采取最小影响的原则。

根据工业控制系统的组织机构管理以及系统(技术)能力评估系统的风险，针对风险产生的结果采用信息安全等级(security level，SL)来表示风险管理过程中的不同风险，这样的结果比较直观，根据SL来确定组织机构的整体安全策略和相应的技术防御措施。同时，组织机构应当综合考虑风险控制成本与风险造成的影响，提出一个可接受的风险范围。对某些资产的风险，如果风险计算值在可接受的范围内，则该风险是可接受的，即残余风险在系统允许风险之内说明系统是健壮的，应保持已经有的安全措施；如果风险评估值在可接受的范围外，但是低于不可接受范围的下限值，则该风险需要采取安全措施降低、并控制风险到可接受的程度；如果评估的风险从经济，健康，安全和环境方面进行评估后发现风险是不可以接受的，那么就要对现有的系统重新设计信息安全程序。见图1。其中的风险评估的工具和方法参见附录C。

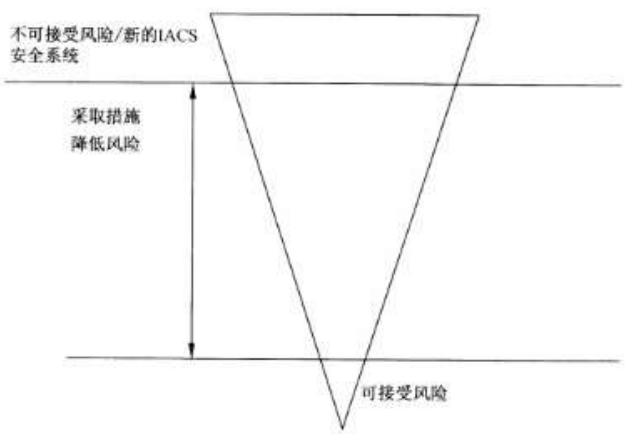

图1 风险可接受的程度

注1：工业控制系统是利用可供选用的各种配置的功能和元件执行要求的任务，系统的该特征难以仅通过评定每一个单独功能和元件的特征来综合评估一个系统的信息安全能力；

注2：工业控制系统信息安全评估的深度在很大程度上取决于系统的复杂程度和边界影响条件以及评估的目的；

注3：评估的范围可以采用汇总统计表的形式，在一个轴线上列出系统的特性另一轴线上列出需考虑的安全影响条件。统计表的方格可用于记录对于每一种系统特性哪一种安全影响条件需要加以考虑。

4.6.2 评估结果等级的划分

评估分为管理评估和系统能力(技术)评估。管理评估宜对照风险接受准则和组织机构相关目标，识别、量化并区分风险的优先次序。风险评估的结果宜指导并确定适当的管理措施及其优先级，评估风险和选择控制措施的过程需要执行多次，以覆盖组织机构的不同部门或各个工业控制系统。

管理评估分为三个级别，分别为管理等级(management level)的ML1、ML2、ML3，由低到高分别对应低级、中级和高级。具体的评估内容见第5章，表格参见表A.1。系统能力(技术)评估分为四个级别，由小到大分别对应系统能力等级(capability level)的CL1、CL2、CL3和CL4，具体的评估内容见第6

章，表格见表 B.1。综合管理评估和系统能力评估的结果，得到工业控制系统的评估结果，亦即信息安全等级（SL1、SL2、SL3、SL4），见表 2。

表 2　工业控制系统的评估结果

信息安全等级				
管理等级	系统能力等级			
	CL1	CL2	CL3	CL4
ML1	SL1	SL1	SL1	SL1
ML2	SL1	SL2	SL2	SL3
ML3	SL1	SL2	SL3	SL4

5　组织机构管理评估

5.1　安全方针

5.1.1　信息安全方针

目标：依据业务要求和相关法律法规提供管理指导并支持信息安全。

要求：管理者应根据业务目标制定清晰的方针指导，并通过在整个组织机构中颁布和维护信息安全方针来表明对信息安全的支持和承诺。

5.1.1.1　信息安全方针文件

控制措施：

信息安全方针文件应由管理者批准、发布并传达给所有员工和外部相关方。

评估指南：

信息安全方针文件应说明管理承诺。并提出组织机构的管理信息安全的方法。方针文件建议包括以下声明：

a）　信息安全、整体目标和范围的定义，以及在允许信息共享机制下安全的重要性；

b）　管理者意图的声明，以支持符合业务策略和目标的信息安全目标和原则；

c）　设置控制目标和控制措施的框架，包括风险评估和风险管理的结构；

d）　对组织机构特别重要的安全方针策略、原则、标准和符合性要求的简要说明，包括：

1）　符合法律法规和合同要求；

2）　安全教育、培训和意识要求；

3）　业务连续性管理；

4）　违反信息安全方针的后果。

e）　信息安全管理（包括报告信息安全事件）的一般和特定职责的定义；

f）　对支持方针的文件的引用，例如，特定信息系统的更详细的安全策略和规程，或用户要遵守安全规则。

5.1.1.2　信息安全方针的评审

控制措施：

应按计划的时间间隔或当重大变化发生时进行信息安全方针评审，以确保持续的适宜性、充分性和

有效性。

评估指南：

信息安全方针应有专人负责，他负有安全方针制定、评审和评价的管理职责。评审要包括评估组织机构信息安全方针改进的机会和管理信息安全适应组织机构环境、业务状况、法律条件或技术环境变化的方法。

信息安全方针评审应考虑管理评审的结果。定义管理评审规程，包括时间表或评审周期。

管理评审的输入建议包括以下信息：

a) 相关方的反馈；

b) 独立评审的结果(见 5.2.1.7)；

c) 预防和纠正措施的状态(见 5.2.1.7 和 5.11.2.1)；

d) 以往管理评审的结果；

e) 过程执行情况和信息安全方针符合性；

f) 可能影响组织机构管理信息安全的方法的变更，包括组织机构环境、业务状况、资源可用性、合同、规章和法律条件或技术环境的变更；

g) 威胁和脆弱性的趋势；

h) 已报告的信息安全事件(见 5.9.1)；

i) 相关政府部门的建议(见 5.2.1.6)。

管理评审的输出建议包括与以下方面有关的任何决定和措施：

a) 组织机构管理信息安全的方法及其过程的改进；

b) 控制目标和控制措施的改进；

c) 资源和/或职责分配的改进；

d) 维护管理评审的记录并获得管理者对修订的方针的批准。

5.2 信息安全组织机构

5.2.1 内部组织机构

目标：管理组织机构范围内信息安全。

应建立管理框架，以启动和控制组织机构范围内的信息安全的实施。

管理者应批准信息安全方针、指派安全角色以及协调和评审整个组织机构安全的实施。

若必要，在组织机构范围内建立专家信息安全建议库，并在组织机构内可用。发展与外部安全专家或组织机构(包括相关权威人士)的联系，以便跟上行业趋势、跟踪标准和评估方法，并且当处理信息安全事件时，提供合适的联络点。

5.2.1.1 信息安全的管理承诺

控制措施：

管理者应通过清晰的说明、可证实的承诺、明确的信息安全职责分配及确认，来积极支持组织机构内的安全。

评估指南：

建议管理者：

a) 确保信息安全目标得以识别，满足组织机构要求，并已被整合到相关过程中；

b) 制定、评审、批准信息安全方针；

c) 评审信息安全方针实施的有效性；

d) 为安全启动提供明确的方向和支持；

e) 为信息安全提供所需的资源；

f) 批准整个组织机构内信息安全专门的角色和职责分配；

g) 启动计划和程序来保持信息安全意识；

h) 确保整个组织机构内的信息安全控制措施的实施是相互协调的(见 5.2.1.2)。

管理者识别内外部专家的信息安全建议的需求，并在整个组织机构内评审和协调专家建议结果。

根据组织机构的规模不同，这些职责可以由一个专门的管理协调小组或由一个已存在的机构(例如董事会)承担。

5.2.1.2 信息安全协调

控制措施：

信息安全活动应由来自组织机构不同部门并具备相关角色和工作职责的代表进行协调。

评估指南：

工业控制系统信息安全协调建议包括工业控制系统专家、管理人员、用户、行政人员、应用设计人员、审核员和安全专员，以及保险、法律、人力资源、IT 或风险管理等领域专家的协调和协作。这些活动能：

a) 确保安全活动的实施与信息安全方针相一致；

b) 确定如何处理不符合项；

c) 核准信息安全的方法和过程，例如风险评估、信息分类；

d) 识别重大的威胁变更和暴露在威胁下的信息和信息处理设施；

e) 评估信息安全控制措施实施的充分性和协调性；

f) 有效地促进整个组织机构内的信息安全教育、培训和意识；

g) 评价在信息安全事件的监视和评审中获得的信息，推荐适当的措施响应识别的信息安全事件。

如果组织机构没有使用一个独立的跨部门的小组，例如因为这样的小组对组织机构规模来说是不适当的，上面描述的措施建议由其他合适的管理机构或单独管理人员实施。

5.2.1.3 信息安全职责的分配

控制措施：

所有的信息安全职责应予以清晰地定义。

评估指南：

信息安全职责的分配宜和信息安全方针(见 5.1)相一致。各个资产的保护和执行特定安全过程的职责要被清晰地识别。在必要时补充这些职责，来为特定地点和信息处理设施提供更详细指南。资产保护和执行特定安全过程(例如业务连续性计划)的局部职责予以清晰地定义。

分配有安全职责的人员可以将安全任务委托给其他人员，但不能因此免除其责任，以保证任何被委托的任务已被正确地执行。

个人负责的领域予以清晰地规定，特别是，进行下列工作：

a) 与每个特殊系统相关的资产和安全过程要予以识别并清晰地定义；

b) 要分配每一资产或安全过程的实体职责，并且该职责的细节要形成文件(见 5.3.1.2)；

c) 授权级别要清晰地予以定义，并形成文件。

在许多组织机构中，应任命一名信息安全管理人员全面负责安全的开发和实施，并支持控制措施识别。

然而，提供控制措施资源并实施这些控制措施的职责通常归于各个管理人员。一种通常的做法为每一项资产指定一名责任人负责该项资产的日常保护。

5.2.1.4 信息处理设施的授权过程

控制措施：

应为新的信息处理设施定义和实施一个管理授权过程。

评估指南：

授权过程考虑下列指南：

a) 新设施要有适当的用户管理授权，以批准其用途和使用；还要获得负责维护本地系统安全环境的管理人员的授权，以确保所有相关的安全方针策略和要求得到满足；

b) 若必要，硬件和软件需进行核查，以确保其与其他系统组件兼容；

c) 使用个人或私有信息处理设施（例如便携式电脑、家用电脑或手持设备）处理业务信息，可能引入新的脆弱性，因此需识别和实施必要的控制措施。

5.2.1.5 保密性协议

控制措施：

应识别并定期评审反映组织机构信息保护需要的保密性或不泄露协议的要求。

评估指南：

保密性或不泄露协议要使用合法的可实施条款来解决保护保密信息的要求。要识别保密性或不泄露协议的要求，建议考虑下列因素：

a) 定义要保护的信息（例如保密信息）；

b) 协议的期望持续时间，包括不确定地需要维持保密性的情形；

c) 协议终止时所需的措施；

d) 签署者的职责和行为，以避免未授权信息泄露（例如“知其所必需”）；

e) 信息、商业秘密和知识产权的所有权，及其如何与保密信息保护相关；

f) 保密信息的许可使用，及签署者使用信息的权力；

g) 对涉及保密信息的活动的审核和监视的权力；

h) 未授权泄露或保密信息破坏的通知和报告过程；

i) 关于协议终止时信息归档或销毁的条款；

j) 违反协议时期望采取的措施。

基于组织机构的安全要求，在保密性或不泄露协议中可能需要其他因素。

保密性和不泄露协议针对他适用的管辖范围遵循所有适用的法律法规（见 5.11.1.1）。周期性评审保密性和不泄露协议的要求，当发生影响这些要求的变更时，也要进行评审。

保密性和不泄密协议保护组织机构信息，并告知签署者他们的职责，以授权、负责的方式保护、使用和公开信息。

对于一个组织机构来说，可能需要在不同环境中使用保密性或不泄密协议的不同格式。

5.2.1.6 与政府部门的联系

控制措施：

应保持与政府相关部门的适当联系。

评估指南：

组织机构的规程中要指明什么时候与哪个部门（例如，执法部门、消防部门、监管部门）联系，以及怀疑已识别的信息安全事件可能触犯了法律时，如何及时报告。

受到来自互联网攻击的组织机构可能需要外部第三方（例如互联网服务提供商或电信运营商）采取措施以应对攻击源。

保持这样的联系可能是支持信息安全事件管理(见5.9.2)或业务连续性和应急规划过程(5.10)的要求。与法规部门的联系有助于预先知道组织机构必须遵循的法律法规方面预期的变化,并为这些变化做好准备。与其他相关部门的联系包括公共设施、紧急服务和安监部门等。

5.2.1.7 信息安全的独立评审

控制措施:

组织机构管理信息安全的方法及其实施(例如信息安全的控制目标、控制措施、策略、过程和规程)应按计划的时间间隔进行独立评审,当安全实施发生重大变化时,也要进行独立评审。

评估指南:

独立评审应由管理者启动。对于确保一个组织机构管理信息安全方法的持续的适宜性、充分性和有效性,这种独立评审是必要的。评审要包括评估安全方法改进的机会和变更的需要,包括方针和控制目标。

这样的评审由独立于被评审范围的人员执行,例如内部审核部门、独立的管理人员或专门进行这种评审的第三方组织机构。从事这些评审的人员要具备适当的技能和经验。

记录独立评审的结果并报告给启动评审的管理者。这些记录加以保持。

如果独立评审识别出组织机构管理信息安全的方法和实施不充分,或不符合信息安全方针文件(见5.1.1.1)中声明的信息安全的方向。管理者应考虑纠正措施。

对于管理人员应定期评审(见5.11.2.1)的范围也可以独立评审。评审方法包括会见管理者、核查记录或安全方针文件的评审。GB/T 19011—2003《质量和(或)环境管理体系审核指南》也提供了实施独立评审的有益指导信息,包括评审方案的建立和实施。5.11.3详细说明了与运行的评估系统独立评审相关的控制措施和系统审计工具的使用。

5.2.2 外部方

目标:保持组织机构被外部方访问、处理、管理或与外部进行通信的信息和信息处理设施的安全。

组织机构的信息和信息处理设施的信息安全不应由于引入外部方的产品或服务而降低。

外部方对组织机构信息处理设施的任何访问、对信息资产的处理和通信都应予以控制。

若有与外部方一起工作的业务需要,他可能要求访问组织机构的信息和信息处理设施、从外部方获得产品和服务,或提供给外部方产品和服务,应进行风险评估以确定涉及信息安全的方面和控制要求。在与外部方签定的协议中宜商定和定义控制措施。

5.2.2.1 与外部方相关风险的识别

控制措施:

应识别涉及外部方业务过程中工业控制系统的信息和信息处理设施的风险,并在允许访问前实施适当的控制措施。

评估指南:

当需要允许外部方访问组织机构的信息处理设施或信息时,应实施风险评估以识别特定控制措施的要求。关于外部方访问的风险的识别建议考虑以下问题:

a) 外部方需要访问的信息处理设施。

b) 外部方对信息和信息处理设施的访问类型,例如:

   1) 物理访问,例如进入中控室、控制现场、电子设备间、档案室;

   2) 逻辑访问,例如访问控制系统、组态信息、数据库;

   3) 组织机构和外部方之间的网络连接,例如,固定连接、远程访问;

   4) 现场访问还是非现场访问。

c) 所涉及信息的价值和敏感性，及对业务运行的关键程度。

d) 为保护不希望被外部方访问到的信息必要的控制措施。

e) 与处理组织机构信息有关的外部方人员。

f) 能够识别组织机构或人员如何被授权访问、如何进行授权验证，以及多长时间需要再确认。

g) 外部方在存储、处理、传送、共享和交换信息过程中所使用的不同的方法和控制措施。

h) 因外部方需要时无法访问，以及由于外部方输入或接收不正确的或是误导的信息而产生的影响。

i) 处理信息安全事件和潜在破坏的惯例和规程，及当发生信息安全事件时外部方持续访问的条款和条件。

j) 需考虑与外部方有关的法律法规要求和其他合同责任。

k) 这些安排对其他利益相关人的利益可能造成怎样的影响。

除非已实施了适当的控制措施，才可允许外部方访问组织机构信息，可行时，应签定合同规定外部方连接或访问以及工作安排的条款和条件。一般而言，与外部方合作引起的安全要求或内部控制措施应通过与外部方的协议反映出来(见 5.2.2.2 和 5.2.2.3)。

要使外部方意识到他们的责任，并且接受在访问、处理、通信或管理组织机构的信息和信息处理设施时所涉及的职责和责任。

安全管理不充分，可能使信息由于外部方介入而处于风险中。要确定和应用控制措施，以管理外部方对信息处理设施的访问。例如，如果对信息的保密性有特殊的要求，就需要使用不泄漏协议。

如果外包程度高，或涉及几个外部方时，组织机构会面临与组织机构间的处理、管理和通信相关的风险。

5.2.2.2 和 5.2.2.3 提出的控制措施涵盖了对不同外部方的安排，例如，建议包括：

a) 服务提供商(例如互联网服务提供商)、网络提供商、电话服务、维护和支持服务；

b) 受管理的安全服务；

c) 顾客；

d) 设施和/或运行的外包；

e) 管理者、业务顾问和审核员；

f) 开发者和提供商，例如软件产品和 ICS 信息安全系统的开发者和提供商；

g) 保洁、餐饮和其他外包支持服务；

h) 临时人员、实习学生和其他临时短期安排。

这些协议有助于减少与外部方相关的风险。

5.2.2.2 处理与顾客有关的安全问题

控制措施：

应在允许顾客访问组织机构信息或资产之前处理所有确定的安全要求。

评估指南：

在允许顾客访问组织机构任何资产(依据访问的类型和范围，并不需要应用所有的条款)前解决安全问题，要充分考虑下列各项：

a) 资产保护，包括：

1) 保护组织机构资产(包括信息和软件)的规程，以及对已知脆弱性的管理；

2) 判定资产是否受到损害(例如丢失数据或修改数据)的规程；

3) 完整性；

4) 对拷贝和公开信息的限制。

b) 拟提供的产品或服务的描述。

c) 顾客访问的不同原因、要求和利益。

d) 访问控制策略，包括：

1) 允许的访问方法，唯一标识符(例如用户 ID 和口令)的控制和使用；

2) 用户访问和权限的授权过程；

3) 没有明确授权的访问均被禁止的声明；

4) 撤销访问权或中断系统间连接的处理。

e) 对信息错误(例如个人信息的错误)、信息安全事件和安全违规进行报告、通知和调查的安排。

f) 每项可用服务的描述。

g) 服务的目标级别和服务的不可接受级别。

h) 监视和撤销与组织机构资产有关的任何活动的权利。

i) 组织机构和顾客各自的义务。

j) 相关法律问题和如何确保满足法律要求(例如，数据保护法律)，如果协议涉及与其他国家顾客的合作，特别要考虑到不同国家的法律体系(也见 5.11.1)。

k) 知识产权(IPR)和版权转让(见 5.11.1.2)以及任何合著作品的保护(见 5.2.1.5)。

与顾客访问组织机构资产有关的安全要求，可能随所访问的信息处理设施和信息的不同而有明显差异。

在顾客协议中明确这些安全要求，包括所有已确定的风险和安全要求(见 5.2.2.1)。

与外部方的协议也可能涉及多方。允许外部方访问的协议要包括允许指派其他合作方，并规定他们访问和介入的条件。

5.2.2.3 处理第三方协议中的安全问题

控制措施：

涉及访问、处理或管理组织机构的信息或信息处理设施以及与之通信的第三方协议，或在信息处理设施中增加产品或服务的第三方协议，应涵盖所有相关的安全要求。

评估指南：

协议要确保在组织机构和第三方之间不存在误解。第三方的保证满足组织机构自己的需要。

为满足识别的安全要求(见 5.2.2.1)，建议考虑将下列各项包含在协议中：

a) 信息安全方针；

b) 确保资产保护的控制措施，包括：

1) 保护组织机构资产(包括信息、软件和硬件)的规程；

2) 所有需要的物理保护控制措施和机制；

3) 确保防范恶意软件(见 5.6.4.1)的控制措施；

4) 判定资产是否受到损害(例如信息、软件和硬件的丢失或修改)的规程；

5) 确保在协议终止时或在合同执行期间，双方同意的某一时刻对信息和资产的返还或销毁的控制措施；

6) 完整性、可用性、保密性和任何其他相关的资产属性；

7) 对拷贝和公开信息，以及保密性协议的使用的限制(见 5.2.1.5)。

c) 对用户和管理员在方法、规程和安全方面的培训；

d) 确保用户意识到信息安全职责和问题；

e) 若适宜，人员调动的规定；

f) 关于硬件和软件安装和维护的职责；

g) 一种清晰的报告结构和商定的报告格式；

h) 一种清晰规定的变更管理过程；

i) 访问控制策略，包括：
   1) 导致必要的第三方访问的不同原因、要求和利益；
   2) 允许的访问方法，唯一标识符(例如用户 ID 和口令)的控制和使用；
   3) 用户访问和权限的授权过程；
   4) 维护被授权使用可用服务的个人清单以及他们与这种使用相关的权利和权限的要求；
   5) 没有明确授权的所有访问都要禁止的声明；
   6) 撤销访问权或中断系统间连接的处理。
j) 报告、通知和调查信息安全事件和安全违规以及违背协议中所声明的要求的安排；
k) 提供的每项产品或服务的描述，根据安全分类(见 5.3.2.1)提供可获得信息的描述；
l) 服务的目标级别和服务的不可接受级别；
m) 可验证的性能准则的定义、监视和报告；
n) 监视和撤销与组织机构资产有关的任何活动的权利；
o) 审核协议中规定的责任、第三方实施的审核、列举审核员的法定权限等方面的权利；
p) 建立逐级解决问题的过程；
q) 服务连续性要求，包括与一个组织机构的业务优先级一致的可用性和可靠性措施；
r) 协议各方的相关义务；
s) 有关法律的责任和如何确保满足法律要求(例如，数据保护法律)，如果该协议涉及与其他国家的组织机构的合作，特别要考虑到不同国家的法律体系(也见 5.11.1)；
t) 知识产权(IPR)和版权转让(见 5.11.1.2)以及任何合著作品的保护(见 5.2.1.5)；
u) 涉及具有次承包商的第三方，要对这些次承包商需要实施安全控制措施；
v) 重新协商/终止协议的条件：
   1) 提供应急计划以处理任一方机构在协议到期之前希望终止合作关系的情况；
   2) 如果组织机构的安全要求发生变化，协议的重新协商；
   3) 资产清单、许可证、协议或与他们相关的权利的当前文件。

协议会随组织机构和第三方机构类型的不同发生很大的变化。因此，要注意在协议中包括所有识别的风险和安全要求(见 5.2.2.1)。必要时，在安全管理计划中扩展所需的控制措施和规程。

如果外包信息安全管理，协议要指出第三方将如何保证维持风险评估中定义的适当的安全，安全如何适于识别和处理风险的变化。

外包和其他形式第三方服务之间的区别包括责任问题、交付期的规划问题、在此期间潜在的运行中断问题、应急规划安排、约定的详细评审以及安全事件信息的收集和管理。因此，组织机构要计划和管理外包安排的交付，并提供适当的过程管理变更和协议的重新协商/终止，这是十分重要的。

需要考虑当第三方不能提供其服务时的连续处理规程，以避免在安排替代服务时的任何延迟。

与外部方的协议也可能涉及多方。允许外部方访问的协议要包括允许指派其他合格者，并规定他们访问以及与访问有关的条件。

与第三方的协议也可能涉及多方。允许第三方访问的协议要包括允许指派其他合格者，并规定他们访问及与访问有关的条件。

一般而言，协议主要由组织机构制定。在一些环境下，也可能有例外，即协议由第三方制定并强加于组织机构。组织机构需要确保其本身的安全不会被没有必要的第三方在强制协议中规定的要求所影响。

5.3 资产管理

5.3.1 对资产负责

目标：实现和保持对组织机构资产的适当保护。

所有资产是可核查的，并且有指定的责任人。

所有资产应指定责任人，并且赋予保持相应控制措施的职责。特定控制措施的实施可以由责任人适当地委派别人承担，但责任人仍有对资产提供适当保护的责任。

5.3.1.1 资产清单

控制措施：

应清晰地识别所有资产，编制并维护所有重要资产的清单。

评估指南：

组织机构识别所有资产并将资产的重要性形成文件。资产清单要包括所有为从灾难中恢复而必要的信息，包括资产类型、格式、位置、备份信息、许可证信息和业务价值。该清单不宜复制其他不必要的清单，但确保内容是相关联的。

另外，商定每一项资产的责任人(见 5.3.1.2)和信息分类(见 5.3.2)，并形成文件。基于资产的重要性、其业务价值和安全级别，识别与资产重要性对应的保护级别。

与信息安全系统相关的资产有很多类型。主要包括：

a) 信息资产：数据库和数据文件、合同和协议、系统文件、研究信息、用户手册、培训材料、操作或支持规程、业务连续性计划、基本维持运行的安排、审核踪迹、归档信息；

b) 软件资产：应用软件、系统软件、开发工具和实用程序；

c) 物理资产：工业控制系统设备、电控设备、通信设备、可移动媒体和其他设备；

d) 服务：设计、安装、调试、运行、维护、计算和通信服务、公用服务设施等；

e) 人员：他们的资格、技能和经验；

f) 无形资产，例如组织机构的声誉和形象。

资产清单可帮助确保有效的资产保护，其他业务目的也可能需要资产清单，例如健康与安全(safety)、保险或财务(资产管理)等原因。编制一份资产清单的过程是风险管理的一个重要的先决条件。

5.3.1.2 资产责任人

控制措施：

与信息处理设施有关的所有信息和资产应由组织机构的指定部门或人员承担责任。

评估指南：

资产责任人要负责：

a) 确保与信息处理设施相关的信息和资产进行了适当的分类；

b) 确定并定期地评审访问限制和分类，并要考虑到可应用的访问控制策略。

责任可以分配给：

a) 业务过程；

b) 已定义的活动集；

c) 应用；

d) 已定义的数据集。

日常任务可以委派给其他人，例如委派给一个管理人员每天照看资产，但责任人仍保留职责。

在复杂的信息系统中，将一组资产指派给一个责任人，可能是比较有用的，他们一起工作来提供特殊的“服务”功能。在这种情况下，服务责任人负责提供服务，包括资产本身提供的功能。

5.3.1.3 资产的可接受使用

控制措施：

与信息处理设施有关的信息和资产可接受使用规则应被确定、形成文件并加以实施。

评估指南：

所有雇员、承包方人员和第三方人员要遵循信息处理设施相关信息和资产的可接受的使用规则，包括：

a) 电子邮件和互联网使用(见5.6.8)规则；

b) 移动设备。尤其是在组织机构外部使用设备的使用指南。

相关管理者提供具体规则或指南。使用或拥有访问组织机构资产权的雇员、承包方人员和第三方人员要意识到他们使用信息处理设施相关的信息和资产以及资源时的限制条件。他们要对其使用信息处理资源以及在他们职责下的使用负责。

5.3.2 信息分类

目标：确保信息受到适当级别的保护。

信息应分类，以在处理信息时指明保护的需求、优先级和期望的安全程度。

信息具有各种程度的敏感性和关键性。某些项可能要求附加等级的保护或特殊处理。信息分类机制用来定义一组合适的保护等级并传达处理措施的需求。

5.3.2.1 分类指南

控制措施：

信息应按照其对组织机构的价值、法律要求、敏感性和关键性予以分类。

评估指南：

信息的分类及相关保护控制措施要考虑到共享或限制信息的业务需求以及与这种需求相关的业务影响。

分类指南包括根据预先确定的访问控制策略(见5.7.1.1)进行初始分类及一段时间后进行重新分类的惯例。

确定资产的类别、对其周期性评审、确保其最新并处于适当的级别，这些都是资产责任人(见5.3.1.2)的职责。分类宜考虑5.6.7.2提及的集合效应。

要考虑分类类别的数目和从其使用中获得的好处。过度复杂的方案可能对使用来说不方便，也不经济，或许是不实际的。在解释从其他组织机构获取的文件的分类标记时要小心，因为其他组织机构可能对于相同或类似命名的标记有不同的定义。

保护级别可通过分析被考虑信息的完整性、可用性、保密性及其他要求进行评估。

在一段时间后，信息通常不再是敏感的或关键的，例如，当该信息已经公开时。这些方面要予以考虑，因为过多的分类致使实施不必要的控制措施，从而导致附加成本。

当分配分类级别时，考虑具有类似安全要求的文件可简化分类的任务。

一般地说，给信息分类是确定该信息如何予以处理和保护的简便方法。

5.3.2.2 信息的标记和处理

控制措施：

应按照组织机构所采纳的分类机制建立和实施一组合适的信息标记和处理规程。

评估指南：

信息标记的规程需要涵盖物理和电子格式的信息资产。

包含分类为敏感或关键信息的系统输出要在该输出中携带合适的分类标记。该标记要根据5.3.2.1中所建立的规则反映出分类。待考虑的项目包括打印报告、屏幕显示、记录介质(例如磁带、磁盘、CD)、电子消息和文件传送。

对每种分类级别，定义包括安全处理、储存、传输、删除、销毁的处理规程。还包括一系列任何安全

相关事态的监督和记录规程。

涉及信息共享的与其他组织机构的协议要包括识别信息分类和解释其他组织机构分类标记的规程。

分类信息的标记和安全处理是信息共享的一个关键要求。物理标记是常用的标记形式。然而，某些信息资产(例如电子形式的文件等)不能做物理标记，而需要使用电子标记手段。例如，通知标记可在屏幕或显示器上显示出来。当标记不适用时，可能需要应用指定信息分类指定的其他方式，例如通过规程或元数据。

5.4 人力资源安全

5.4.1 任用之前

目标：应确保雇员、承包方人员和第三方人员理解其职责、考虑对其承担的角色是适合的，以降低设施被窃、欺诈和误用的风险。

应于任用前在适当的岗位描述、任用条款和条件中指出安全职责。

所有要任用、承包方人员和第三方人员的候选者要充分的审查，特别是对敏感岗位的成员。

使用信息处理设施的雇员、承包方人员和第三方人员要签署关于他们安全角色和职责的协议。

5.4.1.1 角色和职责

控制措施：

雇员、承包方人员和第三方人员的安全角色和职责应按组织机构的信息安全方针定义并形成文件。

评估指南：

安全角色和职责包括了以下要求：

a) 按照组织机构的信息安全方针(见 5.1.1)实施和运行；

b) 保护资产免受未授权访问、泄露、修改、销毁或干扰；

c) 执行特定的安全过程或活动；

d) 确保职责分配给可采取措施的个人；

e) 向组织机构报告安全事态或潜在事态或其他安全风险。

并在任用前对安全角色和职责清晰定义并传达给岗位候选者。

岗位描述能被用来将安全角色和职责形成文件。要清晰地定义并传达没有在组织机构任用过程(例如通过第三方组织机构任用)中任用的个人的安全角色和职责。

5.4.1.2 审查

控制措施：

关于所有任用的候选者、承包方人员和第三方人员的背景验证核查应按照相关法律法规、道德规范和对应的业务要求、被访问信息的类别和察觉的风险来执行。

评估指南：

验证核查要考虑所有相关的隐私、个人数据保护和/或与任用相关的法律，并包括以下内容(允许时)：

a) 令人满意的个人资料的可用性(例如，一项业务和一个个人)；

b) 申请人履历的核查(针对完备性和准确性)；

c) 声称的学术、专业资质的证实；

d) 个人身份核查(护照或类似文件)；

e) 更多细节的核查，例如信用卡核查或犯罪记录核查。

当一个职务(最初任命的或提升的)涉及对信息处理设施进行访问的人时,特别是,如果这些设施正在处理敏感信息,例如,财务信息或高度保密的信息,那么,该组织机构还要考虑进一步的、更详细的核查。

应有规程确定验证核查的准则和限制,例如谁有资格审查人员,以及如何、何时、为什么执行验证核查。

对于承包方人员和第三方人员也要执行审查过程。若承包方人员是通过代理提供的,那么,与代理的合同宜清晰地规定代理对审查的职责,以及如果未完成审查或结果引起怀疑或关注时,这些代理需要遵守的通知规程。同样,与第三方(也见 5.2.2.3)的协议清晰地指定审查的所有职责和通知规程。

被考虑在组织机构内录用的所有候选者的信息要按照相关管辖范围内存在的合适的法律来收集和处理。依据适用的法律,要将审查活动提前通知候选者。

5.4.1.3 任用条款和条件

控制措施:

作为他们合同义务的一部分,雇员、承包方人员和第三方人员应同意并签署他们的任用合同的条款和条件,这些条款和条件声明他们在组织机构中的信息安全职责。

评估指南:

任用的条款和条件除澄清和声明以下内容外,还要反映组织机构的安全方针:

a) 所有访问敏感信息的雇员、承包方人员和第三方人员宜在给予访问信息处理设施权之前签署保密或不泄露协议;

b) 雇员、承包方人员和其他人员的法律责任和权利,例如关于版权法、数据保护法(见 5.11.1.1 和 5.11.1.2);

c) 与雇员、承包方人员和第三方人员操作的信息系统和服务有关的信息分类和组织机构资产管理的职责(见 5.3.2.1 和 5.6.7.3);

d) 雇员、承包方人员和第三方人员操作来自其他公司或外部方的信息的职责;

e) 组织机构处理人员信息的职责,包括由于组织机构任用或在组织机构任用过程中产生的信息;

f) 扩展到组织机构场所之外和正常工作时间之外的职责,例如在家中工作的情形(见 5.5.2.5 和 5.7.7.1);

g) 如果雇员、承包方人员和第三方人员漠视组织机构的安全要求所要采取的措施(见 5.4.2.3)。

组织机构要确保雇员、承包方人员和第三方人员同意适用于他们将访问的与信息系统和服务有关的组织机构资产的性质和程度的信息安全条款和条件。

若适用,包含于任用条款和条件中的职责要在任用结束后持续一段规定的时间(见 5.4.3)。

一个行为细则可覆盖雇员、承包方人员和第三方人员关于保密性、数据保护、道德规范、组织机构设备和设施的适当使用以及组织机构期望的最佳实践的职责。承包方人员或第三方人员可能与一个外部组织机构有关,这个外部组织机构可能需要代表已签约的人遵守契约的安排。

5.4.2 任用中

目标:确保所有的雇员、承包方人员和第三方人员知悉信息安全威胁和利害关系、他们的职责和义务,并准备好在其正常工作过程中支持组织机构的安全方针,以减少人为出错的风险。

应确定管理职责来确保安全措施应用于组织机构内个人的整个任用期。

为尽可能减小安全风险,对所有雇员、承包方人员和第三方人员提供安全规程的适当程度的意识、教育和培训以及信息处理设施的正确使用方法。还要建立一个正式的处理安全违规的纪律处理过程。

5.4.2.1 管理职责

控制措施:

管理者应要求雇员、承包方人员和第三方人员按照组织机构已建立的方针策略和规程对安全尽心尽力。

评估指南：

管理职责包括确保雇员、承包方人员和第三方人员：

a) 在被授权访问敏感信息或信息系统前了解其信息安全角色和职责；

b) 获得声明他们在组织机构中角色的安全期望的指南；

c) 被激励以实现组织机构的安全策略；

d) 对于他们在组织机构内的角色和职责的相关安全问题的意识程度达到一定级别；

e) 遵守任用的条款和条件，包括组织机构的信息安全方针和工作的合适方法；

f) 持续拥有适当的技能和资质。

如果雇员、承包方人员和第三方人员没有意识到他们的安全职责，他们会对组织机构造成相当大的破坏。被激励的人员更可靠并能减少信息安全事件的发生。

缺乏有效的管理会使员工感觉被低估，并由此导致对组织机构的负面安全影响。例如，缺乏有效的管理可能导致安全被忽视或组织机构资产的潜在误用。

5.4.2.2 信息安全意识、教育和培训

控制措施：

组织机构的所有雇员，适当时，包括承包方人员和第三方人员，应受到与其工作职能相关的适当的意识培训和组织机构方针策略及规程的定期更新培训。

评估指南：

意识培训要从一个正式的介绍过程开始，这个过程用来在允许访问信息或服务前介绍组织机构的安全方针策略和期望。

持续地培训要包括安全要求、法律职责和业务控制，还有正确使用信息处理设施的培训，例如登录规程、软件包的使用和纪律处理过程(见 5.4.2.3)的信息。

安全意识、教育和培训活动要与员工的角色、职责和技能相关，并包括关于已知威胁的信息，向谁咨询进一步的安全建议以及合适的报告信息安全事件(见 5.9.1)的渠道。

加强意识的培训旨在使个人认识到信息安全问题及事件，并按照他们岗位角色的需要对其响应。

5.4.2.3 违规处理过程

控制措施：

对于安全违规的雇员，应有一个正式的纪律处理过程。

评估指南：

纪律处理过程之前要有一个安全违规的验证过程(见 5.9.2.3 的证据收集)。

正式的纪律处理过程宜确保正确和公平的对待被怀疑安全违规的雇员。无论违规是第一次或是已发生过，无论违规者是否经过适当的培训，正式的纪律处理过程规定一个分级的响应。要考虑例如违规的性质、重要性及对于业务的影响等因素，相关法律、业务合同和其他因素也是需要考虑的。对于严重的明知故犯的情况，要立即免职、删除访问权和特殊权限，如果必要，直接护送出现场。

纪律处理过程也可用于对雇员、承包方人员和第三方人员的一种威慑，防止他们违反组织机构的安全策略和规程及其他安全违规。

5.4.3 任用的终止或变更

目标：确保雇员、承包方人员和第三方人员以一个规范的方式退出一个组织机构或改变其任用关系。

应有合适的职责确保管理雇员、承包方人员和第三方人员从组织机构退出，并确保他们归还所有设备及删除他们的所有访问权。

组织机构内职责和任用的变更管理应符合本章内容，与职责或任用的终止管理相似，任何新的任用宜遵循 5.4.1 的内容进行管理。

5.4.3.1 终止职责

控制措施：

任用终止或任用变更的职责应清晰地定义和分配。

评估指南：

终止职责的传达要包括正在进行的安全要求和法律职责，适当时，还包括任何保密协议规定的职责（见 5.2.1.5），并且在雇员、承包方人员或第三方人员的雇佣结束后持续一段时间仍然有效的任用条款和条件（见 5.4.1.3）。

规定职责和义务在任用终止后仍然有效的内容宜包含在雇员、承包方人员或第三方人员的合同中。

职责或任用的变更管理宜与职责或任用的终止管理相似，新的任用责任宜遵循 5.4.1 的内容。

人力资源的职能通常是与管理相关规程的安全方面的监督管理员一起负责总体的任用终止处理。

在承包方人员的情况下，终止职责的处理可能由代表承包方人员的代理完成，其他情况下的用户可能由他们的组织机构来处理。

有必要通知雇员、顾客、承包方人员或第三方人员关于组织机构人员的变更和运营上的安排。

5.4.3.2 资产的归还

控制措施：

所有的雇员、承包方人员和第三方人员在终止任用、合同或协议时应归还他们使用的所有组织机构资产。

评估指南：

终止过程要被正式化，包括所有先前发放的软件、公司文件和设备的归还。其他组织机构资产，例如移动计算设备、信用卡、访问卡、软件、手册和存储于电子介质中的信息也需要归还。

当雇员、承包方人员或第三方人员购买了组织机构的设备或使用他们自己的设备时，要遵循规程确保所有相关的信息已转移给组织机构，并且已从设备中安全地删除（见 5.6.7.1）。

当一个雇员、承包方人员或第三方人员拥有的知识对正在进行的操作具有重要意义时，此信息要形成文件并传达给组织机构。

5.4.3.3 撤销访问权

控制措施：

所有雇员、承包方人员和第三方人员对信息和信息处理设施的访问权应在任用、合同或协议终止时删除，或在变化时调整。

评估指南：

任用终止时，个人对与信息系统和服务有关的资产的访问权宜被重新考虑。这将决定删除访问权是否是必要的。任用的变更要体现在不适用于新岗位的访问权的删除上。删除或改变的访问权包括物理和逻辑访问、密钥、ID 卡、信息处理设施（见 5.7.2.4）、签名，并要从标识其作为组织机构的现有成员的文件中删除。如果一个已离开的雇员、承包方人员或第三方人员知道仍保持活动状态的账户的密码，则应在任用、合同或协议终止或变更后改变口令。

对信息资产和信息处理设施的访问权在任用终止或变更前是否减少或删除，依赖于对风险因素的评价，例如：

a) 终止或变更是由雇员、承包方人员或第三方人员发起还是由管理者发起，以及终止的原因；

b) 雇员、承包方人员或任何其他用户的现有职责；

c) 当前可访问资产的价值。

在某些情况下，访问权的分配基于对多人可用而不是只基于离开的雇员、承包方人员或第三方人员，例如组 ID。在这种情况下，从组访问列表中删除离开的人员，还要建议所有相关的其他雇员、承包方人员和第三方人员不要再与已离开的人员共享信息。

在管理者发起终止的情况下，不满的雇员、承包方人员或第三方人员可能故意破坏信息或破坏信息处理设施。在员工辞职的情况下，他们可能为将来的使用而收集必要的信息。

5.5 物理和环境安全

5.5.1 安全区域

目标：防止对组织机构场所和信息的未授权物理访问、损坏和干扰。

关键或敏感的信息处理设施应放置在安全区域内，并受到确定的安全周边的保护，包括适当的安全屏障和入口控制。这些设施要在物理上避免未授权访问、损坏和干扰。

所提供的保护要与所识别的风险相匹配。

5.5.1.1 物理安全周边

控制措施：

应使用安全周边(诸如墙、卡控制的入口或有人管理的接待台等屏障)来保护包含工业控制系统设施的区域。

评估指南：

对于物理安全周边，若合适，考虑和实施下列指南：

a) 安全周边清晰地予以定义，各个周边的设置地点和强度取决于周边内资产的安全要求和风险评估的结果；

b) 包含信息处理设施的建筑物或场地的周边要在物理上是安全的(即，在周边或区域内不要存在可能易于闯入的任何缺口)；场所的外墙是坚固结构，所有外部的门要使用控制机制来适当保护，以防止未授权进入，例如，身份识别仪器、门禁系统、报警器、锁、控制柜等。

c) 对场所或建筑物的物理访问手段要到位(如有人管理的接待区域或其他控制)；进入场所或建筑物要仅限于已授权人员；

d) 如果可行，要建立物理屏障以防止未经授权进入，或防止环境污染；

e) 安全周边的所有防火门要可发出报警信号、被监视并经过测试，与墙一起按照我国相关标准建立所需的防卫级别；他们要使用故障保护方式按照当地防火规则来运行；

f) 要按照我国标准安装适当的安防监测系统，并定期测试以覆盖所有的外部门窗；要一直警惕空闲区域；其他区域要提供掩护方法，例如计算机室或通信室；

g) 组织机构管理的信息处理设施要在物理上与第三方管理的设施分开。

其他信息物理保护可以通过在组织机构边界和信息处理设施周围设置一个或多个物理屏障来实现。多重屏障的使用将提供附加保护，一个屏障的失效不意味着立即危及到安全。

一个安全区域可以是一个可上锁的房间，或是被连续的内部物理安全屏障包围的几个区域。在安全边界内具有不同安全要求的区域之间需要控制物理访问的附加屏障和周边。

具有多个组织机构的建筑物要考虑专门的物理访问安全。

5.5.1.2 物理入口控制

控制措施：

安全区域应由适合的人员控制所保护，以确保只有授权的人员才允许访问。

评估指南：

要考虑下列指南：

a) 记录访问者进入和离开的日期和时间，所有的访问者要予以监督，除非他们的访问事前已经经过批准；只允许他们访问特定的、已授权的目标，并要向他们宣布关于该区域的安全要求和应急规程的说明。

b) 访问处理敏感信息或储存敏感信息的区域要受到控制，并且仅限于已授权的人员；鉴别控制（例如，访问控制卡加个人识别号）应用于授权和确认所有访问；所有访问的审核踪迹要安全地加以维护。

c) 所有雇员、承包方人员和第三方人员以及所有访问者要佩戴某种形式的可视标识，如果遇到无人护送的访问者和未佩戴可视标识的任何人要立即通知保安人员。

d) 第三方支持服务人员只有在需要时才能有限制的访问安全区域或敏感信息处理设施；这种访问要被授权并受监视。

e) 对安全区域的访问权要定期地予以评审和更新，并在必要时废除（见 5.4.3.3）。

5.5.1.3 办公室、房间和设施的安全保护

控制措施：

应为办公室、房间和设施设计并采取物理安全措施。

评估指南：

为保护办公室、房间和设施，要考虑下列指南：

a) 相关的健康与安全（safety）法规和标准要考虑在内；

b) 关键设施要坐落在可避免公众进行访问的场地；

c) 如果可行，建筑物要不引人注目，并且在建筑物内侧或外侧用不明显的标记给出其用途的最少指示，以标识信息处理活动的存在；

d) 标识敏感信息处理设施位置的目录和内部电话簿不要轻易被公众得到。

5.5.1.4 外部和环境威胁的安全防护

控制措施：

为防止火灾、洪水、地震、爆炸、社会动荡和其他形式的自然或人为灾难引起的破坏，应设计和采取物理保护措施。

评估指南：

考虑任何邻近区域所带来的安全威胁，例如，邻近建筑物的火灾、屋顶漏水或地下室地板渗水或者街上爆炸。

为避免火灾、洪水、地震、爆炸、社会动荡和其他形式的自然灾难或人为灾难的破坏，要考虑以下指南：

a) 危险或易燃材料要在离安全区域安全距离以外的地方存放。大批供应品（例如文具）不要存放于安全区域内；

b) 基本维持运行的设备和备份介质的存放地点要与主要场所有一段安全的距离，以避免影响主要场所的灾难产生的破坏；

c) 要提供适当的灭火设备，并要放在合适的地点。

5.5.1.5 在安全区域工作

控制措施：

应设计和应用用于安全区域工作的物理保护和指南。

评估指南：

要考虑下列指南：

a) 只在有必要知道的基础上，员工才应知道安全区域的存在或其中的活动；

b) 为了安全原因和减少恶意活动的机会，均要避免在安全(safety)区域内进行不受监督的工作；

c) 未使用的安全区域在物理上要上锁并定期地予以核查；

d) 除非授权，不要允许携带摄影、视频、声频或其他记录设备，例如移动设备中的照相机。

在安全区域工作的安排包括对工作在安全区域内的雇员、承包方人员和第三方人员的控制，以及对其他发生在安全区域的第三方活动的控制。

5.5.1.6 公共访问、交接区安全

控制措施：

访问点(例如交接区)和未授权人员可进入办公场所的其他点应加以控制，如果可能，应与信息处理设施隔离，以避免未授权访问。

评估指南：

考虑下列指南：

a) 由建筑物外进入交接区的访问要局限于已标识的和已授权的人员；

b) 交接区要设计为在无需交货人员获得对本建筑物其他部分的访问权的情况下就能卸下物资；

c) 当内部门打开时，交接区的外部门要得到安全保护；

d) 在进来的物资从交接区运到使用地点之前，要检查是否存在潜在威胁(见 5.5.2.1d)；

e) 进来的物资要按照资产管理规程(见 5.3.1.1)在场所的入口处进行登记；

f) 如果可能，进入和运出的货物要在物理上予以隔离。

5.5.2 设备安全

目标：防止设备资产的丢失、损坏、失窃或危及资产安全以及相关组织机构活动的中断。

应保护设备免受物理的和环境的威胁。

对设备(包括离开组织机构使用和财产移动)的保护是减少未授权访问信息的风险和防止丢失或损坏所必需的。

这样做还要考虑设备安置和处置。可能需要专门的控制用来防止物理威胁以及防护支持性设施，例如供电和电缆基础设施。

5.5.2.1 设备安置和保护

控制措施：

应安置或保护设备，以减少由环境威胁和危险所造成的各种风险以及未授权访问的机会。

评估指南：

为保护设备，建议考虑下列指南：

a) 设备要进行适当安置，以尽量减少不必要的对工作区域的访问；

b) 要把处理敏感数据的信息处理设施放在适当的限制观测的位置，以减少在其使用期间信息被窥视的风险，还要保护储存设施以防止未授权访问；

c) 要求专门保护的部件要予以隔离，以降低所要求的总体保护等级；

d) 要采取控制措施以最小化潜在的物理威胁的风险，例如偷窃、火灾、爆炸、烟雾、水(或供水故障)、尘埃、振动、化学影响、电源干扰、通信干扰、电磁辐射和故意破坏；

e) 要建立在信息处理设施附近进食、喝饮料和抽烟的指南；

f) 对于可能对信息处理设施运行状态产生负面影响的环境条件(例如温度和湿度)要予以监视;
g) 所有建筑物都要采用避雷保护,所有进入的电源和通信线路都要装配雷电保护过滤器;
h) 对于工业环境中的设备,要考虑使用专门的保护方法,例如键盘保护膜;
i) 要保护处理敏感信息的设备,以最小化因辐射而导致信息泄露的风险。

5.5.2.2 支持性设施

控制措施:

应保护设备使其免于由支持性设施的失效而引起的电源故障和其他中断。

评估指南:

a) 要有足够的支持性设施(例如电、供水、排污、加热/通风和空调)来支持系统。支持性设施定期检查并适当的测试以确保他们正常工作和减少由于他们的故障或失效带来的风险。按照设备制造商的说明提供合适的供电。
b) 对支持关键业务操作的设备,推荐使用支持有序关机或连续运行的不间断电源(UPS)。电源应急计划要包括UPS故障时要采取的措施。如果电源故障延长,而处理要继续进行,则考虑备份发电机。
c) 要提供足够的燃料供给,以确保在延长的时间内发电机可以进行工作。UPS设备和发电机宜定期地核查,以确保他们拥有足够能力,并按照制造商的建议予以测试。另外,宜考虑使用多来源电源,或者如果办公场所很大,则考虑使用一个单独变电站。
d) 应急电源开关宜位于设备房间应急出口附近,以便紧急情况时快速切断电源。万一主电源出现故障时提供应急照明。
e) 要有稳定和足够的供水以支持空调、加湿设备和灭火系统(当使用时)。供水系统的故障可能破坏设备或阻止有效的灭火。如果需要,要评价和安装报警系统来检测支撑实施的故障。
f) 连接到设施提供商的通信设备至少有两条不同线路以防止在一条连接路径发生故障时语音服务失效。要有足够的语音服务以满足国家法律对于应急通信的要求。
g) 实现连续供电的选项包括多路供电,以避免供电的单一故障点。

5.5.2.3 布缆安全

控制措施:

应保证传输数据或支持信息服务的电源布缆和通信布缆免受窃听或损坏。

评估指南:

对于布缆安全,建议考虑下列指南:

a) 进入信息处理设施的电源和通信线路宜在地下。若可能,或提供足够的可替换的保护。
b) 网络布缆要免受未授权窃听或损坏,例如,利用电缆管道或使路由避开公共区域。
c) 为了防止干扰,电源电缆要与通信电缆分开。
d) 要使用清晰的可识别的电缆和设备记号,以使处理差错最小化,例如,错误网络电缆的意外配线。
e) 要使用文件化配线列表减少出错的可能性。
f) 对于敏感的或关键的系统,更进一步的控制措施考虑要包括:
   1) 在检查点和终接点处安装铠装电缆管道和上锁的房间或盒子;
   2) 使用可替换的路由选择和/或传输媒体,以提供适当的安全性;
   3) 使用光缆;
   4) 使用电磁防辐射装置保护电缆;
   5) 对于电缆连接的未授权装置要主动实施技术清除和物理检查;

6) 控制对配线盘和电缆室的访问。

5.5.2.4 设备维护

控制措施：

设备应予以正确地维护，以确保其持续的可用性和完整性。

评估指南：

对于设备维护，建议考虑下列指南：

a) 要按照供应商推荐的服务时间间隔和规范对设备进行维护；

b) 只有已授权的维护人员才可对设备进行修理和服务；

c) 要保存所有可疑的或实际的故障以及所有预防和纠正维护的记录；

d) 当对设备安排维护时，要实施适当的控制，并考虑到维护是由场所内部人员执行还是由组织机构外部人员执行；当必要时，敏感信息要从设备中删除或者维护人员要是足够可靠的；

e) 要遵守由保险策略所施加的所有要求。

5.5.2.5 组织机构场所外的设备安全

控制措施：

应对组织机构场所外的设备采取安全措施，要考虑工作在组织机构场所以外的不同风险。

评估指南：

无论责任人是谁，在组织机构场所外使用任何信息处理设备都要通过管理者授权。

对于离开场所的设备的保护，建议考虑下列信息：

a) 离开建筑物的设备和媒体在公共场所，应有必要的看管措施；

b) 制造商的设备保护说明要始终加以遵守，例如，防止暴露于强电磁场内；

c) 远程工作的控制措施要根据风险评估确定，当适合时，要施加合适的控制措施；

d) 要有足够的安全保障掩蔽物，以保护离开办公场所的设备。

安全风险在不同场所可能有显著不同，例如，损坏、盗窃和截取，要考虑确定最合适的控制措施。

用于远程工作或从正常工作地点运走的信息存储和处理设备包括所有形式的个人计算机、管理设备、移动电话、智能卡、纸张或其他形式的设备。

关于保护移动设备的其他方面的更多信息在 5.7.7.1 中可以找到。

5.5.2.6 设备的安全处置或再利用

控制措施：

包含储存介质的设备的所有项目应进行核查，以确保在处置之前，任何敏感信息和注册软件已被删除或安全地写覆盖。

评估指南：

包含敏感信息的设备在物理上要予以摧毁，或者采用使原始信息不可获取的技术破坏、删除或写覆盖，而不能采用标准的删除或格式化功能。

包含敏感信息的已损坏的设备可能需要实施风险评估，以确定这些设备是否要进行销毁，而不是送去修理或丢弃。

信息可能通过对设备的草率处置或重用而被泄漏(见 5.6.7.2)。

5.5.2.7 资产的移动

控制措施：

设备、信息或软件在授权之前不应带出组织机构场所。

评估指南：

建议考虑下列指南：

a) 在未经事先授权的情况下，不要让设备、信息或软件离开组织机构场所；

b) 要明确识别有权允许资产移动，离开办公场所的雇员、承包方人员和第三方人员；

c) 要设置设备移动的时间限制，并在返还时执行符合性核查；

d) 若必要并合适，要对设备作出移出记录，当返回时，要作出送回记录。

执行检测未授权资产移动的抽查，以检测未授权的记录装置、设备等，防止他们进入组织机构场所。

这样的抽查要按照相关法律和规章执行。要让每个人都知道将进行抽查，并且只能在法律法规要求的适当授权下执行核查。

5.6 通信和操作管理

5.6.1 操作规程和职责

目标：确保对信息处理设施进行正确、安全的操作。

应建立所有信息处理设施的管理与操作的职责和规程。这包括制定合适的操作规程。

当合适时，要实施责任分割，以减少疏忽或故意误用系统的风险。

5.6.1.1 文件化操作规程

控制措施：

操作规程应形成文件、保持并对所有需要的用户可用。

评估指南：

与信息处理和通信设施相关的系统活动应具备形成文件的规程。例如计算机启动和关机规程、备份、设备维护、媒体处理、计算机机房、邮件处置管理和安全(safety)等。

操作规程宜详细规定执行每项工作的说明，其内容包括：

a) 信息处理和处置；

b) 备份(见 5.6.5)；

c) 时间安排要求，包括与其他系统的相互关系、最早工作开始时间和最后工作完成期限；

d) 对在工作执行期间可能出现的处理差错或其他异常情况的指导，包括对使用系统实用工具的限制(见 5.7.5.4)；

e) 出现不期望操作或技术困难时的支持性联络；

f) 特定输出及介质处理的指导，例如使用特殊信纸或管理保密输出，包括任务失败时输出的安全处置规程(见 5.6.7.2 和 5.6.7.3)；

g) 供系统失效时使用的系统重启和恢复规程；

h) 审核踪迹和系统日志信息的管理(见 5.6.9)。

要将操作规程和系统活动的文件化规程看作正式的文件，其变更由管理者授权。技术上可行时，信息系统要使用相同的规程、工具和实用程序进行一致的管理。

5.6.1.2 变更管理

控制措施：

对信息处理设施和系统的变更应加以控制。

评估指南：

运行系统和应用软件宜有严格的变更管理控制。

特别是，建议考虑下列各项：

a) 重大变更的标识和记录；

b) 变更的策划和测试；

c) 对这种变更的潜在影响的评估，包括安全影响；

d) 对建议变更的正式批准规程；

e) 向所有有关人员传达变更细节；

f) 基本维持运行的规程，包括从不成功变更和未预料事态中退出和恢复的规程与职责。

正式的管理者职责和规程要到位，以确保对设备、软件或规程的所有变更有令人满意的控制。当发生变更时，包含所有相关信息的审核日志要予以保留。

对信息处理设施和系统的变更缺乏控制是系统故障或安全失效的常见原因。对运行环境的变更，特别是当系统从开发阶段向运行阶段转移时。可能影响应用的可靠性(见 5.8.5.1)。

对运行系统的变更宜在仅存在一个有效的业务需求时进行，例如系统风险的增加。使用操作系统或应用程序的最新版本进行系统更新并不总是业务需求，因为这样做可能会引入比现有版本更多的脆弱性和不稳定性。尤其是在移植期间，还需要额外培训、许可证费用、支持、维护和管理开支以及新的硬件等。

5.6.1.3 责任划分

控制措施：

各类责任及职责范围应加以划分，以降低未授权或无意识的修改或不当使用组织机构资产的机会。

评估指南：

责任划分是一种减少意外或故意系统误用的风险的方法。应当注意，在无授权或未被检测时，要使个人不能访问、修改或使用资产。事件的启动要与其授权分离。共谋的可能性要在设计控制措施时予以考虑。

小型组织机构可能感到难以实现这种责任划分，但只要具有可能性和可行性，要尽量使用该原则。如果难以划分，要考虑其他控制措施，例如对活动、审核踪迹和管理监督的监视等。重要的是安全审核仍保持独立。

5.6.1.4 开发、测试和运行设施分离

控制措施：

开发、测试和运行设施应分离，以减少未授权访问或改变运行系统的风险。

评估指南：

为防止运行问题，应识别运行、测试和开发环境之间的分离级别，并实施适当的控制措施。

建议考虑下列各项：

a) 要规定从开发状态到运行状态的软件传递规则并形成文件；

b) 开发和运行软件要在不同的系统或计算机处理器上以及在不同的域或目录内运行；

c) 没有必要时，编译器、编辑器和其他开发工具或系统实用工具不要从运行系统上访问；

d) 测试系统环境要尽可能的仿效运行系统环境；

e) 用户在运行和测试系统中使用不同的用户角色，菜单显示合适的标识消息以减少出错的风险；

f) 敏感数据不要拷贝到测试系统环境中(见 5.8.4.2)。

开发和测试活动可能引起严重的问题。例如，文件或系统环境的不期望修改或者系统故障。在这种情况下，有必要保持一种已知的和稳定的环境，在此环境中可执行有意义的测试并防止不适当的开发者访问。

若开发和测试人员访问运行系统及信息，那么他们可能会引入未授权和未测试的代码或改变运行数据。在某些系统中，这种能力可能被误用于实施欺诈，或引入未测试的、恶意的代码，从而导致严重的

运行问题。

开发者和测试者还造成对运行信息保密性的威胁。如果开发和测试活动共享同一计算环境，那么可能引起非故意的软件和信息的变更。因此，为了减少意外变更或未授权访问运行软件和业务数据的风险，分离开发、测试和运行设施是有必要的(见 5.8.4.2)。

5.6.2 第三方服务交付管理

目标：实施和保持符合第三方服务交付协议的信息安全和服务交付的适当水准。

组织机构应宜核查协议的实施，监视协议执行的符合性，并管理变更，以确保交付的服务满足与第三方商定的所有要求。

5.6.2.1 服务交付

控制措施：

应确保第三方实施、运行和保持包含在第三方服务协议中的安全控制措施、服务定义和交付水准。

评估指南：

第三方服务交付应包括商定的安全安排、服务定义和服务管理的各方面。在外包安排的情况下，组织机构宜策划必要的过渡(信息、信息处理设施和其他需要移动的任何资产)，并确保安全在整个过渡期间得以保持。

组织机构要确保第三方保持足够的服务能力和可使用的计划以确保商定的服务水平在主要服务故障或灾难(见 5.10.1)后继续得以保持。

5.6.2.2 第三方服务的监视和评审

控制措施：

应定期监视和评审由第三方提供的服务、报告和记录，审核也应定期执行。

评估指南：

第三方服务的监视和评审要确保坚持协议的信息安全条款和条件，并且信息安全事件和问题得到适当的管理。这将涉及组织机构和第三方之间的服务管理关系和过程，包括：

a) 监视服务执行级别以核查对协议的符合程度；
b) 评审由第三方产生的服务报告，安排协议要求的定期进展会议；
c) 当协议和所有支持性指南及规程需要时，提供关于信息安全事件的信息并由第三方和组织机构实施评审；
d) 评审第三方的审核踪迹及关于交付服务的安全事态、运行问题、失效、故障追踪和中断的记录；
e) 解决和管理所有已确定的问题。

管理与第三方关系的职责要分配给指定人员或服务管理组。另外，组织机构要确保第三方分配了核查符合性和执行协议要求的职责。要获得足够的技术技能和资源来监视满足协议的要求(见 5.2.2.3)，特别是信息安全要求。当在服务交付中发现不足时，采取适当的措施。

组织机构要对第三方访问、处理或管理的敏感或关键信息或信息处理设施的所有安全方面保持充分的全面的控制和可见度。组织机构要确保他们在安全活动中留有可见度，例如变更管理、脆弱性识别和信息安全事件报告/响应，事件的报告/响应使用清晰定义的报告过程、格式及结构。

外包时，组织机构要知晓由外包方处理的信息的最终职责仍属于组织机构。

5.6.2.3 第三方服务的变更管理

控制措施：

应管理服务提供的变更，包括保持和改进现有的信息安全策略、规程和控制措施，并考虑到业务系

统和涉及过程的关键程度及风险的再评估。

评估指南：

对第三方服务变更的管理过程需要考虑：

a) 组织机构要实施的变更：

1) 对提供的现有服务的加强；

2) 任何新应用和系统的开发；

3) 组织机构策略和规程的更改或更新；

4) 解决信息安全事件和改进安全的新的控制措施。

b) 第三方服务实施的变更：

1) 对网络的变更和加强；

2) 新技术的使用；

3) 新产品或新版本的采用；

4) 新的开发工具和环境；

5) 服务设施物理位置的变更；

6) 供应商的变更。

5.6.3 系统规划和验收

目标：将系统失效的风险降至最小。

为确保足够容量和资源的可用性以提供所需的系统性能，需要预先的规划和准备。应作出对于未来容量需求的推测，以减少系统过载的风险。新系统的运行要求应在验收和使用之前建立、形成文件并进行测试。

5.6.3.1 容量管理

控制措施：

资源的使用应加以监视、调整，并作出对于未来容量要求的预测，以确保拥有所需的系统性能。

评估指南：

对于每一个新的和正在进行的活动来说，应识别容量要求。要使用系统调整和监视以确保和改进（必要时）系统的可用性和效率。要有检测控制措施以及时地指出问题。对未来容量要求的推测要考虑新业务、系统要求以及组织机构信息处理能力的当前和预计的趋势。

需要特别关注与长订货交货周期或高成本相关的所有资源，因此管理人员要监视关键系统资源的利用，他们要识别出使用的趋势，特别是与业务应用或管理信息系统工具相关的使用。

管理人员使用该信息来识别和避免可能威胁到系统安全或服务的潜在的瓶颈及对关键员工的依赖，并策划适当的措施。

5.6.3.2 系统验收

控制措施：

应建立对新信息系统、升级及新版本的验收准则，并且在开发中和验收前对系统进行适当的测试。

评估指南：

管理人员要确保验收新系统的要求和准则被明确地定义、商定、形成文件并经过测试。新信息系统升级和新版本只有在获得正式验收后，才能进入生产环节。在验收之前，建议考虑下列项目：

a) 性能和计算机容量要求；

b) 差错恢复和重启规程以及应急计划；

c) 按照已定义标准，准备和测试日常的运行规程；

d) 确定的安全控制措施要到位；

e) 有效的人工操作规程；

f) 业务连续性安排(见 5.10.1)；

g) 新系统的安装对现有系统无负面影响的数据，特别是在高峰处理时间；

h) 考虑新系统对组织机构总体安全影响的证据；

i) 新系统的操作或使用培训；

j) 易用性，这影响到用户使用，避免人员出错。

对于主要的新的开发，在开发过程的各阶段要征询运行职能部门和用户的意见，以确保所建议的系统设计的运行效率。要进行适当的测试，以证实完全满足全部验收标准。

验收可能包括一个正式的认证和认可过程，以验证已经适当解决了安全要求。

5.6.4 防范恶意和移动代码

目标：保护软件和信息的完整性。

要求有预防措施，以防范和检测恶意代码和未授权的移动代码的引入。

软件和信息处理设施易感染恶意代码(例如计算机病毒、网络蠕虫、特洛伊木马和逻辑炸弹)。

应让用户了解恶意代码的危险。若合适，管理人员应引入控制措施，以防范、检测并删除恶意代码，并控制移动代码。

5.6.4.1 控制恶意代码

控制措施：

应实施恶意代码的检测、预防和恢复的控制措施，以及适当的提高用户安全意识的规程。

评估指南：

防范恶意代码要基于恶意代码检测和修复软件、安全意识、适当的系统访问和变更管理控制措施。

建议考虑下列指南：

a) 建立禁止使用未授权软件的正式策略(见 5.11.1.2)；

b) 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上获得的文件和软件相关，此策略指示要采取什么保护措施；

c) 对支持关键业务过程的系统中的软件和数据内容进行定期评审。要正式调查存在的任何未批准的文件或未授权的修正；

d) 安装和定期更新恶意代码检测和修复软件来扫描计算机和介质，以作为预防控制或作为例行程序的基础；执行的核查要包括：

   1) 针对恶意代码，使用前核查电子或光介质文件，以及从网络上收到的文件；

   2) 针对恶意代码，使用前核查电子邮件附件和下载内容；该核查要在不同位置进行，例如，在电子邮件服务器、台式计算机或进入组织机构的网络时；

   3) 针对恶意代码，核查 web 页面。

e) 定义关于系统恶意代码防护、他们使用的培训、恶意代码攻击报告和从中恢复的管理规程和职责(见 5.9.1 和 5.9.2)；

f) 制定适当的从恶意代码攻击中恢复的业务连续性计划，包括所有必要的数据和软件的备份以及恢复安排(见 5.10)；

g) 实施规程定期收集信息，例如订阅邮件列表和/或核查提供新恶意代码的 web 站点；

h) 实施检验与恶意代码相关信息的规程，并确保报警公告是准确情报；管理人员宜确保使用合格的来源(例如，声誉好的期刊、可靠的 Internet 网站或防范恶意代码软件的供应商)，以区分虚假的和真实的恶意代码；要让所有用户了解欺骗问题，以及在收到他们时要做什么。

可安装防恶意代码软件，提供定义文件和扫描引擎的自动更新，以确保防护措施是最新的。另外，也可在每一台台式机上安装该软件，以执行自动核查。

应注意防止在实施维护和紧急规程期间引入恶意代码，因为他们可能旁路正常的恶意代码防护的控制措施。

5.6.4.2 控制移动代码

控制措施：

当授权使用移动代码时，其配置应确保授权的移动代码按照清晰定义的安全策略运行，阻止执行未授权的移动代码。

评估指南：

为防止移动代码执行未授权的活动，考虑下列措施：

a) 在逻辑上隔离的环境中执行移动代码；

b) 阻断移动代码的所有使用；

c) 阻断移动代码的接收；

d) 使技术措施在一个特定系统中可用，以确保移动代码受控；

e) 控制移动代码访问的可用资源；

f) 使用密码控制，以唯一地鉴别移动代码。

移动代码是一种软件代码，他能从一台计算机传递到另一台计算机，随后自动执行并在很少或没有用户干预的情况下完成特定功能。移动代码与大量的中间件服务有关。

除确保移动代码不包含恶意代码外，控制移动代码是必要的，以避免系统、网络或应用资源的未授权使用或破坏，以及其他信息安全违规。

5.6.5 备份

目标：保持信息和信息处理设施的完整性及可用性。

应为备份数据和演练及时恢复建立例行规程来实施已商定的方针和策略(见 5.10.1)。

5.6.5.1 信息备份

控制措施：

应按照已设的备份策略，定期备份和测试信息和软件。

评估指南：

提供足够的备份设施，以确保所有必要的信息和软件能在灾难或介质故障后进行恢复。

对于信息备份，建议考虑下列各项：

a) 要定义备份信息的必要级别；

b) 要建立备份拷贝的准确完整的记录和文件化的恢复规程；

c) 备份的程度(例如全部备份或部分备份)和频率要反映组织机构的业务要求、涉及信息的安全要求和信息对组织机构持续运作的关键度；

d) 备份要存储在一个远程地点，有足够距离，以避免主办公场所灾难时受到损坏；

e) 要给予备份信息一个与主办公场所应用标准相一致的适当的物理和环境保护等级(见 5.5)。要扩展应用于主办公场所介质的控制措施，以涵盖备份场所；

f) 若可行，要定期测试备份介质，以确保当必要的应急使用时可以依靠这些备份介质；

g) 恢复规程要定期核查和测试，以确保他们有效，并能在操作规程恢复所分配的时间内完成；

h) 在保密性十分重要的情况下，备份要通过加密方法进行保护。

各个系统的备份安排要定期测试以确保他们满足业务连续性计划(见 5.10)的要求。对于关键的系

统，备份安排要包括在发生灾难时恢复整个系统所必要的所有系统信息、应用和数据。

要确定最重要业务信息的保存周期以及对要永久保存的档案拷贝的任何要求(见 5.11.1.3)。

为使备份和恢复过程更容易，备份可安排为自动进行。这种自动化解决方案宜在实施前进行充分的测试，并做到定期测试。

5.6.6 网络安全管理

目标：确保网络中信息的安全性并保护支持性的基础设施。

可能跨越组织机构边界的网络安全管理，需要仔细考虑数据流、法律含义、监视和保护。

还可以要求另外的控制，以保护在公共网络上传输的敏感数据。

5.6.6.1 网络控制

控制措施：

应充分管理和控制网络，以防止威胁的发生，维护使用网络的系统和应用程序的安全，包括传输中的信息。

评估指南：

网络管理员应实施控制，以确保网络上的信息安全、防止未授权访问所连接的服务。特别是，建议考虑下列各项：

a) 若合适，网络的操作职责要与计算机操作分开(见 5.6.1.3)；

b) 要建立远程设备(包括用户区域内的设备)管理的职责和规程；

c) 要建立专门的控制，以防护在公用网络上或无线网络上传递数据的保密性和完整性，并且保护已连接的系统及应用(见 5.7.4 和 5.8.3)；为维护所连接的网络服务和计算机的可用性，还可以要求专门的控制；

d) 为记录安全相关的活动，要使用适当的日志记录和监视措施；

e) 为优化对组织机构的服务和确保在信息处理基础设施上始终如一地应用若干控制措施，要紧密地协调管理活动。

5.6.6.2 网络服务安全

控制措施：

安全特性、服务级别以及所有网络服务的管理要求应予以确定并包括在所有网络服务协议中。无论这些服务是由内部提供的还是外包的。

评估指南：

网络服务提供商以安全方式管理商定服务的能力要予以确定并定期监视，还宜商定审核的权利。

要识别特殊服务的安全安排，例如安全特性、服务级别和管理要求。组织机构要确保网络服务提供商实施了这些措施。

网络服务包括接入服务、私有网络服务、增值网络和受控的网络安全解决方案，例如防火墙和入侵检测系统。这些服务既包括简单的未受控的带宽也包括复杂的增值的提供。

网络服务的安全特性可以是：

a) 为网络服务应用的安全技术，例如，鉴别(可参见多种方法，如 ISO/IEC 9798 和 ISO/IEC 20009-2)、加密和网络访问控制(可参见多种方法，如 GB/T 28455—2012)；

b) 按照安全和网络连接规则，网络服务的安全连接需要的技术参数；

c) 若必要，网络服务使用规程，以限制对网络服务或应用的访问。

5.6.7 介质处置

目标：防止资产遭受未授权泄露、修改、移动或销毁以及业务活动的中断。

介质应受到控制和物理保护。

为使文件、计算机介质(如磁带、磁盘)、输入/输出数据和系统文件免遭未授权泄露、修改、删除和破坏,应建立适当的操作规程。

5.6.7.1 可移动介质的管理

控制措施:

应有适当的可移动介质的管理规程。

评估指南:

对于可移动介质的管理,建议考虑下列指南:

a) 对于从组织机构取走的任何可重用的介质中的内容,如果不再需要,要使其不可重现;
b) 如果必要并可行,对于从组织机构取走的所有介质要求授权,所有这种移动的记录要加以保持,以保持审核踪迹;
c) 要将所有介质存储在符合制造商说明的安全、保密的环境中;
d) 如果存储在介质中的信息使用时间比介质生命期长,则还要将信息存储在别的地方,以避免由于介质老化而导致信息丢失;
e) 要考虑可移动介质的登记,以减少数据丢失的机会;
f) 只要在有业务要求时,才使用可移动介质;
g) 移动存储介质只允许在规定的安全区域内使用。

所有规程和授权级别宜清晰地形成文件。

可移动介质包括磁带、磁盘、闪盘、可移动硬件驱动器、CD、DVD等。

5.6.7.2 介质的处置

控制措施:

不再需要的介质,应使用正式的规程可靠并安全地处置。

评估指南:

应建立安全处置介质的正式规程,以使敏感信息泄露给未授权人员的风险减至最小。安全处置包含敏感信息介质的规程宜与信息的敏感性相一致。建议考虑下列各项:

a) 包含有敏感信息的介质宜秘密和安全地存储和处置,例如,利用焚化或切碎的方法,或者将数据删除供组织机构内其他应用使用;
b) 要有规程识别可能需要安全处置的项目;
c) 安排把所有介质部件收集起来并进行安全处置,比试图分离出敏感部件可能更容易;
d) 许多组织机构对纸、设备和介质提供收集和处置服务;注意选择具有足够控制措施和经验的合适的承包方;
e) 若有可能,处置敏感部件要做记录,以便保持审核踪迹。

当处置堆积的介质时,对集合效应要予以考虑,其可能使大量不敏感信息变成敏感信息。

敏感信息可能由于粗心大意的介质处置而被泄露(见5.5.2.6)。

5.6.7.3 信息处理规程

控制措施:

应建立信息的处理及存储规程,以防止信息的未授权的泄漏或不当使用。

评估指南:

制定规程来处置、处理、存储或传达与分类一致的信息(见5.3.2)。建议考虑下列各项:

a) 按照所显示的分类级别,处置和标记所有介质;

b) 确定防止未授权人员访问的限制；
c) 维护数据的授权接收者的正式记录；
d) 确保输入数据完整，正确完成了处理并应用了输出确认；
e) 按照与其敏感性一致的级别，保护等待输出的脱机数据；
f) 根据制造商的规范存储介质；
g) 使分发的数据最少；
h) 清晰地标记介质的所有拷贝，以引起已授权接收者的关注；
i) 以固定的时间间隔评审分发列表和已授权接收者列表。

这些规程应用于文件、计算系统、网络、移动计算、移动通信、邮件、语音邮件、通用语音通信、多媒体、邮政服务/设施、传真机的使用和任何其他敏感项目(例如，空白支票、发票)中的信息。

5.6.7.4 系统文件安全

控制措施：

应保护系统文件以防止未授权的访问。

评估指南：

对于系统文件安全，考虑下列条款：

a) 安全地存储系统文件；
b) 将系统文件的访问人员列表保持在最小范围，并且由应用责任人授权；
c) 要妥善地保护保存在公用网络上的或经由公用网络提供的系统文件。

其他信息系统文件可能包含一系列敏感信息，例如，应用过程的描述、规程、数据结构、授权过程。

5.6.8 信息的交换

目标：保持组织机构内以及与组织机构外信息和软件交换的安全。

组织机构间信息和软件的交换应基于一个正式的交换策略，按照交换协议执行，还要服从任何相关法律(见 5.11)。

应建立规程和标准，以保护传输中的信息和包含的物理介质。

5.6.8.1 信息交换策略和规程

控制措施：

应有正式的交换策略、规程和控制措施，以保护通过使用各种类型通信设施的信息交换。

评估指南：

使用电子通信设施进行信息交换的规程和控制建议考虑下列各项：

a) 设计用来防止交换信息遭受截取、复制、修改、错误寻址和破坏的规程；
b) 检测和防止可能通过使用电子通信传输的恶意代码的规程(见 5.6.4.1)；
c) 保护以附件形式传输的敏感电子信息的规程；
d) 简述电子通信设施可接受使用的策略或指南(见 5.3.1.3)；
e) 无线通信使用的规程，要考虑所涉及的特定风险；
f) 雇员、承包方人员和所有其他使用人员不危害组织机构的职责，例如诽谤、扰乱、扮演、连锁信寄送、未授权购买等；
g) 密码技术的使用，例如保护信息的保密性、完整性和真实性(见 5.8.3)；
h) 所有业务通信(包括消息)的保持和处理指南，要与相关国家和地方法律法规一致；
i) 不将敏感或关键信息留在打印设施上，例如复印机、打印机和传真机，因为这些设施可能被未授权人员访问；

j) 与通信设施转发相关的控制措施和限制，例如将电子邮件自动转发到外部邮件地址；

k) 提醒工作人员，他们要采取相应预防措施，例如，为不泄露敏感信息，避免打电话时通过下列方式被无意听到或窃听：

1) 他们周围的人，特别是当使用移动电话时；

2) 搭线窃听，以及通过物理访问手持电话或电话线路，或者使用扫描接收器的其他窃听方式；

3) 接收端的人。

l) 不要将包含敏感信息的消息留在应答机上，因为可能被未授权个人重放，也不能留在公用系统或者由于误拨号而被不正确地存储；

m) 提醒工作人员关于传真机的使用问题，即：

1) 未授权访问内置消息存储器，以检索消息；

2) 有意的或无意的对传真机编程，将消息发送给特定的电话号码；

3) 由于误拨号或使用错误存储的号码将文件和消息发送给错误的电话号码。

n) 提醒工作人员不要注册统计数据，例如任何软件中的电子邮件地址或其他人员信息，以避免未授权人员收集；

o) 提醒工作人员现代的传真机和影印机都有页面缓冲并在页面或传输故障时存储页面，一旦故障消除，这些将被打印。

另外，要提醒工作人员，不要在公共场所或开放办公室和不隔音墙的会场进行保密会谈。

信息交换设施要符合所有相关的法律要求(见 5.11)。

可能通过使用多种不同类型的通信设施进行信息交换，例如电子邮件、声音、传真和视频。

可能通过多种不同类型的介质进行软件交换，包括从互联网下载和从出售现货的供应商处获得。

要考虑与电子数据交换、电子通信和控制要求相关的业务、法律和安全含义。

由于在使用信息交换设施时缺乏意识、策略或规程，因此可能泄露信息，例如，在公开场所的移动电话被偷听、电子邮件消息的错发、应答机被偷听，未授权访问拨号语音邮件系统或使用传真设备意外地将传真发送到错误的传真设备上。

如果通信设施失灵、过载或中断，则可能中断业务运行并损害信息(见 5.6.3 和 5.10)。如果上述通信设施被未授权用户所访问，也可能损害信息(见 5.7)。

5.6.8.2 交换协议

控制措施：

应建立组织机构与外部方交换信息和软件的协议。

评估指南：

交换协议建议考虑以下安全项目：

a) 控制和通知传输、分派和接收的管理职责；

b) 通知传输、分派和接收的发送者的规程；

c) 确保可追溯性和不可抵赖性的规程；

d) 打包和传输的最低技术标准；

e) 有条件转让契约；

f) 送信人标识标准；

g) 如果发生信息安全事件的职责和义务，例如数据丢失；

h) 商定的标记敏感或关键信息的系统的使用，确保标记的含义能直接理解，信息受到适当的保护；

i) 数据保护、版权、软件许可证符合性及类似考虑的责任和职责(见 5.11.1.2 和 5.11.1.4)；

j) 记录和阅读信息和软件的技术标准；

k) 为保护敏感项，可以要求任何专门的控制措施，例如密钥(见 5.8.3)。

要建立和保持策略、规程和标准，以保护传输中的信息和物理介质(见 5.6.8.3)，这些还要在交换协议中进行引用。

任何协议的安全内容要反映涉及的业务信息的敏感度。

协议可以是电子的或手写的，可能采取正式合同或任用条款的形式。对敏感信息而言，信息交换使用的特定机制对于所有组织机构是一致的。

5.6.8.3 运输中的物理介质

控制措施：

包含信息的介质在组织机构的物理边界以外运送时，应防止未授权的访问、不当使用或毁坏。

评估指南：

为保护不同地点间传输的信息介质，建议考虑下列指南：

a) 要使用可靠的运输或信使；

b) 授权的信使列表要经管理者批准；

c) 要开发核查信使识别的规程；

d) 包装要足以保护信息免遭在运输期间可能出现的任何物理损坏，并且符合制造商的规范(例如对软件的说明)，例如防止町能减少介质恢复效力的任何环境因素，例如暴露于过热、潮湿或电磁区域；

e) 若必要，要采取专门的控制，以保护敏感信息免遭未授权泄露或修改。例子包括：

1) 使用可上锁的容器；

2) 手工交付；

3) 防篡改的包装(他可以揭示任何想获得访问的企图)；

4) 在异常情况下。把托运货物分解成多次交付，并且通过不同的路线发送。

信息在物理传输期间(例如通过邮政服务或送信人传送)易受未授权访问、不当使用或破坏。

5.6.8.4 电子消息发送

控制措施：

包含在电子消息发送中的信息应给予适当的保护。

评估指南：

电子消息发送的安全考虑建议包括以下方面：

a) 防止消息遭受未授权访问、修改或拒绝服务攻击；

b) 确保正确的寻址和消息传输；

c) 服务的通用可靠性和可用性；

d) 法律方面的考虑，例如电子签名的要求；

e) 在使用外部公共服务(例如即时消息或文件共享)前获得批准；

f) 更强的用以控制从公开可访问网络进行访问的鉴别级别。

电子消息(例如电子邮件、电子数据交换、即时消息)在业务通信中充当一个日益重要的角色。电子消息与基于通信的纸质文件相比有不同的风险。

5.6.8.5 业务信息系统

控制措施：

应建立并实施策略和规程，以保护与业务信息系统互联相关的信息。

评估指南：

对于互联的安全和业务蕴涵的考虑建议包括：

a) 信息在组织机构的不同部门间共享时，在管理和会计系统中已知的脆弱性；

b) 业务通信系统中的信息的脆弱性，例如，记录电话呼叫或会议呼叫、呼叫的保密性、传真的存储、打开的邮件、邮件的分发；

c) 管理信息共享的策略和适当的控制措施；

d) 如果系统不提供适当级别的保护(见 5.3.2)，则排除敏感业务信息和分级文件；

e) 限制访问与特定人员(例如，参与敏感项目的工作人员)相关的日志信息；

f) 允许使用系统的工作人员、承包方人员或业务伙伴的类别以及可以访问该系统的位置(见 5.2.2.2和 5.2.2.3)；

g) 对特定类别的用户限制于所选定的设施；

h) 识别出用户的身份，例如，组织机构的雇员。或者为其他用户利益的目录中的承包方人员；

i) 系统上存放的信息的保留和备份(见 5.6.5.1)；

j) 基本维持运行的要求和安排(见 5.10)。

办公信息系统可通过结合使用文件、计算机、移动计算、移动通信、邮件、语音邮件、通用语音通信、多媒体、邮政服务/设施和传真机，来快速传播和共享业务信息。

5.6.9 监视

目标：检测未经授权的信息处理活动。

应监视系统，记录信息安全事态。宜使用操作员日志和故障日志以确保识别出信息系统的问题。

一个组织机构的监视和日志记录活动要遵守所有相关法律的要求。

要使用系统监视以核查所采用控制措施的有效性，并验证与访问策略模型的一致性。

5.6.9.1 审计记录

控制措施：

应产生记录用户活动、异常情况和信息安全事态的审计日志，并保持一个已设的周期以支持将来的调查和访问控制监视。

评估指南：

审计日志在需要时建议包括：

a) 用户 ID；

b) 日期、时间和关键事态的细节，例如登录和退出；

c) 若有可能，终端身份或位置；

d) 成功的和被拒绝的对系统尝试访问的记录；

e) 成功的和被拒绝的对数据以及其他资源尝试访问的记录；

f) 系统配置的变更；

g) 特殊权限的使用；

h) 系统实用工具和应用程序的使用；

i) 访问的文件和访问类型；

j) 网络地址和协议；

k) 访问控制系统引发的警报；

l) 防护系统的激活和停用，例如防病毒系统和入侵检测系统。

审计日志包含入侵和保密人员的数据，要采取适当的隐私保护措施(见 5.11.1.4)。可能时，系统管理员不应有删除或停用他们自己活动日志的权利(见 5.6.1.3)。

5.6.9.2 监视系统的使用

控制措施：

应建立信息处理设施的监视使用规程，并经常评审监视活动的结果。

评估指南：

各个设施的监视级别要由风险评估决定。一个组织机构要符合所有相关的适用于监视活动的法律要求。建议考虑的范围包括：

a) 授权访问，包括细节，例如：
   1) 用户 ID；
   2) 关键事态的日期和时间；
   3) 事态类型；
   4) 访问的文件；
   5) 使用的程序/工具。
b) 所有特殊权限操作，例如：
   1) 特殊权限账户的使用，例如监督员、根用户、管理员；
   2) 系统的启动和停止；
   3) I/O 设备的装配/拆卸。
c) 未授权的访问尝试，例如：
   1) 失败的或被拒绝的用户行为；
   2) 失败的或被拒绝的涉及数据和其他资源的行为；
   3) 违反网关和防火墙的访问策略(的访问)及其通知；
   4) 私有入侵检测系统的警报，以便能够识别入侵者探试、恶意攻击的非法行为。
d) 系统警报或故障，例如：
   1) 控制台警报或消息；
   2) 系统日志异常；
   3) 网络管理警报；
   4) 访问控制系统引发的警报。
e) 改变或试图改变系统的安全设置和控制措施。

监视活动的结果多长时间进行评审宜依赖于涉及的风险，建议考虑的风险因素包括：

a) 应用过程的关键程度；
b) 所涉及信息的价值、敏感度和关键程度；
c) 系统渗透和不当使用的经历，脆弱性被利用的频率；
d) 系统互连接的程度(尤其是公共网络)；
e) 设备被停用的日志记录；
f) 使用监视规程是必要的，以确保用户只执行被明确授权的活动；
g) 日志评审包括系统所面临威胁的理解和可能出现的方式。更多关于事件的例子见 5.9.1.1。

5.6.9.3 日志信息的保护

控制措施：

记录日志的设施和日志信息应加以保护，以防止篡改和未授权的访问。

评估指南：

应实施控制措施以防止日志设施被未授权更改和出现操作问题，包括：

a) 更改已记录的消息类型；

b) 日志文件被编辑或删除；

c) 超越日志文件介质的存储容量，导致不能记录事态或过去记录事态被写覆盖。

一些审计日志可能需要被存档，以作为记录保持策略的一部分或由于收集和保留证据的要求。系统日志通常包含大量的信息，其中许多与安全监视无关。为帮助识别出对安全监视目的有重要意义的事态，要考虑将相应的消息类型自动地拷贝到第二份日志和/或使用适合的系统实用工具或审计工具执行文件查询及规范化。

需要保护系统日志，因为如果其中的数据被修改或删除，可能导致一个错误的安全判断。

5.6.9.4 管理员和操作员日志

控制措施：

系统管理员和系统操作员的活动应记入日志。

评估指南：

日志包括：

a) 事态(成功的或失败的)发生的时间；

b) 关于事态(例如处理的文件)或故障(例如发生的差错和采取的纠正措施)的信息；

c) 涉及的账号和管理员或操作员；

d) 涉及的过程。

系统管理员和操作员日志要定期评审。

对在系统和网络管理员控制之外进行管理的入侵检测系统可以用来监视系统和网络管理活动的符合性。

5.6.9.5 故障日志

控制措施：

故障应被记录、分析，并采取适当的措施。

评估指南：

与信息处理或通信系统的问题有关的用户或系统程序所报告的故障应加以记录。对于处置所报告的故障要有明确的规则，包括：

a) 评审故障日志，以确保故障已得到令人满意的解决；

b) 评审纠正措施，以确保没有损害控制措施，以及所采取的措施给予了充分授权。

如果具有出错记录的系统功能，要确保该功能处于开启状态。

出错和故障日志记录能影响系统的性能。这些日志记录要由胜任的员工激活，对各个系统所需的日志记录的级别由风险评估决定，要考虑性能的降低。

5.6.9.6 时钟同步

控制措施：

一个组织机构或安全域内的所有相关信息处理设施的时钟应使用已设的精确时间源进行同步。

评估指南：

若计算机或通信设备有能力运行实时时钟，则时钟应置为商定的标准，例如，世界标准时间(uTc)或本地标准时间。当已知某些时钟随时间漂移，要有一个核查和校准所有重大变化的规程。日期/时间格式的正确解释对确保时间戳反映实时的日期/时间是重要的。还要考虑局部特殊性(例如夏令时间)。

正确设置计算机时钟对确保审计记录的准确性是重要的，审计日志可用于调查或作为法律、纪律处理的证据。不准确的审计日志可能妨碍调查，并损害这种证据的可信性。链接到国家原子钟无线电广播时间的时钟可用于记录系统的主时钟。可以用网络时间协议保持所有服务器与主时钟同步。

5.7 访问控制

5.7.1 访问控制的业务要求

目标：控制对信息的访问。

对信息、信息处理设施和业务过程的访问应在业务和安全要求的基础上予以控制。

访问控制规则应考虑到信息传播和授权的策略。

5.7.1.1 访问控制策略

控制措施：

访问控制策略应建立、形成文件，并基于业务和访问的安全要求进行评审。

评估指南：

应在访问控制策略中清晰地规定每个用户或每组用户的访问控制规则和权利。访问控制包括逻辑的和物理的(见 5.5)，他们要一起考虑。给用户和服务提供商提供一份清晰的满足业务要求的说明。

策略建议考虑下列内容：

a) 各个业务应用的安全要求；

b) 与业务应用相关的所有信息的标识和信息面临的风险；

c) 信息传播和授权的策略，例如，了解原则和安全等级以及信息分类的需要(见 5.3.2)；

d) 不同系统和网络的访问控制策略和信息分类策略之间的一致性；

e) 关于保护访问数据或服务的相关法律和合同义务(见 5.11.1)；

f) 组织机构内常见工作角色的标准用户访问轮廓；

g) 在认可各种可用的连接类型的分布式和网络化环境中的访问权的管理；

h) 访问控制角色的分割，例如访问请求、访问授权、访问管理；

i) 访问请求的正式授权要求(见 5.7.2.1)；

j) 访问控制的定期评审要求(见 5.7.2.4)；

k) 访问权的取消(见 5.4.3.3)。

在规定访问控制规则时，要认真考虑下列内容：

a) 将强制性规则和可选的或有条件的指南加以区分；

b) 在“未经明确允许，则一律禁止”的前提下，而不是“未经明确禁止，一律允许”的弱规则的基础上建立规则；

c) 信息处理设施自动启动的信息标记(见 5.3.2)和用户任意启动的信息标记的变更；

d) 信息系统自动启动的用户许可变更和由管理员启动的那些用户许可变更；

e) 在颁发之前，需要特别批准的规则以及无须批准的那些规则。

访问控制规则要有正式的规程支持，并清晰地定义职责。

5.7.2 用户访问管理

目标：确保授权用户访问信息系统，并防止未授权的访问。

应有正式的规则来控制对信息系统和服务的访问权的分配。

这些规则应涵盖用户访问生存周期内的各个阶段，从新用户初始注册到不再需要访问信息系统和服务的用户的最终注销。适当时，要特别注意对有特殊权限的访问权的分配加以控制的需要，这种访问权可以使用户越过系统的控制措施。

5.7.2.1 用户注册

控制措施：

应有正式的用户注册及注销规程，来授权和撤销对所有信息系统及服务的访问。

评估指南：

用户注册和注销的访问控制规程建议包括：

a) 使用唯一用户 ID，使得用户与其行为链接起来，并对其行为负责；在对于业务或操作而言必要时，才允许使用组 ID，并经过批准和形成文件；

b) 核查使用信息系统或服务的用户是否具有该系统拥有者的授权；取得管理者对访问权的单独批准也是合适的；

c) 核查所授予的访问级别是否与业务目的(见 5.7.1)相适合，是否与组织机构的安全方针保持一致，例如，它没有违背责任分割原则(见 5.6.1.3)；

d) 给用户一份关于其访问权的书面声明；

e) 要求用户签署表示理解访问条件的声明；

f) 确保直到已经完成授权规程，服务提供者才提供访问；

g) 维护一份注册使用该服务的所有人员的正式记录；

h) 立即取消或封锁工作角色或岗位发生变更、或离开组织机构的用户的访问权；

i) 定期核查并取消或封锁多余的用户 ID 和账号(见 5.7.2.4)；

j) 确保多余的用户 ID 不会发给其他用户。

要考虑基于业务要求建立用户访问角色。将大量的访问权归结到典型的用户访问轮廓中。在这种角色级别上对访问请求和评审(见 5.7.2.4)进行管理要比在特定的权限级别上容易些。

要考虑在人员合同和服务合同中将在员工或服务代理试图进行未授权访问时的有关处罚措施的条款包括进去(见 5.2.1.5、5.4.1.3 和 5.4.2.3)。

5.7.2.2 特殊权限管理

控制措施：

应限制和控制特殊权限的分配及使用。

评估指南：

需要防范未授权访问的多用户系统应通过正式的授权过程使特殊权限的分配受到控制。要考虑下列步骤：

a) 要标识出与每个系统产品(例如，操作系统、数据库管理系统和每个应用程序)相关的访问特殊权限，以及需要将其分配的用户；

b) 特殊权限要按照访问控制策略(见 5.7.1.1)在“按需使用”和“一事一议”的基础上分配给用户，即仅当需要时，才为其职能角色分配最低要求；

c) 要维护所分配的各个特殊权限的授权过程及其记录。在未完成授权过程之前，不要授予特殊权限；

d) 要促进开发和使用系统例行程序，以避免把特殊权限授予用户的需要；

e) 要促进开发和使用避免具有特殊权限才能运行的程序；

f) 特殊权限要被分配一个不同于正常业务用途所用的用户 ID。

系统管理特殊权限(使用户无视系统或应用控制措施的信息系统的任何特性或设施)的不恰当使用可能是一种导致系统故障或违规的主要因素。

5.7.2.3 用户口令管理

控制措施：

应通过正式的管理过程控制口令的分配。

评估指南：

此过程要包括下列要求：

a) 要求用户签署一份声明，以保证个人口令的保密性和组口令仅在该组成员范围内使用；签署的声明可包括在任用条款和条件中(见 5.4.1.3)；
b) 若需要用户维护自己的口令，要在初始时提供给他们一个安全的临时口令(见 5.7.3.1)，并强制其立即改变；
c) 在提供一个新的、代替的或临时的口令之前，要建立验证用户身份的规程；
d) 要以安全的方式将临时口令给予用户；要避免使用第三方或未保护的(明文)电子邮件消息；
e) 临时口令要对个人而言是唯一的、不可猜测的；
f) 用户要确认收到口令；
g) 口令不要以未保护的形式存储在计算机系统内；
h) 要在系统或软件安装后改变提供商的默认口令。

口令是按照用户授权赋予对信息系统或服务的访问权之前，验证用户身份的一种常用手段。用户标识和鉴别的其他技术，诸如生物特征识别(例如指纹验证)、签名验证和硬件标记的使用(例如智能卡)，这些技术均可用，如果合适，要加以考虑。

5.7.2.4 用户访问权的复查

控制措施：

管理者应定期使用正式过程对用户的访问权进行复查。

评估指南：

访问权的复查要考虑下列指南：

a) 要定期(例如，周期为 6 个月)和在任何变更之后[例如提升、降级或雇用终止(见 5.7.2.1)]，对用户的访问权进行复查；
b) 当在同一个组织机构中从一个岗位换到另一个岗位时，要复查和重新分配用户的访问权；
c) 对于特定的特殊权限的访问权的授权(见 5.7.2.2)要在更频繁的时间间隔内进行复查，例如周期为 3 个月；
d) 要定期核查特殊权限的分配，以确保不能获得未授权的特殊权限；
e) 具有特殊权限的账户的变更要在周期性复查时记入日志。

定期复查用户的访问权对于保持对数据和信息服务的有效控制来说，是必要的。

5.7.3 用户职责

目标：防止未授权用户对信息和信息处理设施的访问、损害或窃取。

已授权用户的合作对实现有效的安全十分重要。

应使用户知悉其维护有效的访问控制的职责，特别是关于口令使用和用户设备的安全的职责。

应实施桌面清空策略以降低未授权访问或破坏纸、介质和信息处理设施的风险。

5.7.3.1 口令使用

控制措施：

应要求用户在选择及使用口令时，遵循良好的安全习惯。

评估指南：

建议所有用户要求：

a) 保密口令。
b) 避免保留口令的记录(例如在纸上、软件文件中或手持设备中)，除非可以对其进行安全地存储及存储方法得到批准。
c) 每当有任何迹象表明系统或口令受到损害时就变更口令。

d) 选择具有最小长度的优质口令，这些口令：

1) 要易于记忆；

2) 不能基于别人容易猜测或获得的与使用人相关的信息，例如，名字、电话号码和生日等等；

3) 不容易遭受字典攻击(即不是由字典中的词所组成的)；

4) 避免连续相同的、全数字的或全字母的字符。

e) 定期或以访问次数为基础变更口令(有特殊权限的账户的口令宜比常规口令更频繁地予以变更)，并且避免重新使用旧的口令或周期性使用旧的口令。

f) 在初次登录时更换临时口令。

g) 在任何自动登录过程(例如，以宏或功能键存储)中，不要包含口令。

h) 个人的用户口令不要共享。

i) 不在业务目的和非业务目的中使用相同的口令。

如果用户需要访问多个服务、系统或平台，并且需要维护多个单独的口令，则建议他们可以使用同一个优质的口令[见本条 d)]用于所有服务，但用户要确信在每一个服务、系统或平台内对口令的存储建立了合理级别的保护。

要特别小心管理处理口令丢失或忘记的帮助台系统，因为这也可能是对口令系统的一种攻击手段。

5.7.3.2 无人值守的用户设备

控制措施：

用户应确保无人值守的用户设备有适当的保护。

评估指南：

所有用户要了解保护无人值守的设备的安全要求和规程，以及他们对实现这种保护所负有的职责。

建议用户：

a) 结束时终止活动的会话，除非采用一种合适的锁定机制保证其安全，例如，有口令保护的屏幕保护程序；

b) 当会话结束时退出主计算机、服务器和办公 PC(即不仅仅关掉 PC 屏幕或终端)；

c) 当不使用设备时(见 5.7.3.3)，用带钥匙的锁或与之效果等同的控制措施来保护 PC 或终端免遭未授权使用，例如，口令访问。

在用户范围内安装的设备(例如工作站或文件服务器)在长期无人值守时可能需要专门的保护，以防未授权访问。

5.7.3.3 清空桌面和屏幕策略

控制措施：

应采取清空桌面上文件、可移动存储介质的策略和清空信息处理设施屏幕的策略。

评估指南：

清空桌面和清空屏幕策略应考虑信息分类(见 5.3.2)、法律和合同要求(见 5.11.1)、相应的风险和组织机构的文化方面。建议考虑下列指南：

a) 当不用时，特别是当离开办公室时，要将敏感或关键业务信息，例如在纸质或电子存储介质中的，锁起来(理想情况下，在保险柜或保险箱或者其他形式的安全设备中)；

b) 当无人值守时，计算机和终端要注销，或使用由口令、令牌或类似的用户鉴别机制控制的屏幕和键盘锁定机制进行保护；当不使用时，要使用带钥匙的锁、口令或其他控制措施进行保护；

c) 邮件进出点和无人值守的传真机要受到保护；

d) 要防止复印机或其他复制技术(例如扫描仪、数字照相机)的未授权使用；

e) 包含敏感或涉密信息的文件要立即从打印机中清除。

清空桌面/清空屏幕策略降低了正常工作时间之中和之外对信息的未授权访问、丢失、破坏的风险。保险箱或其他形式的安全存储设施也可保护存储于其中的信息免受灾难(例如火灾、地震、洪水或爆炸)的影响。

要考虑使用带有个人识别码功能的打印机,使得原始操作人员是能获得打印输出的唯一人员和站在打印机边的唯一人员。

5.7.4 网络访问控制

目标:防止对网络服务的未授权访问。

对内部和外部网络网络服务的用户均应加以控制。

访问网络和网络服务的用户不应损害网络服务的安全,要确保:

a) 在本组织机构的网络和其他组织机构拥有的网络,以及公共网络之间有合适的接口;

b) 对用户和设备应用合适的鉴别机制;

c) 对用户访问信息服务的强制控制。

5.7.4.1 网络服务的策略

控制措施:

用户应仅能访问已获专门授权使用的服务。

评估指南:

应制定关于使用网络和网络服务的策略。这一策略建议要包括:

a) 允许被访问的网络和网络服务;

b) 确定允许哪个人访问哪些网络和网络服务的授权规程;

c) 保护访问网络连接和网络服务的管理控制措施和规程;

d) 访问网络和网络服务使用的手段(例如,拨号访问互联网服务提供商或远程系统的条件)。

网络服务使用策略要与业务访问控制策略相一致。

与网络服务的未授权和不安全连接可以影响整个组织机构。对于到敏感或关键业务应用的网络连接或与高风险位置(例如,超出组织机构安全管理和控制的公共区域或外部区域)的用户的网络连接而言,这一控制措施特别重要。

5.7.4.2 外部连接的用户鉴别

控制措施:

应使用适当的鉴别方法以控制远程用户的访问。

评估指南:

远程用户的鉴别可以使用例如密码技术、硬件令牌或询问/响应协议等来实现。在各种各样的虚拟专用网络(VPN)解决方案中可以发现这种技术可能的实施。专线也可用来提供连接来源的保证。

回拨规程和控制措施,例如使用回拨调制解调器,可以提供防范到组织机构信息处理设施的未授权和不希望的连接。这种类型的控制措施可鉴别从远程地点试图与组织机构网络建立连接的用户。当使用这种控制措施时,组织机构不宜使用包括呼叫转发的网络服务。或者,如果使用了这种呼叫转发的网络服务,则宜禁用这种特性,以避免与之相关的弱点。回叫过程确保组织机构发生了实际的连接断开。否则,远程用户可能保持线路开路,假装进行了回叫验证。对于这种可能性,要充分地测试回叫规程和控制措施。

若远程用户组被连接到一个安全的、共享的计算机设施,那么,结点鉴别可作为一种进行鉴别的替代手段。密码技术,例如,建立在机器证书基础上,可用于结点鉴别。这是一些 VPN 解决方案中的一部分。

要实施另外的鉴别控制措施以控制对无线网络的访问。尤其是，由于不可检测的截取和插入网络流的机会较大，在为无线网络选择控制措施时需要特别小心。

外部连接为未授权访问业务信息提供了可能，例如，通过拨号方法的访问。有不同类型的鉴别方法，其中某些方法提供比其他方法更高级别的保护，例如，基于使用密码技术的方法可以提供强鉴别。重要的是根据风险评估确定需要的保护级别。这对于选择一种合适的鉴别方法是必需的。

与远程计算机自动连接的设施可能提供获得对业务应用的未授权访问的一种方式。如果该连接使用了组织机构安全管理控制之外的网络，这一点尤其重要。

5.7.4.3 网络上的设备标识

控制措施：

应考虑自动设备标识，将其作为鉴别特定位置和设备连接的方法。

评估指南：

如果通信只能从某特定位置或设备处开始，则可使用设备标识。设备内的或贴在设备上的标识符可用于表示此设备是否允许连接网络。如果存在多个网络，尤其是如果这些网络有不同的敏感度，这些标识符建议清晰地指明设备允许连接到哪个网络。考虑设备的物理保护以维护设备标识符的安全可能是必要的。

这一控制措施可补充其他技术以鉴别设备的用户(见 5.7.4.2)。设备标识可用于用户鉴别。

5.7.4.4 远程诊断和配置端口的保护

控制措施：

对于诊断和配置端口的物理和逻辑访问应加以控制。

评估指南：

对于诊断和配置端口的访问可能采取的控制措施包括使用带钥匙的锁和支持规程，以控制对端口的物理访问。例如，这种支持规程的实例之一是确保只有按照计算机服务管理人员和需要访问的硬件/软件支持人员之间的安排，才可访问诊断和配置端口。

如果没有特别的业务需要，那么安装在计算机或网络设施中的端口、服务和类似的设施，要禁用或取消。

许多计算机系统、网络系统和通信系统安装了远程诊断或配置工具，以便维护工程师使用。如果未加保护，则这些诊断端口提供了一种未授权访问的手段。

5.7.4.5 网络隔离

控制措施：

应在网络中隔离信息服务、用户及信息系统。

评估指南：

控制大型网络安全的一种方法是将该网络分成独立的逻辑网络域，例如，组织机构的内部网络域和外部网络域，每个域受到已定义的安全周边的保护。不同等级的控制措施集可应用于不同的逻辑网络域，以进一步隔离网络安全环境，例如公共可访问系统、内部网络和关键资产。域的定义要基于风险评估和每个域内的不同安全要求。

这样的网络周边可以通过在互连的两个网络之间安装一个安全网关来实现，以控制这两个域之间的访问和信息流。这一网关要配置成能过滤这些域之间的通信流(见 5.7.4.6 和 5.7.4.7)，并且能按照组织机构的访问控制策略阻挡未授权访问(见 5.7.1)。这种类型网关的实例之一就是通常被称作的防火墙。另外一种隔离独立的逻辑域的方法是通过为组织机构内的用户组使用虚拟专用网来限制网络访问。

还可以使用网络设备的功能来隔离网络，例如 IP 转换。这样，独立域可以通过使用路由/交换性能，例如访问控制列表，控制网络数据流而实现。

将网络隔离成若干域的准则宜基于访问控制策略和访问要求(见 5.6.1)，还宜考虑到相关成本和加入适合的网络路由或网关技术的性能影响(见 5.7.4.6 和 5.7.4.7)。

根据工业现场通信的需求，可以选择基于安全通道的隔离技术、通过专用通信硬件和专有安全协议等安全机制，来实现内外部网络的隔离和数据交换，有效地把内外部网络隔离开来，例如可采用安全隔离网关、工业协议防火墙、工业网闸等。

另外，为减少服务中断的影响，网络的隔离宜基于网络中存储或处理信息的价值和分类、信任级别或业务线。

要考虑无线网络与内部和专用网络的隔离。因为无线网络的周边不好定义，在这种情况下，执行风险评估以识别控制措施(例如，强鉴别、密码手段和频率选择)，以维持网络隔离。

正在日益扩展的网络超出了传统的组织机构边界，因为形成的业务伙伴可能需要信息处理和网络设施的互连或共享。这样的扩展可能增加对使用此网络的现有的信息系统进行未授权访问的风险，其中的某些系统由于其敏感性或关键性可能需要防范其他的网络用户。

5.7.4.6 网络连接控制

控制措施：

对于共享的网络，特别是越过组织机构边界的网络，用户的联网能力应按照访问控制策略和业务应用要求加以限制(见 5.7.1)。

评估指南：

应按照访问控制策略(见 5.7.1.1)的要求，维护和更新用户的网络访问权。

用户的连接能力可通过网关来限制，该网关按照预先定义的表或规则过滤通信流。要运用限制的应用示例为：

a) 消息传递，例如电子邮件；

b) 文件传送；

c) 交互式访问；

d) 应用访问。

要考虑将网络访问权与某天的特定时间或日期连接起来。

共享网络，特别是扩展到跨越组织机构边界的那些共享网络的访问控制策略可能需要引入限制用户连接能力的控制措施。

5.7.4.7 网络路由控制

控制措施：

应在网络中实施路由控制，以确保计算机连接和信息流不违反业务应用的访问控制策略。

评估指南：

路由控制措施应基于确定的源地址和目的地址校验机制。

如果使用了代理和/或网络地址转换技术，则可使用安全网关在内部和外部网络控制点验证源地址和目的地址。实施者应了解所采用机制的强度和缺点。网络路由控制的要求应基于访问控制策略(见 5.7.1)。

共享网络，特别是扩展到跨越组织机构边界的那些共享网络，可能需要另外的路由控制措施。在与第三方(非组织机构)用户共享的网络中，这一控制措施特别适用。

5.7.5 操作系统访问控制

目标：防止对操作系统的未授权访问。

使用安全设施以限制授权用户访问操作系统。这些设施具备下列能力：

a) 按照已定义的访问控制策略鉴别授权用户；

b) 记录成功和失败的系统鉴别企图；

c) 记录专用系统特殊权限的使用；

d) 当违背系统安全策略时发布警报；

e) 提供合适的鉴别手段；

f) 恰当时，限制用户的连接时间。

5.7.5.1 安全登录规程

控制措施：

访问操作系统应通过安全登录规程加以控制。

评估指南：

登录到操作系统的规程要设计成使未授权访问的机会减到最小。因此，登录规程要公开最少有关系统的信息，以避免给未授权用户提供任何不必要的帮助。良好的登录规程建议要：

a) 不显示系统或应用标识符，直到登录过程已成功完成为止；

b) 显示只有已授权的用户才能访问计算机的一般性的告警通知；

c) 在登录规程中，不提供对未授权用户有帮助作用的帮助消息；

d) 仅在所有输入数据完成时才验证登录信息。如果出现差错情况，系统不指出数据的哪一部分是正确的或不正确的；

e) 限制所允许的不成功登录尝试的次数(例如 3 次)并考虑：

   1) 记录不成功的尝试和成功的尝试；

   2) 在允许进一步登录尝试之前，强加一次延迟，或在没有特定授权情况下拒绝任何进一步的尝试；

   3) 断开数据链路连接；

   4) 如果达到登录的最大尝试次数，向系统控制台发送警报消息；

   5) 结合口令的最小长度和被保护系统的价值，设置口令重试的次数。

f) 限制登录规程所允许的最长和最短时间。如果超时，则系统宜终止登录；

g) 在成功登录完成时，显示下列信息：

   1) 前一次成功登录的日期和时间；

   2) 上次成功登录之后的任何不成功登录尝试的细节；

   3) 不显示输入的口令或考虑通过符号隐藏口令字符；

   4) 不在网络上以明文传输口令。

h) 在网络上登录会话期间，如果口令以明文传输，他们可能会被网络上的网络“嗅探器”程序捕获。

5.7.5.2 用户标识和鉴别

控制措施：

所有用户应有唯一的，专供其个人使用的标识符(用户 ID)，选择一种适当的鉴别技术证实用户所宣称的身份。

评估指南：

应将这一控制措施应用于所有类型的用户(包括技术支持人员、操作员、网络管理员、系统程序员和数据库管理员)。

使用用户 ID 来将各个活动追踪到各个责任人。常规的用户活动不使用有特殊权限的账户执行。

在例外情况下，如存在明显的业务利益，可以采用一组用户或一项特定作业使用一个共享的用户ID的做法。对于这样的情况，将管理者的批准形成文件。为保持可核查性，可以要求另外的控制措施。

仅在下列情况下允许个人使用的普通ID，即该ID执行的可访问功能或行为不需要追踪（例如只读访问），或者具有其他控制措施（例如，普通ID的口令一次仅发给一个员工，并记录这种情况）。

需要强鉴别和身份验证时，使用鉴别方法代替口令，例如密码手段、智能卡、令牌或生物特征识别手段。

口令是一种非常通用的提供标识和鉴别的方法，这种标识和鉴别是建立在只有用户知悉的秘密的基础上的。使用密码手段和鉴别协议也可以获得同样的效果。用户标识和鉴别的强度宜和所访问信息的敏感程度相适应。

用户拥有的客体（例如记忆令牌或智能卡）也可以用于标识和鉴别。利用个人的唯一特征或属性的生物特征鉴别技术也可用来鉴别个人的身份。技术和机制的安全组合将产生更强的鉴别。

5.7.5.3 口令管理系统

控制措施：

口令管理系统宜是交互式的，并应确保优质的口令。

评估指南：

一个口令管理系统建议要能够：

a) 强制使用个人用户ID和口令，以保持可核查性；

b) 允许用户选择和变更他们自己的口令，并且包括一个确认规程，以便考虑到输入出错的情况；

c) 强制选择优质口令（见5.7.3.1）；

d) 强制口令变更（见5.7.3.1）；

e) 在第一次登录时强制用户变更临时口令（见5.7.2.3）；

f) 维护用户以前使用的口令的记录，并防止重复使用；

g) 在输入口令时，不在屏幕上显示；

h) 分开存储口令文件和应用系统数据；

i) 以保护的形式（例如加密或哈希运算）存储和传输口令。

口令是确认用户具有访问计算机服务的授权的主要手段之一。

某些应用要求由某个独立授权机构来分配用户口令；在这种情况下，本条评估指南b)、d)和e)不适用。

在大多数情况下，口令由用户选择和维护。使用口令的指南参见5.7.3.1。

5.7.5.4 系统实用工具的使用

控制措施：

对于可能超越系统和应用程序控制措施的实用工具的使用应加以限制并严格控制。

评估指南：

对于系统实用工具的使用，建议考虑下列指南：

a) 对系统实用工具使用标识、鉴别和授权规程；

b) 将系统实用工具和应用软件分开；

c) 将使用系统实用工具的用户限制到可信的、已授权的最小实际用户数（也见5.7.2.2）；

d) 对系统实用工具的特别使用的授权；

e) 限制系统实用工具的可用性，例如，在授权变更的期间内；

f) 记录系统实用工具的所有使用；

g) 对系统实用工具的授权级别进行定义并形成文件；

h) 移去或禁用所有不必要的基于软件的实用工具和系统软件；

i) 当要求责任分割时，禁止访问系统中应用程序的用户使用系统实用工具。

大多数计算机安装有一个或多个可能超越系统和应用控制措施的系统实用工具。

5.7.5.5 会话超时

控制措施：

不活动会话应在一个设定的休止期后关闭。

评估指南：

在一个设定的休止期后，超时设施要清空会话屏幕，并且也可能在超时更长时，关闭应用和网络会话。超时延迟要反映该范围的安全风险、被处理的信息和被使用的应用程序的类别，以及与设备的用户相关的风险。

对某些系统可以提供一种受限制的超时设施形式，即清空屏幕并防止未授权访问，但不关闭应用或网络会话。

这一控制措施在高风险位置特别重要，包括那些在组织机构安全管理之外的公共或外部区域。会话要关闭以防止未授权人员访问和拒绝服务攻击。

5.7.5.6 联机时间的限定

控制措施：

应使用联机时间的限制，为高风险应用程序提供额外的安全。

评估指南：

要考虑对敏感的计算机应用程序，特别是安装在高风险位置(例如，超出组织机构安全管理的公共或外部区域)的应用程序，使用连机时间的控制措施。

这种限制的示例包括：

a) 使用预先定义的时隙，例如对批文件传输，或定期的短期交互会话；

b) 如果没有超时或延时操作的要求，则将连机时间限于正常办公时间；

c) 考虑定时进行重新鉴别。

限制与计算机服务连接的允许时间减少了未授权访问机会。限制活动会话的持续时间可防范用户保持会话打开而阻碍重新鉴别。

5.7.6 应用和信息访问控制

目标：防止对应用系统中信息的未授权访问。

应使用安全设施来限制对应用系统的访问和应用系统内的访问。

对应用软件和信息的逻辑访问宜只限于授权的用户。建议应用系统要：

a) 按照已确定的访问控制策略，控制用户访问信息和应用系统功能；

b) 提供防范能够超越或绕过系统和应用控制措施的任何实用工具、操作系统软件和恶意软件的未授权访问；

c) 不损害与之共享信息资源的其他系统的安全。

5.7.6.1 信息访问限制

控制措施：

用户和支持人员对信息和应用系统功能的访问应依照已确定的访问控制策略加以限制。

评估指南：

对访问的限制基于各个业务应用要求。访问控制策略还宜与组织机构的访问策略(见 5.7.1)一致。

为支持访问限制要求，建议考虑应用以下指南：

a) 提供控制访问应用系统功能的选择单；

b) 控制用户的访问权，例如，读、写、删除和执行；

c) 控制其他应用的访问权；

d) 确保处理敏感信息的应用系统的输出仅包含与使用输出相关的信息，并且仅发送给已授权的终端和地点，包括周期性评审这种输出，以确保去掉多余信息。

5.7.6.2 敏感系统隔离

控制措施：

敏感系统应有专用的(隔离的)运算环境。

评估指南：

对于敏感系统隔离，建议考虑以下内容：

a) 应用程序的责任人要明确识别应用系统的敏感程度，并将其形成文件(见 5.3.1.2)。

b) 当敏感应用程序在共享的环境中运行时，该敏感应用程序的责任人要识别并接受与其共享资源的应用系统及相关风险。

某些应用系统对潜在的损失十分敏感，因此要求特别处理。敏感性可能表示该应用系统：

c) 要运行在专用的计算机上；

d) 要仅与可信的应用系统共享资源。

隔离可通过使用物理或逻辑手段实现(见 5.7.4.5)。

5.7.7 移动计算和远程工作

目标：确保使用移动计算和远程工作设施时的信息安全。

需要的保护措施应与这些特定工作方式引起的风险相称。

当使用移动计算时，要考虑在不受保护的环境中的工作风险，并应用合适的保护措施。在远程工作的情况下，组织机构要在远程工作地点应用保护措施，并确保对这种工作方式有合适的安排。

5.7.7.1 移动计算和通信

控制措施：

应有正式策略并且采用适当的安全措施，以防范使用移动计算和通信设施时所造成的风险。

评估指南：

当使用移动计算和通信设施，如笔记本、掌上电脑、便携式电脑、智能卡和移动电话时，要特别小心确保业务信息不被损害。移动计算策略要考虑到在不受保护的环境下使用移动计算设备工作的风险。

移动计算策略包括对物理保护、访问控制、密码技术、备份和病毒防护的要求。这一策略也要包括关于移动设施与网络连接的规则和建议，以及关于在公共场合使用这些设施的指南。

当在组织机构建筑物之外的公共场所、会议室和其他不受保护的区域使用移动计算设施时，要加以小心。为避免未授权访问或泄露这些设施所存储和处理的信息，要有到位的保护措施，例如，使用密码技术。

在公共场合使用移动计算设施的用户，要小心谨慎以避免未授权人员窥视的风险。防范恶意软件的规程要到位并且保持最新(见 5.6.4)。

要定期对关键业务信息进行备份。要有可用的设备使信息得到快速、简便的备份。对这些备份要采取足够的防范措施，如防范信息被偷窃或丢失。

对与网络连接的移动设施的使用要提供合适的保护。只有在成功标识和鉴别之后，且具有合适的访问控制机制的情况下，才可利用移动计算设施通过公共网络远程访问业务信息(见 5.7.4)。

还要对移动计算设施进行物理保护，以防被偷窃，例如，特别是遗留在汽车和其他形式的运输工具上、旅馆房间、会议中心和会议室。要为移动计算设施的被窃或丢失等情况建立一个符合法律、保险和组织机构的其他安全要求的特定规程。携带重要、敏感和/或关键业务信息的设备不要无人值守，若有可能，要以物理的方式锁起来，或使用专用锁来保护设备(见 5.5.2.5)。

对于使用移动计算设施的人员应安排培训，以提高他们对这种工作方式导致的附加风险的意识，并且应实施控制措施。

移动网络无线连接类似于其他类型的网络连接，但在确定控制措施时，要考虑两者的重要区别。典型的区别有：

a) 一些无线安全协议是不成熟的，并有已知的弱点；
b) 在移动计算机上存储的信息可能不能备份，因为受限的网络带宽和/或因为移动设备在规定的备份时间不能进行连接。

5.7.7.2 远程工作

控制措施：

应为远程工作活动开发和实施策略、操作计划和规程。

评估指南：

组织机构应仅在有合适的安全部署和控制措施到位，且这些符合组织机构的安全方针的情况下，才授权远程工作活动。

要有对远程工作场地的合适保护措施，以防范设备和信息被窃、信息的未授权泄露、对组织机构内部系统的未授权远程访问或设施滥用等。远程工作活动宜由管理者授权和控制，且确保对这种工作方式有合适安排。

建议考虑下列内容：

a) 远程工作场地的现有物理安全，要考虑到建筑物和本地环境的物理安全；
b) 推荐的物理的远程工作环境；
c) 通信安全要求，要考虑远程访问组织机构内部系统的需要、被访问的并在通信链路上传递的信息的敏感性以及内部系统的敏感性；
d) 住处的其他人员(例如，家人和朋友)未授权访问信息或资源的威胁；
e) 家庭网络的使用和无线网络服务配置的要求或限制；
f) 针对私有设备开发的预防知识产权争论的策略和规程；
g) 法律禁止的对私有设备的访问(核查机器安全或在调查期间)；
h) 使组织机构对雇员、承包方人员或第三方人员等私人拥有的工作站上的客户端软件负有责任的软件许可协议；
i) 防病毒保护和防火墙要求。

建议考虑的指南和安排包括：

a) 当不允许使用不在组织机构控制下的私有设备时，对远程工作活动提供合适的设备和存储设施；
b) 确定允许的工作、工作小时数、可以保持的信息分类和授权远程工作者访问的内部系统和服务；
c) 提供适合的通信设备，包括使远程访问安全的方法；
d) 物理安全；
e) 有关家人和来宾访问设备和信息的规则和指南；
f) 硬件和软件支持和维护的规定；
g) 保险的规定；

h) 用于备份和业务连续性的规程；

i) 审核和安全监视；

j) 当远程工作活动终止时，撤销授权和访问权，并返回设备。

远程工作是利用通信技术来使得人员可以在其组织机构之外的固定地点进行远程工作的。

5.8 信息系统获取、开发和维护

5.8.1 信息系统的安全要求

目标：确保安全是信息系统的一个有机组成部分。

信息系统包括操作系统，基础设施、业务应用、非定制产品、服务和用户开发的应用。支持业务过程的信息系统的设计和实施对安全来说可能是关键的。在信息系统开发和/或实施之前，应识别并商定安全要求。

要在项目需求阶段识别所有安全要求，并证明这次安全要求的合理性，对这些安全要求加以商定，并且将这些安全要求形成文件作为信息系统整体业务情况的一部分。

5.8.1.1 安全要求分析和说明

控制措施：

在新的信息系统或增强已有信息系统的业务要求陈述中，应规定对安全控制措施的要求。

评估指南：

控制措施要求的说明应考虑在信息系统中包含的自动控制措施，以及支持人工控制措施的需要。

当评价业务应用(开发或购买)的软件包时，进行类似的考虑。

安全要求和控制措施要反映出所涉及的信息资产的业务价值(见 5.3.2)和可能由于安全故障或安全措施不足引起的潜在的业务损害。

信息安全的系统要求与实施安全的过程要在信息系统项目的早期阶段被集成。在设计阶段引入控制措施要比在实现期间或实现后引入控制措施的实施和维护的费用低得多。

如果购买产品，则遵循一个正式的测试和获取过程。与供货商签订的合同要给出已确定的安全要求。如果推荐的产品的安全功能不能满足安全要求，那么在购买产品之前要重新考虑引入的风险和相关控制措施。如果产品提供的附加功能引起了安全风险，那么要禁用该功能，或者要评审所推荐的控制结构，以判定是否可以利用该增强功能。

5.8.2 应用中的正确处理

目标：防止应用系统中的信息的差错、遗失、未授权的修改或误用。

应用系统(包括用户开发的应用系统)内应设计合适的控制措施以确保正确处理。这些控制措施要包括对输入数据、内部处理和输出数据的确认。

对于处理敏感的、有价值的或关键的信息的系统或对这些信息有影响的系统，可以要求另外的控制措施。这样的控制措施要在安全要求和风险评估的基础上加以确定。

5.8.2.1 输入数据确认

控制措施：

应对输入应用系统的数据加以确认，以确保数据是正确且恰当的。

评估指南：

将校验应用于业务交易、常备数据(例如，姓名和地址、信贷限值、顾客引用号码)和参数表(例如，销售价、货币兑换率、税率)的输入。建议考虑下列指南：

a) 双输入或其他输入校验，例如边界校验或者限制特定输入数据范围的域，以检测下列差错：
   1) 范围之外的值；
   2) 数据字段中的无效字符；
   3) 丢失或不完整的数据；
   4) 超过数据的上下容量限制；
   5) 未授权的或矛盾的控制数据。
b) 定期评审关键字段或数据文件的内容，以证实其有效性和完整性。
c) 检查硬拷贝输入文件是否有任何未授权的变更(输入文件的所有变更均予以授权)。
d) 响应确认了的差错的规程。
e) 测试输入数据合理性的规程。
f) 定义在数据输入过程中所涉及的全部人员的职责。
g) 创建在数据输入过程中所涉及的活动的日志(见 5.6.9.1)。

适用时，可以考虑对输入数据进行自动试验和确认，以减少出错的风险和预防包括缓冲区溢出和代码注入等常见的攻击。

5.8.2.2 内部处理的控制

控制措施：

确认核查应整合到应用中，以检验由于处理的差错或故意的行为造成的信息的任何讹误。

评估指南：

应用系统的设计与实施应确保导致完整性损坏的处理故障的风险减至最小。要考虑的特定范围建议包括：

a) 使用添加、修改和删除功能，以实现数据变更；
b) 防止程序以错误次序运行或在前面处理出现故障后运行的规程(见 5.6.1.1)；
c) 使用适当的规程恢复故障，以确保数据的正确处理；
d) 防范利用缓冲区超出/溢出进行的攻击。

准备适当的核查列表，将核查活动文件化，并保持核查结果的安全。可被整合的核查例子如下：

e) 会话或批控制措施，以便在交易更新之后调节数据文件平衡。
f) 平衡控制措施，对照先前的封闭平衡来核查开放平衡，即：
   1) 运行到运行的控制措施；
   2) 文件更新总数；
   3) 程序到程序的控制措施。
g) 确认系统生成的输入数据(见 5.8.2.1)。
h) 核查在中央计算机和远程计算机之间所下载或上载的数据或软件的完整性、真实性或者其他任何安全特性。
i) 记录和文件的数位总和。
j) 核查以确保应用程序在正确时刻运行。
k) 核查以确保程序以正确的次序运行并且在发生故障时终止，以及在问题解决之前停止进一步的处理。
l) 创建处理中所涉及的活动的日志(见 5.6.9.1)。

正确输入的数据可能被硬件错误、处理出错或故意的行为所破坏。所需的确认核查取决于应用系统的性质和毁坏数据对业务的影响。

5.8.2.3 消息完整性

控制措施：

应用中的确保真实性和保护消息完整性的要求应得到识别，适当的控制措施也应得到识别并实施。

评估指南：

应进行安全风险的评估以判定是否需要消息完整性，并确定最合适的实施方法。

密码技术(见 5.8.3)可被用作一种合适的实现消息鉴别的手段。

5.8.2.4 输出数据确认

控制措施：

从应用系统输出的数据应加以确认，以确保对所存储信息的处理是正确的且适于环境的。

评估指南：

输出确认可以包括：

a) 合理性核查，以测试输出数据是否合理；

b) 调节控制计数，以确保处理所有数据；

c) 为读者或后续的处理系统提供足够的信息，以确定信息的准确性、完备性、精确性和分类；

d) 响应输出确认测试的规程；

e) 定义在数据输出过程中所涉及的全部人员的职责；

f) 创建在数据输出确认过程中活动的日志。

一般来说，系统和应用是在假设已经进行了适当的确认、验证和测试的条件下构建的，其输出总是正确的。然而，这种假设并不总是有效，即已经过测试的系统仍可能在某些环境下产生不正确的输出。

5.8.3 密码控制

目标：通过密码方法保护信息的保密性、真实性或完整性。

应制定使用密码控制的策略。应有密钥管理以支持使用密码技术。

5.8.3.1 使用密码控制的策略

控制措施：

应开发和实施使用密码控制措施来保护信息的策略。

评估指南：

制定密码策略时，建议考虑下列内容：

a) 组织机构间使用密码控制的管理方法，包括保护业务信息的一般原则(见 5.1.1)。

b) 基于风险评估，确定需要的保护级别，并考虑需要的加密算法的类型、强度和质量。

c) 使用加密保护通过可移动或可拆卸的介质、设备或者通信线路传输的敏感信息。

d) 密钥管理方法，包括应对密钥保护的方法，以及在密钥丢失、损害或毁坏后加密信息的恢复方法。

e) 角色和职责，例如，谁负责：

   1) 策略的实施；

   2) 密钥管理，包括密钥生成(见 5.8.3.2)。

f) 为在整个组织机构内有效实施而采用的标准(哪种解决方案用于哪些业务过程)。

g) 使用加密后的信息对依赖于内容检查的控制措施(例如，病毒检测)的影响。

当实施组织机构的密码策略时，要考虑我国应用密码技术的规定和限制，以及加密信息跨越国界时的问题(见 5.11.1.6)。

可以使用密码控制措施实现不同的安全目标，例如：

a) 保密性：使用信息加密以保护存储或传输中的敏感或关键信息；

b) 完整性/真实性：使用数字签名或消息鉴别码以保护存储和传输中的敏感或关键信息的真实

性和完整性；

c) 抗抵赖性：使用密码技术以获得一个事态或行为发生或未发生的证据。

有关一个密码解决方案是否合适的决策，要被看作更广的风险评估和选择控制措施过程的一部分。

评估可以用来判定一个密码控制措施是否合适，要运用什么类型的控制措施以及应用于什么目的和业务过程。

使用密码控制措施的策略对于使利益最大化，使利用密码技术的风险最小化，以及避免不合适或不正确的使用而言，十分必要。在使用数字签名时，宜考虑任何相关的法律，特别是规定什么条件下数字签名被合法绑定的法律(见 5.11.1.1)。

征求专家建议以识别适当的保护级别，确定用以提供所需的保护及支持安全密钥管理系统实施的合适的规范(见 5.8.3.2)。

5.8.3.2 密钥管理

控制措施：

应有密钥管理以支持组织机构使用密码技术。

评估指南：

应保护所有的密钥免遭修改、丢失和毁坏。另外，秘密和私有密钥需要防范非授权的泄露。用来生成、存储和归档密钥的设备宜进行物理保护。

密钥管理系统建议基于已商定的标准、规程和安全方法，以便：

a) 生成用于不同密码系统和不同应用的密钥；

b) 生成和获得公开密钥证书；

c) 分发密钥给预期用户，包括在收到密钥时要如何激活；

d) 存储密钥，包括已授权用户如何访问密钥；

e) 变更或更新密钥。包括要何时变更密钥和如何变更密钥的规则；

f) 处理已损害的密钥；

g) 撤销密钥，包括要如何撤消或解除激活的密钥，例如，当密钥已损害时或当用户离开组织机构时(在这种情况下，密钥也要归档)；

h) 恢复已丢失或损坏的密钥，作为业务连续性管理的一部分，例如，用于加密信息的恢复的密钥；

i) 归档密钥，例如，用于已归档或备份信息的密钥；

j) 销毁密钥；

k) 记录和审核与密钥管理相关的活动。

为了减少密钥损害的可能性，规定密钥的激活日期和解除激活日期，以使他们只能用于有限的时间段。该时间段根据所使用的密码控制的情况和察觉的风险而定。

除了安全地管理秘密和私有密钥外，还考虑公开密钥的真实性。这一鉴别过程可以由证书认证机构正式颁发的公钥证书来完成，该认证机构宜是一个具有合适的控制措施和规程以提供所需的信任度的公认组织机构。

与外部密码服务提供者(例如与认证机构)签订的服务级别协议或合同的内容，要涵盖服务责任、服务可靠性和提供服务的响应次数等若干问题(见 5.2.2.3)。

密钥的管理对有效使用密码技术来说是必需的。GB/T 17901 提供了更多密钥管理的信息。两种类型的密码技术为：

a) 秘密密钥技术，其中双方或更多方共享同一密钥，并且该密钥既用来加密也用来解密信息；这个密钥必须被秘密地保存，因为访问到他的任何人能解密被该密钥加密的所有信息，或引入使用该密钥的未授权信息；

b) 公开密钥技术，其中每个用户拥有一对密钥，一个公开密钥（他可以被展现给任何人）和一个私有密钥（其必须被秘密地保存）；公开密钥技术可用于加密，并可用来产生数字签名（参见GB/T 15851 和 GB/T 17902）。

存在通过替换某用户的公开密钥来伪造数字签名的威胁。这一问题可以通过使用公开密钥证书来解决。

密码技术还可以用来保护密钥。可能需要考虑处理访问密钥的法律请求的规程，例如，加密的信息可能需要以未加密的形式提供，以作为法庭案例的证据。

5.8.4 系统文件的安全

目标：确保系统文件的安全。

应控制对系统文件和程序源的访问。要以安全的方式管理工业控制系统信息安全项目和支持活动。在测试环境中要小心谨慎以避免泄露敏感数据。

5.8.4.1 运行软件的控制

控制措施：

应有规程来控制在运行系统上安装软件。

评估指南：

为使运行系统被损坏的风险减到最小，建议考虑下列指南以控制变更：

a) 要仅由受过培训的管理员，根据合适的管理授权（见 5.8.4.3），进行运行软件、应用和程序库的更新；

b) 运行系统要仅安装经过批准的可执行代码，不安装开发代码和编译程序；

c) 应用和操作系统软件要在大范围的、成功的测试之后才能实施，这种测试要包括实用性、安全性、对其他系统的影响和用户友好性的测试，且测试要在独立的系统上完成（见 5.6.1.4）。要确保所有对应的程序源库已经更新；

d) 要使用配置控制系统对所有已开发的软件和系统文件进行控制；

e) 在变更实施之前要有还原的策略；

f) 要维护对运行程序库的所有更新的审计日志；

g) 要保留应用软件的先前版本作为应急措施；

h) 软件的旧版本，连同所有需要的信息和参数、规程、配置细节以及支持软件。以及进行与归档数据具有相同保留期的归档。

在运行系统中所使用的由厂商供应的软件要在供应商支持的级别上加以维护。一段时间后，软件供应商停止支持旧版本的软件。组织机构要考虑依赖于这种不再支持的软件的风险。

升级到新版的任何决策要考虑变更的业务要求和新版的安全。即引入的新安全功能或影响该版本安全问题的数量和严重程度。当软件补丁有助于消除或减少安全弱点（见 5.8.6.1）时，要使用软件补丁。

必要时在管理者批准的情况下，仅为了技术支持的目的，才授予供应商物理或逻辑访问权。要监督供应商的活动。

计算机软件可能依赖于外部提供的软件和模块，要对这些产品进行监视和控制，以避免可能引入安全弱点的非授权的变更。

操作系统要仅在需要升级的时候才进行升级，例如，在操作系统的当前版本不再支持业务要求的时候。只有在具有了可用的新版本的操作系统后才能进行升级。

5.8.4.2 系统测试数据的保护

控制措施：

测试数据应认真地加以选择、保护和控制。

评估指南：

要避免使用包含个人信息或其他敏感信息的运行数据库用于测试。如果测试使用了个人或其他敏感信息，那么在使用之前要去除或修改所有的敏感细节和内容。当用于测试时，要使用下列指南保护运行数据：

a) 要用于运行应用系统的访问控制规程，还应用于测试应用系统；

b) 运行信息每次被拷贝到测试应用系统时要有独立的授权；

c) 在测试完成之后，要立即从测试应用系统清除运行信息；

d) 要记录运行信息的拷贝和使用日志以提供审核踪迹。

系统和验收测试常常要求相当多的尽可能接近运行数据的测试数据。

5.8.4.3 对程序源代码的访问控制

控制措施：

应限制访问程序源代码。

评估指南：

对程序源代码和相关事项(例如设计、说明书、验证计划和确认计划)的访问应严格控制，以防引入非授权功能和避免无意识的变更。对于程序源代码的保存，可以通过这种代码的中央存储控制来实现，更好的是放在源程序库中。为了控制对源程序库的访问以减少潜在的计算机程序的破坏，建议考虑下列指南：

a) 若有可能，在运行系统中不要保留源程序库；

b) 程序源代码和源程序库要根据制定的规程进行管理；

c) 要限制支持人员访问源程序库；

d) 更新源程序库和有关事项，向程序员发布程序源代码要在获得适当的授权之后进行；

e) 程序列表要保存在安全的环境中(见 5.6.7.4)；

f) 要维护对源程序库所有访问的审计日志；

g) 维护和拷贝源程序库要受严格变更控制规程的制约(见 5.8.5.1)。

5.8.5 开发和支持过程中的安全

目标：维护应用软件和信息的安全。

应严格控制项目和支持环境。

负责应用系统的管理人员，也应负责项目或环境的安全。他们要确保评审所有推荐的系统变更，以核查这些变更不会损害系统或操作系统的安全。

5.8.5.1 变更控制规程

控制措施：

应使用正式的变更控制规程来控制变更的实施。

评估指南：

应将正式的变更控制规程文件化，并强制实施，以将信息系统的损坏减到最小。引入新系统和对已有系统进行大的变更要按照从文件、规范、测试、质量控制到实施管理这个正式的过程进行。

这个过程要包括风险评估、变更影响分析和所需的安全控制措施规范。这一过程还要确保不损害现有的安全和控制规程，确保支持程序员仅能访问系统中其工作那些必要的部分，确保任何变更要获得正式商定和批准。

只要可行，应用和运行变更控制规程建议集成起来(见 5.6.1.2)。该变更规程建议包括：

a) 维护所商定授权级别的记录；

b) 确保由授权的用户提交变更；

c) 评审控制措施和完整性规程，以确保他们不因变更而损害；

d) 识别需要修正的所有软件、信息、数据库实体和硬件；

e) 在工作开始之前，获得对详细建议的正式批准；

f) 确保已授权的用户在实施之前接受变更；

g) 确保在每个变更完成之后更新系统文件设置，并将旧文件归档或丢弃；

h) 维护所有软件更新的版本控制；

i) 维护所有变更请求的审核踪迹；

j) 当必要时，确保对操作文件(见 5.6.1.1)和用户规程作合适的变更；

k) 确保变更的实施发生在正确的时刻，并且不干扰所涉及的业务过程。

变更软件会影响运行环境。

良好的惯例包括在一个与生产和开发环境隔离(见 5.6.1.4)的环境中测试新软件。这提供对新软件进行控制和允许对被用于测试目的的运行信息给予附加保护的手段。这包括补丁、服务包和其他更新。不应在关键系统中使用自动更新，因为某些更新可能会导致关键应用程序的失败(见 5.8.6)。

5.8.5.2 操作系统变更后应用的技术评审

控制措施：

当操作系统发生变更时，应对业务的关键应用进行评审和测试，以确保对组织机构的运行和安全没有负面影响。

评估指南：

这一过程建议涵盖：

a) 评审应用控制和完整性规程，以确保他们不因操作系统变更而损害；

b) 确保年度支持计划和预算将包括由于操作系统变更而引起的评审和系统测试；

c) 确保及时提供操作系统变更的通知，以便于在实施之前进行合适的测试和评审；

d) 确保对业务连续性计划进行合适的变更(见 5.10)。

指定专门的组织机构或个人负责监视脆弱性和供应商发布的补丁和修正(见 5.8.6)。

5.8.5.3 软件包变更的限制

控制措施：

应对软件包的修改进行劝阻，只限于必要的变更，且对所有的变更加以严格控制。

评估指南：

如果可能且可行，应使用厂商提供的软件包，而无需修改。在需要修改软件包时，要考虑下列要点：

a) 内置控制措施和完整性过程被损害的风险；

b) 是否获得厂商的同意；

c) 当标准程序更新时，从厂商获得所需要变更的可能性；

d) 作为变更的结果，组织机构要负责进一步维护此软件的影响。

如果变更是必要的，则原始软件宜保留，并将变更应用于已明显确定的拷贝。要实施软件更新管理过程，以确保最新批准的补丁和应用更新已经安装在所有的授权软件中(见 5.8.6)。要充分测试所有变更，并将其形成文件，若必要，可以使他们重新应用于进一步的软件升级。如果必要，所有的更新要由独立的评估机构进行测试和确认。

5.8.5.4 信息泄露

控制措施：

应防止信息泄露的可能性。

评估指南：

要考虑下列事项以限制信息泄露的风险，例如通过使用和利用隐蔽通道：

a) 扫描隐藏信息的对外介质和通信；

b) 掩盖和调整系统和通信的行为，以减少第三方从这些行为中推断信息的可能性；

c) 使用被认为具有高完整性的系统和软件，例如使用经过评价的产品(见 GB/T 18336)；

d) 在现有法律或法规允许的情况下，定期监视个人和系统的活动；

e) 监视计算机系统的资源使用。

隐蔽信道不是故意用来引导信息流的通道，但其仍可能存在于系统或网络中。例如，通信协议包中的隐藏比特可能被作为信号隐藏的方法。从本质上说，如果可能的话，防止所有可能的隐蔽通道的存在将是很困难的。然而，特洛伊木马经常利用这种隐蔽通道(见 5.6.4.1)。因此，采取措施防范特洛伊木马能够减少隐蔽通道被利用的风险。

防止非授权的网络访问(见 5.7.4)和阻止人员对信息服务的误用(见 5.11.1.5)的策略和规程，有助于防范隐蔽通道。

5.8.5.5 外包软件开发

控制措施：

组织机构应管理和监视外包软件的开发。

评估指南：

在外包软件开发时，建议考虑下列要点：

a) 许可证安排、代码所有权和知识产权(见 5.11.1.2)；

b) 所完成工作的质量和准确性的认证；

c) 第三方发生故障时的契约安排；

d) 审核所完成的工作质量和准确性的访问权；

e) 代码质量和安全功能的合同要求；

f) 在安装前，检测恶意代码和特洛伊木马。

5.8.6 技术脆弱性管理

目标：降低利用公布的技术脆弱性导致的风险。

技术脆弱性管理应以一种有效的、系统的、可重复的，并可测量以证实其有效性的方式实施。这些考虑事项要包括使用中的操作系统和任何其他的应用程序。

5.8.6.1 技术脆弱性的控制

控制措施：

应及时得到现用信息系统技术脆弱性的信息，评价组织机构对这些脆弱性的暴露程度，并采取适当的措施来处理相关的风险。

评估指南：

当前的、完整的资产清单(见 5.3.1)是进行有效技术脆弱性管理的先决条件。支持技术脆弱性管理所需的特定信息包括软件供应商、版本号、部署的当前状态(例如，在什么系统上安装什么软件)，以及组织机构内负责软件的人员。

采取适当的、及时的措施以响应潜在的技术脆弱性。建立有效的技术脆弱性管理过程遵循下列指南：

a) 组织机构要定义和建立与技术脆弱性管理相关的角色和职责，包括脆弱性监视、脆弱性风险评估、打补丁、资产追踪和任意需要的协调责任。

b) 用于识别相关的技术脆弱性和维护有关这些脆弱性的认识的信息资源，要被识别用于软件和其他技术（基于资产清单，见 5.3.1.1）；这些信息资源要根据清单的变更而更新，或当发现其他新的或有用的资源时，也要更新。

c) 要制定时间表对潜在的相关技术脆弱性的通知做出反映。

d) 一旦潜在的技术脆弱性被确定，组织机构要识别相关的风险并采取措施；这些措施可能包括对脆弱的系统打补丁和/或应用其他控制措施。

e) 按照技术脆弱性需要解决的紧急程度，要根据变更管理相关的控制措施（见 5.8.5.1），或者遵照信息安全事件响应规程（见 5.9.2），采取措施。

f) 如果有可用的补丁，则要评估与安装该补丁相关的风险（脆弱性引起的风险要与安装补丁带来的风险进行比较）。

g) 在安装补丁之前，要进行测试与评价，以确保他们是有效的，且不会导致不能容忍的负面影响；如果没有可用的补丁，要考虑其他控制措施，例如：

   1) 关闭与脆弱性有关的服务和功能；

   2) 调整或增加访问控制措施，例如在网络边界上添加防火墙（见 5.7.4.5）；

   3) 增加监视以检测或预防实际的攻击；

   4) 提高脆弱性意识。

h) 要对所有执行的规程进行审计日志。

i) 要定期对技术脆弱性管理过程进行监视和评价，以确保其有效性和效率。

j) 处于高风险中的系统要首先解决。

一个组织机构的技术脆弱性管理过程的正确实施对许多组织机构来说是非常重要的，因此要定期对其进行监视。一个准确的清单对于确保识别潜在的相关技术脆弱性而言，是必要的。

技术脆弱性管理可被看作是变更管理的一个子功能，因此可以利用变更管理的过程和规程（见 5.6.1.2和 5.8.5.1）。

供应商往往是在很大的压力下发布补丁。因此，补丁可能不足以解决该问题，并且可能存在负作用。而且，在某些情况下，一旦补丁被安装后，很难被卸载。

如果不能对补丁进行充分的测试，如由于成本或资源缺乏，那么可以考虑推迟打补丁，以便基于其他用户报告的经验来评价相关的风险。

5.9 信息安全事件管理

5.9.1 报告信息安全事态和弱点

目标：确保与信息系统有关的信息安全事态和弱点能够以某种方式传达，以便及时采取纠正措施。

应有正式的事态报告和上报规程。所有雇员、承包方人员和第三方人员都要了解这些规程，以便报告可能对组织机构的资产安全造成影响的不同类型的事态和弱点。要求他们尽可能快地将信息安全事态和弱点报告给指定的联系点。

5.9.1.1 报告信息安全事态

控制措施：

信息安全事态应尽可能快地通过适当的管理渠道进行报告。

评估指南：

要建立正式的信息安全事态报告规程和事件响应及上报规程，以在收到信息安全事态报告时着手采取措施。为了报告信息安全事态，要建立联系点。并确保整个组织机构都知道该联系点，该联系点一直保持可用并能提供充分且及时的响应。

所有雇员、承包方人员和第三方人员都应知道他们有责任尽可能快地报告任何信息安全事态。他们还应知道报告信息安全事态的规程和联系点。报告规程建议包括：

a) 适当的反馈过程，以确保在信息安全事态处理完成后，能够将处理结果通知给事态报告人。

b) 信息安全事态报告单，以支持报告行为和帮助报告人员记下信息安全事态中的所有必要的行为。

c) 信息安全事态发生后要采取正确的行为，即：

1) 立即记录下所有重要的细节(如，不符合或违规的类型、出现的故障、屏幕上显示的消息、异常行为)；

2) 不要采取任何个人行动，但要立即向联系点报告。

d) 引用已制定的正式违纪处理过程。来处理有安全违规行为的雇员、承包方人员或第三方人员。

在高风险环境下，可以提供强迫警报，借此被强迫的人员可以指出这种问题。对强迫警报的响应规程应反映该警报所指明的高风险情况。

信息安全事态和事件的示例如下：

a) 服务、设备或设施的丢失；

b) 系统故障或超载；

c) 人为差错；

d) 策略或指南的不符合；

e) 物理安全安排的违规；

f) 未加控制的系统变更；

g) 软件或硬件故障；

h) 非法访问。

在注意保密性各方面的情况下，信息安全事件可以在用户意识培训(见 5.4.2.2)中作为一些例子，这些例子是，可能发生什么事件，如何对该事件进行响应，以及在将来如何避免这些事件。为了正确指出信息安全事态和事件，在其发生后尽可能地收集证据是必要的(见 5.9.2.3)。

故障或其他异常的系统行为可能是安全攻击和实际安全违规的显示，因此要将其当作信息安全事态进行报告。

5.9.1.2 报告安全弱点

控制措施：

应要求信息系统和服务的所有雇员、承包方人员和第三方人员记录并报告他们观察到的或怀疑的任何系统或服务的安全弱点。

评估指南：

为了预防信息安全事件，所有雇员、承包方人员和第三方人员要尽可能快地将这些事情报告给他们的管理者，或者直接报告给服务提供者。报告机制要尽可能容易、可访问和可利用。要告知他们，在任何情况下，他们都不要试图去证明被怀疑的弱点。

要建议雇员、承包方人员和第三方人员不要试图去证明被怀疑的安全弱点。测试弱点可能被看作是潜在的系统误用，还可能导致信息系统或服务的损害，并引起测试人员的法律责任。

5.9.2 信息安全事件和改进的管理

目标：确保采用一致和有效的方法对信息安全事件进行管理。

应有职责和规划，以便一旦信息安全事态和弱点报告上来，就能有效的处理他们。要使用一个连续的改进过程对信息安全事件进行响应、监视、评价和整体管理。

如果需要证据的话，则收集证据以确保符合法律要求。

5.9.2.1 职责和规程

控制措施：

应建立管理职责和规程，以确保快速、有效和有序地响应信息安全事件。

评估指南：

除了对信息安全事态和弱点进行报告(见 5.9.1)外，还要利用对系统、报警和脆弱性的监视来检测信息安全事件。信息安全事件管理规程要考虑下列指南：

a) 要建立规程以处理不同类型的信息安全事件，包括：
   1) 信息系统故障和服务丢失；
   2) 恶意代码(见 5.6.4.1)；
   3) 拒绝服务；
   4) 不完整或不准确的业务数据导致的差错；
   5) 违反保密性和完整性；
   6) 信息系统误用。
b) 除了正常的应急计划(见 5.10.1.3)，规程还要包括(见 5.9.2.2)：
   1) 事件原因的分析和确定；
   2) 遏制事件影响扩大的策略；
   3) 如果必要，计划和实施纠正措施以防止事件再发生；
   4) 同受到事件影响或涉及事件恢复的人员进行沟通；
   5) 向合适的机构报告所采取的措施。
c) 合适时，要收集和保护审核踪迹和类似的证据(见 5.9.2.3)，以用于：
   1) 内部问题分析；
   2) 用作关系到对合同或规章要求的潜在违规，或发生民事和刑事程序诉讼(如计算机误用或数据保护法)时的法庭证据；
   3) 同软件和服务提供者谈判赔偿事宜。
d) 恢复安全违规和纠正系统故障的措施要谨慎地、正式地加以控制，规程要确保：
   1) 只有明确确定和授权的人员才允许访问正在运行的系统和数据(见 5.2.2)；
   2) 所有采取的应急措施宜详细的形成文件；
   3) 应急措施以有序的方式向管理者报告并进行评审；
   4) 对业务系统和控制措施的完整性以最小时延加以确认。

要与管理者商定信息安全事件管理的目标。要确保负责信息安全事件管理的人员理解组织机构处理信息安全事件的优先顺序。

信息安全事件可能超越组织机构和国家的边界。为了响应这样的事件，适当时，与外部组织机构协同响应和共享这些事件的信息的需求日益递增。

5.9.2.2 对信息安全事件的总结

控制措施：

应有一套机制量化和监视信息安全事件的类型、数量和代价。

评估指南：

从信息安全事件评价中获取的信息应用来识别再发生的事件或高影响的事件。

对信息安全事件的评价可以指出需要增强的或另外的控制措施，以限制事件未来发生的频率、损害和费用，或者可以用在安全方针评审过程中(见 5.1.1.2)。

5.9.2.3 证据的收集

控制措施：

当一个信息安全事件涉及诉讼(民事的或刑事的)，需要进一步对个人或组织机构进行起诉时，应收集、保留和呈递证据，以使其符合相关管辖区域对证据的要求。

评估指南：

当为了在组织机构内进行纪律处理措施而收集和提交证据时，要制定和遵循内部规程。

总的来说，关于证据的规则建议包括：

a) 证据的可采纳性：证据是否可在法庭上使用；

b) 证据的权重：证据的质量和完备性。

为了获得被容许的证据，组织机构要确保其信息系统符合任何公布的标准或实用规则，以产生被容许的证据。

提供证据的权重要符合任何适用的要求。为了获得证据的权重，在该证据的存储和处理的整个时期内，用来正确一致地保护证据(即过程控制证据)的控制措施的质量和完备性，要通过一种强证据踪迹来证明。一般情况下，这种强踪迹可以在下面的条件下建立：

c) 对于纸质文件：原稿应被安全保存且带有下列信息的记录：谁发现了该文件，文件是在哪儿被发现的，文件是什么时候被发现的，谁来证明这个发现；任何调查要确保原物没有被篡改过；

d) 对于计算机介质上的信息：要采用所有可移动介质、硬盘或内存信息的镜像或副本(依赖于适用的要求)，以确保其可用性；复制过程中所有的行为日志都要保存下来，且要有证据证明该过程；原始的介质和日志(如果这是不可能的，则至少有一个镜像或副本)要安全保存且是未改变的。

任何法律取证工作要仅在证据材料的副本上进行。所有证据材料的完整性要得到保护。证据材料的复制要在可信赖人员的监督下进行，要将关于复制过程执行时间、地点、人员、工具和程序的信息记入日志。

当一个信息安全事态首次被检测到时，这个事态是否会导致法庭起诉可能不是显而易见的。因此，在认识到事件的严重性之前，保存必要的证据以防被故意或意外毁坏的危险。可取的做法是在任何预期的法律行为中及早聘请一位律师或警察，以获取所需证据的建议。

证据可以超越组织机构和/或管辖区域的边界。在这样的情况下，要确保组织机构有资格去收集要求的信息作证据。还要考虑不同管辖区域的要求，以使证据跨越相关管辖区域被允许进入的机会最大化。

5.10 业务连续性管理

5.10.1 业务连续性管理的信息安全方面

目标：防止业务活动中断，保护关键业务过程免受信息系统重大失误或灾难的影响，并确保及时恢复。

为通过使用预防和恢复控制措施，将对组织机构的影响减少到最低，并从信息资产的损失(例如，可能是自然灾害、意外事件、设备故障和故意行为的结果)中恢复到可接受的程度，要实施业务连续性管理过程。这个过程要确定关键的业务过程。并将业务连续性的信息安全管理要求同其他的连续性要求如运行、员工、材料、运输和设施等结合起来。

灾难、安全失效、服务丢失和服务可用性的后果要经受业务影响分析。制定和实施业务连续性计划，以确保重要的运行能及时恢复。信息安全是整体业务连续性过程和组织机构内其他管理过程的一

个有机组成部分。

除了一般的风险评估过程之外，业务连续性管理要包括识别和减少风险的控制措施，以限制破坏性事件的后果，并确保业务过程需要的信息便于使用。

5.10.1.1 在业务连续性管理过程中包含信息安全

控制措施：

应为贯穿于组织机构的业务连续性开发和保持一个管理过程，以解决组织机构的业务连续性所需的信息安全要求。

评估指南：

这个过程建议包含下列业务连续性管理的关键要素：

a) 根据风险的可能性及其影响，及时理解组织机构所面临的风险，包括关键业务过程的识别和优先顺序(见 5.10.1.2)；

b) 识别关键业务过程中涉及的所有资产(见 5.3.1.1)；

c) 理解由信息安全事件引起的中断可能对业务产生的影响(重要的是找到处理产生较小影响的事件，和可能威胁组织机构生存的严重事件的解决方案)，并建立信息处理设施的业务目标；

d) 考虑购买合适的保险，该保险可以形成业务连续性过程的一部分，也是运行风险管理的一部分；

e) 识别和考虑实施另外的预防和减轻控制措施；

f) 识别足够的财务的、组织机构的、技术的和环境的资源以处理已确定的信息安全要求；

g) 确保人员的安全(safety)及信息处理设备和组织机构财产的保护；

h) 按照已商定的业务连续性策略，制定应对信息安全要求的业务连续性计划，并将其形成文件(见 5.10.1.3)；

i) 定期测试和更新已有的计划和过程(见 5.10.1.5)；

j) 确保把业务连续性的管理包含在组织机构的过程和结构中；业务连续性管理过程的职责宜分配给组织机构范围内的适当级别(见 5.2.1.1)。

5.10.1.2 业务连续性和风险评估

控制措施：

应识别能引起业务过程中断的事态，连同这种中断发生的概率和影响，以及他们对信息安全所造成的后果。

评估指南：

业务连续性的信息安全方面要从识别可能导致组织机构业务过程中断的事态(或一系列事态)开始，例如，设备故障、人为差错、盗窃、火灾、自然灾害和恐怖行为。随后是风险评估，根据时间、损坏程度和恢复周期，确定中断发生的概率和影响。

业务连续性风险评估的执行要有业务资源和过程责任人的全面参与。这种评估考虑所有业务过程，并不局限于信息处理设施，但包括信息安全特有的结果。重要的是要将不同方面的风险链接起来，以获得一幅完整的组织机构业务连续性要求的构图。该评估要按照组织机构的相关准则和目标，包括关键资源、中断影响、允许中断时间和恢复的优先级，来识别、量化并列出风险的优先顺序。

根据风险评估的结果，开发业务连续性策略，以确定整体的业务连续性方法。该策略一旦被制定，就要由管理者签署，并制定和签署实施该策略的计划。

5.10.1.3 制定和实施包含信息安全的连续性计划

控制措施：

应制定和实施计划来保持或恢复运行，以在关键业务过程中断或失败后能够在要求的水平和时间

内确保信息的可用性。

评估指南：

业务连续性规划过程建议考虑下列内容：

a) 识别和商定所有职责和业务连续性规程；

b) 识别可接受的信息和服务的损失；

c) 实施规程以在所要求的时段内恢复和复原业务运行和信息的可用性；特别需要注意对现有的内部和外部业务依赖及合同的评估；

d) 在恢复和复原完成之前遵循的运行规程；

e) 将已商定的规程和过程形成文件；

f) 在已商定的规程和过程中对员工进行适当的教育，包括危机管理；

g) 测试和更新计划。

规划过程要关注所要求的业务目标，例如，在可接受的时间内恢复到顾客的特定通信服务。识别有利于这项工作的服务和资源，包括人员储备、非信息处理资源，以及信息处理设施的基本维持运行的安排。这些基本维持运行的安排可以包括以互惠协议或者以商业捐助服务的形式与第三方的安排。

业务连续性计划要解决组织机构的脆弱性，因此可以包含需要适当保护的敏感信息。业务连续性计划的拷贝要存储在足够远的地方，以免遭主要站点的灾难损害。管理者要确保业务连续性计划的拷贝保持最新，且受到与主站点相同级别的安全保护。执行连续性计划必需的其他材料也要在远程存储。

如果使用了可替换的临时场所。则对这些场所实施的安全控制措施的级别要与主站点相同。

注意危机管理计划与活动[见 5.10.1.3f)]可能与业务连续性管理不同；即，危机可能发生，但能被正常的管理规程所涵盖。

5.10.1.4 业务连续性计划框架

控制措施：

应保持一个唯一的业务连续性计划框架，以确保所有计划是一致的，能够协调地解决信息安全要求，并为测试和维护确定优先级。

评估指南：

每个业务连续性计划要说明实现连续性的方法，例如确保信息或信息系统可用性和安全的方法。

每个计划还要规定上报计划和激活该计划的条件，以及负责执行该计划每一部分的人员。当确定新的要求时，相应地修正现有的应急规程，例如，撤离计划或基本维持运行的安排。这些规程包括在组织机构的变更管理程序中，以确保业务连续性事宜总能够得到适当地解决。

每个计划要有一个特定的责任人。应急规程、人工基本维持运行的计划，以及重新使用计划要属于相应业务资源或所涉及过程的责任人的职责范围。可替换技术服务，例如信息处理和通信设施的基本维持运行的安排通常宜是服务提供者的职责。

业务连续性计划框架提出已确定的信息安全要求，建议考虑下列内容：

a) 启动计划的条件，描述在启动每个计划之前，要遵循的过程(例如，如何评估这种情况，谁将参与)；

b) 应急规程，描述在一个危及业务运行的事件之后要采取的措施；

c) 基本维持运行的规程，描述转移重要的业务活动或支持服务到可替换的临时场所，以及在要求的时段内将业务过程带回到运行状态，需要采取的措施；

d) 在完成恢复和复原之前，要遵循的临时运行规程；

e) 重新使用规程，描述返回到正常的业务运行需要采取的措施；

f) 维护计划，规定如何及何时测试计划，以及维护该计划的过程；

g) 意识、教育和培训活动，被用来创建理解业务连续性过程和确保该过程持续有效；

h) 各人员的职责，描述谁负责执行计划的哪个部分。若要求，宜指定可替换的人；

i) 能够执行紧急的、基本维持运行的和恢复规程所需的关键资产和资源。

5.10.1.5 测试、维护和再评估业务连续性计划

控制措施：

业务连续性计划应定期测试和更新，以确保其及时性和有效性。

评估指南：

业务连续性计划的测试要确保恢复小组中的所有成员和其他有关人员了解该计划和他们对于业务连续性和信息安全的职责，并知道在计划启动后他们的角色。

业务连续性计划的测试计划安排要指出如何和何时测试该计划的每个部分。计划中的每个要素建议经常测试。

使用各种技术，为该计划在实际生存周期中的操作提供保障。建议这些技术包括：

a) 各种场景的桌面测试(使用中断例子讨论业务恢复安排)；

b) 模拟(特别是培训处于事件处理后/危机管理角色的人员)；

c) 技术恢复测试(确保信息系统可以有效地予以恢复)；

d) 在供替换场地测试恢复(远离主场地，在恢复操作同时运行业务过程)；

e) 供应商设施和服务的测试(确保外部提供的服务和产品将满足合同的承诺)；

f) 完整的演习(测试组织机构、人员、设备、设施和过程能够应付中断)。

任何组织机构都可以使用这些技术。要以一种与特定恢复计划相关的方式来使用这些技术。必要时，要记录测试结果，并采取措施改进计划。

对于每个业务连续性计划的定期评审要分配职责。识别了尚未反映在业务连续性计划中的业务安排变更后，适当地更新计划。这一正式的变更控制过程确保通过整个计划的定期评审来分发和补充已更新的计划。

建议考虑更新业务连续性计划的变更示例包括新设备的获取、系统的升级和以下方面的变更：

a) 人员；

b) 地址或电话号码；

c) 业务策略；

d) 位置、设施和资源；

e) 法律；

f) 承包方、供应商和关键顾客；

g) 过程，或者新的或撤销的过程；

h) 风险(运行的和财务的)。

5.11 符合性

5.11.1 符合法律要求

目标：避免违反任何法律、法令、法规或合同义务以及任何安全要求。

信息系统的设计、运行、使用和管理都要受法令、法规，以及合同安全要求的限制。

应从组织机构的法律顾问或者合格的法律从业人员处获得特定的法律要求建议。法律要求因国家而异，而且对于在一个国家所产生的信息发送到另一国家(即越境的数据流)的法律要求亦不同。

5.11.1.1 可用法律的识别

控制措施：

对每一个信息系统和组织机构而言，所有相关的法令、法规和合同要求，以及为满足这些要求组织机构所采用的方法，应加以明确地定义、形成文件并保持更新。

评估指南：

为满足这些要求的特定控制措施和人员的职责应同样加以定义并形成文件。

5.11.1.2 知识产权(IPR)

控制措施：

应实施适当的规程，以确保在使用具有知识产权的材料和具有所有权的软件产品时，符合法律、法规和合同的要求。

评估指南：

在保护被认为具有知识产权的材料时，建议考虑下列指南：

a) 发布一个知识产权符合性策略，该策略定义了软件和信息产品的合法使用；

b) 仅通过知名的和声誉好的渠道获得软件，以确保不侵犯版权；

c) 保持对保护知识产权的策略的了解，并通知对违规人员采取惩罚措施的意向；

d) 维护适当的资产登记簿，识别具有保护知识产权要求的所有资产；

e) 维护许可证、主盘、手册等所有权的证明和证据；

f) 实施控制措施，以确保不超过所允许的最大用户数目；

g) 进行核查，确保仅安装已授权的软件和具有许可证的产品；

h) 提供维护适当的许可证条件的策略；

i) 提供处理软件或转移软件给其他人的策略；

j) 使用合适的审核工具；

k) 符合从公共网络获得软件和信息的条款和条件；

l) 不对版权法不允许的商业录音带(胶片、音频)进行复制、格式转换或摘取内容；

m) 不对版权法不允许的书籍、文章、报告或其他文件中进行全部或部分地拷贝。

知识产权包括软件或文件的版权、设计权、商标、专利权和源代码许可证。

通常具有所有权的软件产品的供应是根据许可协议进行的，该许可协议规定了许可条款和条件，例如，限制产品用于指定的机器或限制只能拷贝到创建的备份副本上。组织机构所开发的软件的知识产权情况需要跟员工阐述清楚。

法律、法规和合同的要求可以对具有所有权的材料的拷贝进行限制。特别是，这些限制可能要求只能使用组织机构自己开发的资料，或者开发者许可组织机构使用或提供给组织机构的资料。版权侵害可能导致法律行为，这可能涉及犯罪诉讼。

5.11.1.3 保护组织机构的记录

控制措施：

应防止重要的记录的遗失、毁坏和伪造，以满足法令、法规、合同和业务的要求。

评估指南：

将记录分为记录类型，例如，账号记录、数据库记录、事务日志、审计日志等，和运行规程，每个记录都带有详细的保存周期和存储介质的类型，例如，纸质、缩微胶片、磁介质、光介质。还要保存与已加密的归档文件或数字签名(见5.8.3)相关的任何有关密钥材料，以使得录在保存期内能够解密。

考虑到存储记录的介质性能下降的可能性。要按照制造商的建议实施存储和处理规程。对于长期

保存，要考虑使用纸文件和微缩胶片。

若选择了电子存储介质，要建立规程。以确保在整个保存周期内能够访问数据（介质和格式的可读性），以防护由于未来技术变化而造成的损失。

要选择数据存储系统，使得所需要的数据能根据要满足的要求，在可接受的时间内、以可接受的格式检索出来。

存储和处理系统要确保能按照国家或地区法律或法规的规定，清晰地标识出记录及其保存期限。

该系统要允许在保存期后恰当地销毁记录，如果组织机构不再需要这些记录的话。

为满足这些记录防护目标，在组织机构范围内建议采取下列步骤：

a) 要颁发关于保存、存储、处理和处置记录和信息的指南；

b) 要起草一个保存时间计划，以标识记录及其要被保存的时间周期；

c) 要维护关键信息源的清单；

d) 要实施恰当的控制措施，以防止记录和信息丢失、损坏和篡改。

某些记录可能需要安全地保存，以满足法令、法规或合同的要求，以及支持必要的业务活动。举例来说，可以要求这些记录作为组织机构在法令或法规规则下运行的证据，以确保充分防御潜在的民事或刑事诉讼，或者和股份持有者、外部方和审核员确认组织机构的财务状况。可以根据国家法律或规章来设置信息保存的时间和数据内容。

5.11.1.4 数据保护和个人信息的隐私

控制措施：

应依照相关的法律、法规和合同条款的要求，确保数据保护和隐私。

评估指南：

制定和实施组织机构的数据保护和隐私策略。该策略通知到涉及私人信息处理的所有人员。

符合该策略和所有相关的数据保护法律法规需要合适的管理结构和控制措施。通常，这一点最好通过任命一个负责人来实现，如数据保护官员，该数据保护官员宜向管理人员、用户和服务提供商提供他们各自的职责以及宜遵守的特定规程的指南。处理个人信息和确保了解数据保护原则的职责宜根据相关法律法规来确定。宜实施适当的技术和组织机构措施以保护个人信息。

许多国家已经具有控制个人数据（一般是指可以从该信息确定生命个体的信息）收集、处理和传输的法律。根据不同的国家法律，这种控制措施可以使那些收集、处理和传播个人信息的人承担责任，而且可以限制将该数据转移到其他国家的能力。

5.11.1.5 防止滥用信息处理设施

控制措施：

应禁止用户使用信息处理设施用于未授权的目的。

评估指南：

管理者应批准信息处理设施的使用。在没有管理者批准（见 5.2.1.4）的情况下，任何出于非业务或未授权目的使用这些设施，均宜看作不正确的使用设施。如果通过监视或其他手段确定了任何非授权的活动，要使该活动引起相关管理人员的注意，以考虑合适的惩罚和/或法律行为。

在实施监视规程之前，应征求法律建议。

所有用户宜知道允许其访问的准确范围和采取监视手段检测非授权使用的准确范围。这一点可以通过下列方式实现：给用户一份书面授权，该授权的副本宜由用户签字，并由组织机构加以安全地保存。建议通知组织机构的雇员、承包方人员和第三方人员，除所授权的访问外，不允许任何访问。

登录时，建议出现警告消息，以表明正在进入的信息处理设施是组织机构所拥有的，并且不允许未授权访问。用户必须确认屏幕上的消息，并对其作出适当反应，以继续登录过程（见 5.7.5.1）。

组织机构的信息处理设施主要或只能用于业务目的。

入侵检测、内容检查和其他监视工具有助于预防和检测信息处理设施的滥用。

许多国家拥有防范计算机滥用的法律。未授权使用计算机是一种刑事犯罪。

监视的合法性因国家而异，可以要求管理者将这种监视通知给所有用户以获得他们同意。当进入的系统被用于公众访问(例如公共网站服务器)，且处于安全监控时，要显示消息说明这一情况。

5.11.1.6 密码控制措施的规则

控制措施：

使用密码控制措施应遵从相关的协议、法律和法规。

评估指南：

为符合相关的协议、法律和法规，建议考虑下面的事项：

a) 限制执行密码功能的计算机硬件和软件的入口和/或出口；

b) 限制被设计用以增加密码功能的计算机硬件和软件的入口和/或出口；

c) 限制密码的使用；

d) 利用国家对硬件或软件加密的信息的授权的强制或任意的访问方法提供内容的保密性。

要征求法律建议，以确保符合国家法律法规。在将加密信息或密码控制措施转移到其他国家之前，也要获得法律建议。

5.11.2 符合安全策略和标准以及技术符合性

目标：确保系统符合组织机构的安全策略及标准。

应定期评审信息系统的安全。

这种评审按照适当的安全策略进行，应审核技术平台和信息系统，看其是否符合适用的安全实施标准和文件的安全控制措施。

5.11.2.1 符合安全策略和标准

控制措施：

管理人员应确保在其职责范围内的所有安全规程被正确地执行，以确保符合安全策略及标准。

评估指南：

管理人员要对自己职责范围内的信息处理是否符合合适的安全策略、标准和任何其他安全要求进行定期评审。

如果评审结果发现任何不符合。管理人员要：

a) 确定不符合的原因；

b) 评价确保不符合不再发生的措施需要；

c) 确定并实施适当的纠正措施；

d) 评审所采取的纠正措施。

评审结果和管理人员采取的纠正措施要被记录，且这些记录要予以维护。当在管理人员的职责范围内进行独立评审时，管理人员宜将结果报告给执行独立评审的人员。

5.11.2.2 技术符合性核查

控制措施：

信息系统应被定期核查是否符合安全实施标准。

评估指南：

技术符合性核查建议由有经验的系统工程师手动地(如必要，由适当的软件工具支持)和/或在自动

化工具辅助下实施，以产生供技术专家进行后续解释的技术报告。

如果使用渗透测试或脆弱性评估工具，则格外小心，因为这些活动可能导致系统安全的损害。这样的测试建议预先计划，形成文件，且可重复执行。

任何技术符合性核查要仅由有能力的、已授权的人员来完成，或在他们的监督下完成。

技术符合性核查包括运行系统的试验，以确保硬件和软件控制措施被正确实施。这种类型的符合性核查需要专业技术专家。

符合性核查还包括，例如渗透测试和脆弱性评估，该项工作可以由针对此目的而专门签约的独立专家来完成。符合性核查有助于检测系统的脆弱性和核查为预防由于这些脆弱性引起的未授权访问而采取的控制措施的有效性。

渗透测试和脆弱性评估提供系统在特定时间特定状态的简单记录。这个简单记录只限制在渗透企图期间实际被测试系统的那些部分中。渗透测试和脆弱性评估不能代替风险评估。

5.11.3 信息系统审计考虑

目标：将信息系统审计过程中的有效性最大化，干扰最小化。

在信息系统审计期间，应有效控制措施防护运行系统和审计工具。

为防护审计工具的完整性和防止滥用审计工具，也要求有保护措施。

5.11.3.1 信息系统审计控制措施

控制措施：

涉及对运行系统核查的审计要求活动，应谨慎地加以规划并取得批准，以便最小化造成业务过程中断的风险。

评估指南：

建议遵守下列指南：

a) 要与合适的管理者商定审计要求；

b) 要商定和控制核查范围；

c) 核查要限于对软件和数据的只读访问；

d) 非只读的访问要仅用于对系统文件的单独拷贝，当审计完成时，要删除这些拷贝，或者按照审计文件要求，具有保留这些文件的义务，则要给予适当的保护；

e) 要明确地识别和提供执行核查所需的资源；

f) 要识别和商定特定的或另外的处理要求；

g) 要监视和记录所有访问，以产生参照踪迹；对关键数据或系统，要考虑使用时间戳参照踪迹；

h) 要将所有的规程、要求和职责形成文件；

i) 执行审计的人员要独立于被审计的活动。

5.11.3.2 信息系统审计工具的保护

控制措施：

对于信息系统审计工具的访问应加以保护，以防止任何可能的滥用或损害。

评估指南：

信息系统审计工具，如软件或数据文件，要与开发和运行系统分开，并且不能保存在磁带或用户区域内，除非给予合适级别的附加保护。

如果审计涉及第三方，则可能存在审计工具被第三方滥用，以及信息被第三方组织机构访问的风险。像5.2.2.1(评估风险)和5.5.1.2(限制物理访问)中的控制措施可以用来解决这种风险，并采取相应行动，如立即改变泄露给审核人员的口令。

6 系统能力(技术)评估

6.1 基本要求(FR)、系统要求(SR)和系统能力等级(CL)的说明

6.1.1 基本要求(FR)和系统要求(SR)的说明

系统能力的评估基于基本要求(FR),每一项基本要求又分为若干个系统要求(SR),其中有些系统要求还包含了增强要求(RE)。其与能力等级(CL)的映射见附录 B。

对于 FR1:标识和认证,是所有用户(人、软件进程和设备)在被允许访问控制系统之前,对他们进行标识和认证。

对于 FR2:使用控制,是指为已认证用户(人、软件进程或设备)分配特权以执行所请求的操作,并对这些特权的使用进行监视。

对于 FR3:系统完整性,是指确保工业控制系统完整性,以防止未经授权的操纵。

对于 FR4:数据保密性,是指确保通信信道和数据仓库的信息的保密性,防止未授权泄露。

对于 FR5:限制的数据流,是指利用区域和管道对控制系统分区,来限制不必要的数据流。

对于 FR6:对事件的及时响应,是指当事故发生时,通过以下方式对安全违背进行响应:通知适当的权威、报告所需证据、采取及时的纠正行动。

对于 FR7:资源可用性,是指确保控制系统的可用性,防止拒绝基本服务。

6.1.2 系统能力等级(CL)的说明

a) 能力等级 CL1 :提供机制保护控制系统防范偶然的、轻度的攻击。
b) 能力等级 CL2 :提供机制保护控制系统防范有意的、利用较少资源和一般技术的简单手段可能达到较小破坏后果的攻击。
c) 能力等级 CL3 :提供机制保护控制系统防范恶意的、利用中等资源、ICS 特殊技术的复杂手段的可能达到较大破坏后果的攻击。
d) 能力等级 CL4 :提供机制保护控制系统防范恶意的、使用扩展资源、ICS 特殊技术的复杂手段与工具可能达到重大破坏后果的攻击。

6.2 FR1:标识和认证控制

6.2.1 SR1.1:用户(人)的标识和认证

控制系统应提供标识和认证所有用户(人)的能力。这一能力应在访问控制系统的所有访问接口上实施,以支持符合相应安全策略和规程的职责分离和最小特权原则。

评估目标:

a) 验证用户标识符能在所有访问接口上被认证;
b) 验证无效用户标识符在所有访问接口上被拒绝。

评估指南:

验证控制系统能在所有访问接口上标识和认证所有用户,将结果记录为"支持"或"不支持"。

6.2.1.1 SR1.1 RE(1):唯一标识和认证

控制系统应对所有用户(人)提供唯一标识和认证的能力。

评估目标:

见 6.2.1;

验证所有合法用户(人)拥有唯一标识。

评估指南：

验证控制系统能在所有访问接口上唯一的标识和认证所有用户(人)，将结果记录为“支持”或“不支持”。

6.2.1.2 SR1.1 RE(2)：非可信网络的多因子认证

当人通过非可信网络访问(例如远程访问)控制系统时，控制系统应为其提供多因子认证的能力。

评估目标：

对于经由非可信网络的远程访问的认证方法要求多于一种。

评估指南：

验证控制系统能为远程访问提供多因子认证能力，记录结果为“支持”或“不支持”。

6.2.1.3 SR1.1 RE(3)：对所有网络的多因子认证

控制系统应为所有用户(人)访问控制系统提供多因子认证的能力。

评估目标：

见 6.2.1.2；

验证本地访问的认证方法要多于一种。

评估指南：

验证控制系统能为本地访问(如区域内访问)提供多因子认证能力，记录结果为“支持”或“不支持”。

6.2.2 SR1.2：软件进程和设备的标识和认证

控制系统应提供标识和认证所有用户(软件进程和设备)的能力。这一能力应在访问控制系统的所有访问接口上实施，以支持符合相应安全策略和规程的职责分离和最小特权原则。

评估目标：

a) 验证用户标识符能在所有访问接口上被认证。

b) 验证无效用户标识符在所有访问接口上被拒绝。

评估指南：

验证控制系统能在所有访问接口上标识和认证所有用户(软件进程、设备)，将结果记录为“支持”或“不支持”。

6.2.2.1 SR1.2 RE(1)：唯一标识和认证

控制系统应对所有用户(软件进程、设备)提供唯一标识和认证的能力。

评估目标：

见 6.2.1；

验证所有合法用户(软件进程、设备)拥有唯一标识。

评估指南：

验证控制系统能在所有访问接口上唯一的标识和认证所有用户(软件进程、设备)，将结果记录为“支持”或“不支持”。

6.2.3 SR1.3：账号管理

控制系统应提供对所有账号的管理，包括创建、激活、修改、禁用和移除账号的能力。

评估目标：

a) 验证控制系统账号管理员能创建账号；

b) 验证控制系统账号管理员能激活账号；

c) 验证控制系统账号管理员能修改账号；

d) 验证控制系统账号管理员能禁用账号；

e) 验证控制系统账号管理员能移除账号；

f) 验证当一个或多个账号被修改或移除时，未被修改的账号保持激活和账号权限不变。

评估指南：

验证控制系统支持账号管理功能，通过管理员类型的角色实施创建、激活、修改、禁用和移除账号，结果记录为“支持”或“不支持”。

6.2.3.1 SR1.3 RE(1)：统一的账号管理

控制系统应提供能力支持统一的账号管理。

评估目标：

控制系统应提供统一的账号管理的能力。

评估指南：

验证控制系统支持账号的统一管理，结果记录为“支持”或“不支持”。

6.2.4 SR1.4：标识符管理

控制系统应提供按照用户、组、角色和/或控制系统接口管理标识符(例如用户 ID)的能力。

评估目标：

a) 验证用户标识符可以按照用户进行管理；

b) 验证用户标识符可以按照组进行管理；

c) 验证用户标识符可以按照角色进行管理；

d) 验证用户标识符可以按照控制系统接口进行管理。

评估指南：

验证用户文档指明控制系统允许按照用户、组、角色和/或接口来管理标识符，结果记录为“支持”或“不支持”。

6.2.4.1 SR1.4 RE

无

6.2.5 SR1.5：认证码管理

控制系统应提供以下能力：

a) 定义初始的认证码内容；

b) 控制系统安装后改变默认认证码；

c) 周期的变更/更新认证码；

d) 保护认证码存储和传输时不被未经授权的泄露和更改。

评估目标：

a) 验证初始的认证码内容能被定义；

b) 验证控制系统安装后默认认证码可被变更；

c) 验证认证码可被周期的变更/更新；

d) 验证认证码在存储和传输时能被保护不受未经授权的泄露和更改。

评估指南：

a) 验证用户文档指明定义初始认证码内容的能力，结果记录为“支持”或“不支持”；

b) 验证用户文档指明变更默认认证码的能力，结果记录为“支持”或“不支持”；

c) 验证用户文档指明认证码可被变更/更新的能力，结果记录为“支持”或“不支持”；

d) 验证用户文档指明认证码在存储和传输时能被保护不受未授权的泄露和更改，结果记录为“支持”或“不支持”。

6.2.5.1 SR1.5 RE(1)：软件进程标识凭证的硬件安全

对于软件进程和设备用户，控制系统应提供使用硬件机制保护相关认证码的能力。

评估目标：

见 6.2.4；

验证控制系统能提供硬件机制保护软件进程和设备用户的相关认证码。

评估指南：

验证用户文档指明利用硬件机制保护相关认证码的能力，结果记录为“支持”或“不支持”。

6.2.6 SR1.6：无线访问管理

对参与无线通信的所有的用户（人、软件进程或设备），控制系统应提供标识和认证的能力。

评估目标：

a) 验证合法用户标识符能在无线访问接口上被认证；

b) 验证无效用户标识符在无线访问接口上被拒绝。

评估指南：

验证控制系统对于参与无线通信的用户（人、软件进程或设备）能进行标识和认证，结果记录为“支持”或“不支持”。

6.2.6.1 SR1.6 RE(1)：唯一标识和认证

对参与无线通信的所有的用户（人、软件进程或设备），控制系统应提供唯一标识和认证的能力。

评估目标：

见 6.2.6；

验证所有合法用户在无线接口上拥有唯一标识。

评估指南：

验证控制系统能在无线访问接口上唯一的标识和认证所有用户（人、软件进程或设备），将结果记录为“支持”或“不支持”。

6.2.7 SR1.7：口令认证的加强

对于使用口令认证的控制系统，控制系统应提供能力，实施可配置的基于最小长度和不同字符类型的口令强度。

评估目标：

a) 验证控制系统提供实施口令的最小长度的能力。验证小于最小长度的口令被拒绝用于认证。

b) 验证控制系统提供能力，实施口令中除字母字符外至少还要包含最小数目的特殊字符。验证不符合最小字符集的口令被拒绝用于认证。

评估指南：

a) 验证用户文档指明控制系统支持基于最小长度来配置口令强度，结果记录为“支持”或“不支持”；

b) 验证用户文档指明控制系统支持基于不同字符类型变化来配置口令强度，结果记录为“支持”或“不支持”。

6.2.7.1 SR1.7 RE(1):对用户(人)的口令生成和口令有效期的限制

控制系统应为用户(人)提供口令重用次数限制、以及口令最小和最大有效期限制的能力,这些能力符合普遍接受的安全工业实践。

评估目标:

验证口令被重用一定次数后不能再用于认证;

验证超出口令有效期的口令不能用于认证。

评估指南:

验证用户文档指明了口令重用次数被限制在一个指定的数目内、用户可以设定口令的最小和最大有效期限,结果记录为"支持"或"不支持"。

6.2.7.2 SR1.7 RE(2):对所有用户的口令有效期的限制

控制系统应为所有用户提供实施口令最小和最大有效期限制的能力。

评估目标:

验证控制系统能为所有用户提供口令最小和最大有效期限制。

评估指南:

验证用户文档指明对所有用户可以设置口令的最小和最大有效期限制,结果记录为"支持"或"不支持"。

6.2.8 SR1.8:公钥基础设施证书

当使用公钥基础设施 PKI 时,控制系统应提供能力按照普遍接受的最佳实践运行 PKI 或从现有 PKI 中获取公钥证书。

评估目标:

验证控制系统能按照普遍接受的最佳实践运行 PKI 或从现有 PKI 中获取公钥证书。

评估指南:

验证控制系统能与现有 PKI 接口,结果记录为"支持"、"不支持"或"不适用(未使用密码)"。

6.2.8.1 SR1.8 RE

无

6.2.9 SR1.9:公钥认证的加强

对于使用公钥认证的控制系统,控制系统应提供以下能力:

a) 通过检查给定证书的签名的有效性来证实证书;

b) 通过建立证书路径到可接受的证书认证机构(CA)证实证书,或在自签名证书情况下,某主体被分发证书后,所有与该主体通信的主机部署叶子证书;

c) 通过给定证书的撤销状态证实证书;

d) 建立用户(人、软件进程和设备)对相应私钥的控制;

e) 将已认证的标识映射为用户(人、软件进程和设备)。

评估目标:

对于采用公钥认证的控制系统,验证控制系统能证实证书并将已认证的身份映射为用户。

评估指南:

验证用户文档指明如果具备公钥功能,则支持要求的公钥认证,记录结果为"支持"、"不支持"或"不适用-如果不支持公钥"。

6.2.9.1 SR1.9 RE(1)：公钥认证的硬件安全

控制系统应提供能力，按照普遍接受的安全工业实践和推荐，通过硬件机制保护相关的私钥。

评估目标：

验证控制系统能按照普遍接受的安全工业实践采用硬件机制保护私钥。

评估指南：

验证私钥采用硬件机制保护，结果记录为“支持”、“不支持”或“不适用(未使用密码)”。

6.2.10 SR1.10：认证反馈

在认证过程中，控制系统应提供将认证信息的反馈模糊化的能力。

评估目标：

验证控制系统将认证信息的反馈模糊化，使得当一个或多个凭证无效时，失败的认证尝试不提供任何合法凭证有效性的信息(例如用户名和口令)。

评估指南：

验证控制系统能模糊化认证信息的反馈，记录结果为“支持”或“不支持”。

6.2.10.1 SR1.10 RE

无

6.2.11 SR1.11：失败的登录尝试

控制系统应提供能力，对任何用户(人、软件进程和设备)在可配置的时间周期内连续无效访问尝试的次数限制为一个可配置的数目。控制系统应提供能力，在可配置时间周期内未成功尝试次数超过上限时，在指定时间内拒绝访问或者直到由管理员解锁。

代表哪些关键服务或服务器运行的系统账号，控制系统不应允许交互式登录。

评估目标：

验证控制系统能监视不成功的登录尝试，具有可配置的能力，可基于反复的未成功尝试拒绝其访问。

评估指南：

a) 验证控制系统有能力监视不成功的登录尝试，基于反复的不成功登录尝试可以配置永久拒绝访问或者一段可配置时间内拒绝访问，记录结果为“支持”或“不支持”；

b) 验证用户文档指明代表哪些关键服务或服务器运行的系统账号，不允许交互式登录，记录结果为“支持”或“不支持”。

6.2.11.1 SR1.11 RE

无

6.2.12 SR1.12：系统使用通知

控制系统应有能力在认证之前，显示可配置的系统使用通知消息。

评估目标：

a) 验证配置系统使用通知的能力；

b) 验证控制系统可以在登录时显示配置好的系统使用通知。

评估指南：

验证控制系统有能力显示用户可配置的系统使用通知，记录结果为“支持”或“不支持”。

6.2.12.1 SR1.12 RE

无

6.2.13 SR1.13:经由非可信网络的访问

控制系统应提供能力监视和控制所有经由不可信网络对控制系统的访问方法。

评估目标:

a) 验证控制系统控制来自不可信网络的远程访问;

b) 验证控制系统识别和监视来自不可信网络的远程访问。

评估指南:

验证用户文档指明支持监视和控制来自不可信网络的所有形式的远程访问,结果记录为"支持"或"不支持"。

6.2.13.1 SR1.10 RE(1):明确地对访问请求的批准

默认的,控制系统应提供能力拒绝来自不可信网络的访问,除非被指定角色批准。

评估目标:

验证控制系统有能力默认的拒绝所有远程访问。

评估指南:

验证用户文档包含默认拒绝远程访问的能力,结果记录为"支持"或"不支持"。

6.3 FR2:使用控制

6.3.1 SR2.1:授权的执行

在所有接口上,控制系统应提供能力执行分配给所有用户(人)的授权,按照职责分离和最小特权来控制对控制系统的使用。

评估目标:

验证已认证的用户(人)不能执行未授权的功能。

评估指南:

验证控制系统依照账号管理的配置执行授权来控制用户(人)对控制系统的使用,结果记录为"支持"或"不支持"。

6.3.1.1 SR2.1 RE(1):对所有用户执行授权

在所有接口上,控制系统应提供能力执行分配给所有用户(人、软件进程和设备)的授权,按照职责分离和最小特权来控制对控制系统的使用。

评估目标:

验证已认证的所有用户(人、软件进程和设备)不能执行未授权的功能。

评估指南:

验证控制系统依照账号管理的配置执行授权来控制所有用户(人、软件进程和设备)对控制系统的使用,结果记录为"支持"或"不支持"。

6.3.1.2 SR2.1 RE(2):许可映射到角色

控制系统应为资产所有者提供修改许可到角色的映射的能力。

评估目标:

确认控制系统提供以下预先配置的角色和/或可由用户配置的角色：

a) 浏览；

b) 操作员；

c) 控制应用工程师；

d) 控制系统管理员；

e) 操作主管；

f) 仪表技术员。

评估指南：

验证主管级账号授权的情况下，控制系统有能力映射许可到角色，结果记录为“支持”或“不支持”。

6.3.1.3 SR2.1 RE(3)：主管越权

控制系统应支持主管在可配置的时间内或事件顺序上手工越权于当前用户(人)的授权。

评估目标：

如果提供该功能，确认控制系统为主管手工越权提供配置时限或配置事件顺序限制的能力。

评估指南：

验证控制系统为主管手工越权提供可配置的时间限制或事件顺序限制，结果记录为“支持”、“不支持”或“不适用(如果不支持主管手工越权)”。

6.3.1.4 SR2.1 RE(4)：双授权

在行为可能对工业流程产生严重影响之处，控制系统应支持双授权。

评估目标：

验证控制系统在需要时可配置双授权。

评估指南：

验证控制系统在需要时能提供双授权，结果记录为“支持”或“不支持”。

6.3.2 SR2.2：无线使用控制

控制系统应提供能力，对控制系统的无线连接应依据普遍接受的安全工业实践进行授权、监视和限制使用。

评估目标：

a) 验证控制系统能授权、监视和限制对控制系统的无线访问；

b) 验证控制系统能使用适当的认证机制保护无线访问。

评估指南：

a) 验证控制系统提供能力，使用认证机制保护对控制系统的无线访问，结果记录为“支持”、“不支持”或“不适用(如果不支持无线访问)”；

b) 验证控制系统提供能力，监视对控制系统的无线访问，结果记录为“支持”、“不支持”或“不适用(如果不支持无线访问)”。

6.3.2.1 SR2.2 RE(1)：对未授权的无线设备进行识别和报告

控制系统应提供识别和报告未授权的无线设备在控制系统物理环境内发射信号的能力。

评估目标：

a) 验证控制系统能扫描控制系统物理环境内发射信号的无线设备；

b) 验证控制系统能识别和报告识别和报告在控制系统物理环境内发射信号的未授权的无线设备。

评估指南：

验证控制系统提供识别和报告未授权的无线设备的能力，结果记录为“支持”、“不支持”或“不适用（如果不支持无线访问）”。

6.3.3 SR2.3：对便携和移动设备的使用控制

对于便携和移动设备，控制系统应提供自动实施可配置的使用限制的能力，包括：

a) 防止使用便携和移动设备；

b) 要求上下文特定的授权；

c) 限制代码和数据传入和传出便携和移动设备。

评估目标：

a) 验证控制系统提供手段来禁用/控制便携或移动设备的使用；

b) 验证控制系统监视和记录便携和移动设备的访问和使用；

c) 如适用，验证控制系统安全手册提供了对便携和移动设备使用限制的列表。

评估指南：

验证控制系统提供了对便携和移动设备自动实施可配置的使用限制的能力，结果记录为“支持”或“不支持”。

6.3.3.1 SR2.3 RE(1)：便携和移动设备的安全状态的实施

控制系统应提供能力确保，便携和移动设备连接到一个区域之前，其安全状态符合该区域的安全策略和规程。

评估目标：

a) 验证控制系统提供在授权连接之前对便携和移动设备进行扫描；

b) 验证控制系统监视和记录扫描结果；

c) 验证控制系统安全手册提供对移动设备合规扫描进行配置的指示。

评估指南：

验证控制系统有方法确保便携和移动设备连接到控制系统之前，其安全状态符合安全策略和规程，结果记录为“支持”或“不支持”。

6.3.4 SR2.4：移动代码

控制系统应提供以下能力，基于移动代码破坏控制系统的潜在可能性，对移动代码技术的使用进行限制包括对移动代码的使用进行监视：

a) 预防移动代码的执行；

b) 对代码源要求适当的认证和授权；

c) 限制移动代码传入/传出控制系统；

d) 监视移动代码的使用。

评估目标：

a) 验证控制系统提供禁用/控制使用移动代码技术的方法；

b) 验证控制系统监视和记录移动代码技术的使用；

c) 验证控制系统安全手册提供了限制使用移动代码技术的列表。

评估指南：

验证用户文档提供了限制移动代码技术的手段，结果记录为“支持”或“不支持”。

6.3.4.1 SR2.4 RE(1)：移动代码的完整性检查

控制系统应提供能力，在允许代码执行之前验证移动代码的完整性。

评估目标：

验证控制系统提供验证移动代码完整性的方法。

评估指南：

验证控制系统提供了验证移动代码完整性的手段，结果记录为“支持”或“不支持”。

6.3.5 SR2.5：会话锁

控制系统应提供能力，在会话不活跃状态超过可配置的时间周期之后，启用会话锁防止其进一步的访问，会话锁应保持有效直到用户（人）或被授权的主管人员使用适当的标识和认证规程重新建立访问。

评估目标：

a) 验证会话期间无活动超过配置的超时周期后，会话锁超时被启动；

b) 验证仅当同一个授权个人用户或角色或者主管人员成功完成重新认证流程之后，会话锁才被移除。

评估指南：

验证用户文档包含证据证明支持会话锁超时，结果记录为“支持”或“不支持”。

6.3.5.1 SR2.5 RE

无

6.3.6 SR2.6：远程会话终止

控制系统应提供在可配置的不活跃时间周期后自动终止远程会话或由发起会话的用户手动终止远程会话的能力。

评估目标：

验证可配置的超时周期内无活动后，远程会话被终止；

验证发起会话的用户可以手动终止远程会话。

评估指南：

验证控制系统能够配置为超过可配置的时间后自动终止、或由发起会话的用户手动终止远程会话，结果记录为“支持”或“不支持”。

6.3.6.1 SR2.6 RE

无

6.3.7 SR2.7：并发会话控制

对任意给定用户（人、软件进程或设备），控制系统应提供将每个接口的并发会话的数目限制为一个可配置的数目的能力。

评估目标：

验证控制系统在配置的时限被超过时能够限制并发远程会话的数据。

评估指南：

验证控制系统能够配置为限制并发远程会话的数目，结果记录为“支持”或“不支持”。

6.3.7.1 SR2.7 RE

无

6.3.8 SR2.8：可审计的事件

控制系统应提供为以下类别生成审计记录的能力：访问控制、请求错误、系统事件、备份和存储事

件、配置变更、潜在的侦查行为和审计日志事件。

每个审计记录应包括时间戳、源(发起设备、软件进程或人)、类别、类型、事件 ID 和事件结果。

评估目标:

验证控制系统能够识别需要审计的以及与控制系统安全相关的重要事件。

评估指南:

a) 通过用户文档验证控制系统支持为以下类别生成审计记录的能力:访问控制、请求错误、系统事件、备份和存储事件、配置变更、潜在的侦查行为和审计日志事件,结果记录为"支持"或"不支持";

b) 通过用户文档验证控制系统生成的审计记录至少包含时间戳、每个日志记录应包括时间戳、源(发起设备、软件进程或人)、类别、类型、事件 ID 和事件结果,结果记录为"支持"或"不支持"。

6.3.8.1 SR2.8 RE(1):中央管理的、系统范围的审计跟踪

控制系统应提供能力,对审计事件进行中央管理,并将来自整个控制系统内多个元器件的审计记录汇聚为系统范围的、时间相关的审计跟踪。控制系统应提供按照工业标准格式输出审计记录的能力,以便标准的商业日志分析工具(例如安全信息和事件管理 SIEM)对其分析。

评估目标:

a) 验证控制系统能中央管理审计和分析事件;

b) 验证控制系统能适当的输出审计记录。

评估指南:

通过用户文档验证控制系统支持将来自整个控制系统内多个元器件的审计记录进行汇聚的能力,结果记录为"支持"或"不支持"。

6.3.9 SR2.9:审计存储容量

控制系统应根据日志管理和系统配置普遍认可的推荐值来分配足够的审计记录存储容量。控制系统应提供审计机制减少超出该容量的可能性。

评估目标:

验证控制系统能考虑以下因素情况下提供足够的审计存储容量,这些因素包括保存策略、应执行的审计和在线审计处理要求。

评估指南:

验证供货商已进行分析指明了审计记录存储容量是足够的,验证该分析与普遍认可的日志管理的推荐值一致。验证控制系统具备机制来避免容量被超出,结果记录为"支持"或"不支持"。

6.3.9.1 SR7.9 RE(1):达到审计记录存储容量上限时发出警告

当分配的审计记录存储量达到最大审计记录存储容量的某个可配置比例时,控制系统应提供发出警告的能力。

评估目标:

验证控制系统能在达到审计记录存储容量上限时发出警告。

评估指南:

验证用户文档包含证据证明审计功能在存储使用率达到门限时支持通知功能,结果记录为"支持"或"不支持"。

6.3.10 SR2.10:对审计流程失败时的响应

验证控制系统能对审计流程失败提供适当的响应。

评估目标：

a) 在审计流程失败时，控制系统应提供向人员告警并防止技术服务和功能丢失的能力。

b) 当审计流程失败时，控制系统应提以下响应的能力：覆盖最老的审计记录、停止生成审计记录。

评估指南：

a) 验证用户文档包含证据证明控制系统能在审计流程失败时生成告警，结果记录为“支持”或“不支持”；

b) 验证用户文档包含证据证明审计功能当存储空间不足以记录新事件时支持采用以下方式：覆盖最老的审计记录、停止生成审计记录，结果记录为“支持”或“不支持”。

6.3.11 SR2.11：时间戳

控制系统应提供时间戳用于生成审计记录。

评估目标：

a) 验证可记录的系统行为被记录下来并带有时间戳；

b) 验证在系统事件精度范围内，多个可记录行为采用唯一的时间戳被记录下来。

评估指南：

通过查看系统审计日志，验证系统范围的审计记录包含时间戳，结果记录为“支持”或“不支持”。

6.3.11.1 SR2.11 RE(1)：内部时间同步

控制系统应提供以可配置的频率同步内部系统时钟的能力。

评估目标：

验证跨越多个子系统的具有不同系统时钟的多个系统行为日志被同步。

评估指南：

验证用户文档包含证据证明提供时间戳同步，结果记录为“支持”或“不支持”。

6.3.11.2 SR2.11 RE(2)：时间源的完整性的保护

时间源应被保护不受未授权的变更，其变更应触发审计事件。

评估目标：

a) 验证改变系统时间需要的方法和授权；

b) 验证未授权的系统时间改变被防止。

评估指南：

验证用户文档包含证据证明，用于时间戳的时间同步受到保护不被未授权变更，结果记录为“支持”或“不支持”。

6.3.12 SR2.12：不可否认性

控制系统应提供对给定用户(人)是否实施了某个特定行为进行判定的能力。

评估目标：

验证控制系统能为人的行为提供不可否认性。

评估指南：

验证用户文档包含证据，为发起某事件负责的人可以被包含在审计记录中，结果记录为“支持”或“不支持”。

6.3.12.1 SR2.12 RE(1)：所有用户的不可否认性

控制系统应提供对所有用户是否执行了某个行为进行判定的能力。

评估目标：

验证控制系统能为所有用户的行为提供不可否认性。

评估指南：

验证用户文档包含证据，为发起某事件负责的用户（包括人、软件进程和设备）可以被包含在审计记录中，结果记录为“支持”或“不支持”。

6.4 FR3：系统完整性

6.4.1 SR3.1：通信完整性

控制系统应保护传输的信息的完整性。

评估目标：

验证控制系统能在信息传输时保护其完整性。

评估指南：

检查设计和用户文档，确定通信信道上传输的关键数据的完整性受到保护。

6.4.1.1 SR3.1 RE(1)：基于密码技术的完整性保护

控制系统应提供能力采用密码学机制识别信息在通信过程中的变更，除非信息已被其他可替换的物理措施保护。

评估目标：

验证控制系统能利用密码学的机制保护信息在传输中的完整性。

评估指南：

检查设计和用户文档，确定通信信道上传输的关键任务数据的完整性通过密码学机制来保护，结果记录为“支持”或“不支持”。

6.4.2 SR3.2：恶意代码的防护

控制系统应提供能力，采用防护机制来防止、检测、报告和消减恶意代码或非授权软件的影响。控制系统应提供更新防护机制的能力。

评估目标：

a) 验证控制系统提供或推荐产品以防护恶意代码；

b) 验证防护产品被配置、被启用；

c) 验证防护产品被更新到最新版本；

d) 验证防护产品提供其能防护的恶意代码类型的列表或说明。

评估指南：

a) 验证控制系统提供或推荐产品以防护恶意代码，结果记录为“支持”或“不支持”；

b) 验证防护产品被配置、被启用，结果记录为“支持”或“不支持”；

c) 验证防护产品被更新到最新版本，结果记录为“支持”或“不支持”；

d) 验证防护产品提供其能防护的恶意代码类型的列表或说明。结果记录为“支持”或“不支持”。

6.4.2.1 SR3.2 RE(1)：在入口和出口点防护恶意代码

控制系统应提供在所有入口和出口点上采用恶意代码防护机制的能力。

评估目标：

a) 验证控制系统在区域边界提供恶意代码的防护；

b) 验证防护产品被配置和被启用；

c) 验证防护产品被更新到最新的版本；

d) 验证防护产品提供其能防护的恶意代码类型的列表或说明。

评估指南：

验证控制系统提供区域边界的恶意代码防护，结果记录为“支持”或“不支持”。

6.4.2.2 SR3.2 RE(2)：恶意代码防护的中央管理和报告

控制系统应提供管理恶意代码防护机制的能力。

评估目标：

验证控制系统能对恶意代码防护机制进行中央管理。

评估指南：

通过审查设计文档验证控制系统对恶意代码防护机制提供中央管理和报告能力，结果记录为“支持”或“不支持”。

6.4.3 SR3.3：安全功能验证

控制系统应提供能力，验证安全功能的预期操作，并在工厂验收测试 FAT、现场验收测试 SAT 和预定维护中发现异常时进行报告。控制系统应提供能力来验证产品提供商和/或系统集成商提供如何测试所设计的安全控制的指导。

评估目标：

验证控制系统能在工厂验收测试(FAT)、现场验收测试(SAT)和预定维护中验证安全功能的预期操作并在发现异常时进行报告。

评估指南：

验证控制系统或者控制系统文档提供方法，在 FAT、SAT 或预定维护时验证安全功能，并报告异常，结果记录为“支持”或“不支持。”

6.4.3.1 SR3.3 RE(1)：安全功能验证的自动化机制

控制系统应提供能力在 FAT、SAT 和预定维护时采用自动化机制支持分布式安全验证的管理。

评估目标：

验证控制系统能采用自动化机制在 FAT、SAT 和预定维护时管理分布式安全验证。

评估指南：

验证控制系统或控制系统文档提供方法在 FAT、SAT 或预定维护时测试安全功能，结果记录为“支持”或“不支持。”

6.4.3.2 SR3.3 RE(2)：正常运行中的安全功能验证

控制系统应提供能力，在正常运行时验证安全功能的预期操作。

评估目标：

控制系统能在正常运行时验证安全功能的预期操作。

评估指南：

验证控制系统提供正常运行时测试安全功能的方法，结果记录为“支持”或“不支持。”

6.4.4 SR3.4：软件和信息完整性

控制系统应提供能力检测、记录和保护软件和信息不受未经授权的变更。

评估目标：

验证控制系统能提供保护软件和信息完整性的机制。

评估指南：

验证控制系统或控制系统文档提供手工的或自动化的完整性机制（例如密码学哈希）来验证关键控制系统软件和控制信息的完整性，结果记录为“支持”或“不支持。”

6.4.4.1 SR3.4 RE(1)：对破坏完整性进行自动通知

控制系统应提供能力，使用自动化工具在完整性验证期间发现不符时通知人员。

评估目标：

验证控制系统能在配置范围内检测和报告不符。

评估指南：

验证控制系统提供自动化方法验证软件和配置完整性，并自动通知，结果记录为“支持”或“不支持”。

6.4.5 SR3.5：输入验证

控制系统应验证任何输入的语法和内容，这些输入是作为工业过程控制输入或直接影响控制系统行为的输入。

评估目标：

验证控制系统能验证输入的语法和内容。

评估指南：

验证控制系统或控制系统文档提供手册或自动化方法来验证来自外部源的信息的完整性，结果记录为“支持”、“不支持”或“不适用——控制系统不接受来自外部源的过程控制输入”。

6.4.5.1 SR3.5 RE

无

6.4.6 SR3.6：确定性的输出

控制系统提供能力，在遭受攻击无法保持正常运行时能够将输出设为预先定义的状态。

评估目标：

验证控制系统能够将输出设为预先定义的状态，这些状态包括：

a) 未上电状态；

b) 可知的最后的值；

c) 由资产属主或应用确定的固定值。

验证

评估指南：

验证控制系统或控制系统文档提供手册或方法将输出设为预先定义的状态，结果记录为“支持”或“不支持”。

6.4.6.1 SR3.6 RE

无

6.4.7 SR3.7：错误处理

控制系统识别和处理错误条件的方式应能够实施有效的补救，这一方式不能提供可能被敌人利用来攻击工业控制系统 ICS 的信息，除非泄露这一信息对于及时发现并修理问题是必须的。

评估目标：

验证控制系统能规定错误信息的适当的结构和内容，以提供及时有用的信息而不暴露潜在的有害信息。

评估指南：

验证控制系统错误信息提供足够的和必须的信息帮助工厂人员识别和诊断系统问题，而不暴露可能被攻击者用来攻击系统的敏感信息，结果记录为“支持”或“不支持”。

6.4.7.1 SR3.7 RE

无

6.4.8 SR3.8：会话完整性

控制系统应提供保护通信会话完整性的机制。

评估目标：

验证控制系统能为通信会话的每一端提供对对端身份和传输信息正确性的信任。

评估指南：

验证控制系统或控制系统文档提供保护会话完整性的机制，结果记录为“支持”或“不支持”。

6.4.8.1 SR3.8 RE(1)：会话终止后会话 ID 的失效

在用户退出或会话终止(包括浏览器会话)后，控制系统应提供使其会话标识失效的能力。

评估目标：

a) 验证已有会话不能被重用，直到该会话终止之后超过一个预定义的周期后。

b) 验证用户退出后会话 ID 无效。

评估指南：

验证用户会话标识符在用户退出后无效，结果记录为“支持”、“不支持”或“不适用如果不支持会话或会话 ID”。

6.4.8.2 SR3.8 RE(2)：唯一会话 ID 的产生和承认

控制系统应提供能力，为每个会话生成唯一的会话标识 ID，并且只认可系统生成的会话标识。

评估目标：

a) 验证只有控制系统能生成和确认会话标识；

b) 验证非法会话标识不被控制系统接受。

评估指南：

验证用户会话标识符是唯一的，并拒绝非系统生成的标识符，结果记录为“支持”、“不支持”或“不适用如果不支持会话或会话 ID”。

6.4.8.3 SR3.8 RE(3)：会话 ID 的随机性

控制系统应提供使用普遍接受的随机源生成唯一的会话标识的能力。

评估目标：

验证会话 ID 不能被追踪。

评估指南：

验证用户会话标识符由系统产生并具有可接受的随机性水平，结果记录为“支持”、“不支持”或“不适用如果不支持会话或会话 ID”。

6.4.9 SR3.9：审计信息的保护

控制系统应保护审计信息和审计工具不被未授权的访问、修改和删除。

评估目标：

验证控制系统能保护审计信息和审计工具不被未授权的访问、修改和删除。

评估指南：

验证用户文档包含证据证明，审计记录只能被授权用户正确认证之后访问，结果记录为“支持”或“不支持”。

6.4.9.1 SR3.9 RE(1)：一次性写入介质上的审计记录

控制系统应提供在基于硬件的、一次性写入介质上生成审计记录的能力。

评估目标：

验证系统能利用基于硬件的、一次性写入介质保护审计记录的完整性。

评估指南：

验证用户文档包含证据证明审计记录能被存储在一次性写入介质上，结果记录为“支持”或“不支持”。

6.5 FR4：数据保密性

6.5.1 SR4.1：信息保密性

控制系统应提供能力，对有读授权的信息在静态和传输中进行保密性保护。

评估目标：

a) 验证控制系统通过维护具有可控物理访问的可信网络来保护敏感信息的保密性（认证信息，例如用户名和口令应考虑保密）；

b) 验证敏感信息已被识别；

c) 验证控制系统对敏感信息的访问和传输进行控制，以防止窃听和篡改。

评估指南：

验证控制系统保护敏感信息的机密性，结果记录为“支持”或“不支持”。

6.5.1.1 SR4.1 RE(1)：静态和经由不可信网络传输的数据的保密性保护

控制系统应提供能力保护静态信息和穿越不可信网络的远程访问会话的保密性。

评估目标：

验证敏感的控制系统信息，例如口令，在存储和穿过外部网络传输时是加密的。

评估指南：

验证控制系统能保护敏感（保密）信息在静态时、在穿过外部的非可信网络的远程访问会话中的机密性。

6.5.1.2 SR4.1 RE(2)：区域边界的机密性保护

控制系统应提供能力保护穿越所有区域边界的信息的机密性。

评估目标：

验证敏感的控制系统数据例如口令在存储和穿越区域边界时是加密的。

评估指南：

验证控制系统能保护敏感（保密）信息穿过区域边界的机密性，结果记录为“支持”或“不支持”。

6.5.2 SR4.2：信息存留

控制系统感应提供退役能力，清除被在用服务所释放的元器件中所有与安全相关的资料。

评估目标：

验证从在用服务中移除一个控制系统组件不应提供无意泄露安全相关资料的机会。

评估指南：

验证控制系统提供退役能力或指示如何在系统组件被在用服务释放之前，清除该系统组件的所有安全相关资料，结果记录为“支持”或“不支持”。

6.5.2.1 SR4.2 RE(1)：共享内存资源的清除

控制系统应防止借助易失性存储资源进行的未经授权的和无意的信息传输，当易失性共享存储释放回控制系统供不同用户使用时，所有的特有数据及特有数据的关联都应从资源中清除，从而使新用户对其不可见和不可访问。

评估目标：

验证控制系统能防止借助易失性存储资源进行的未经授权和无意的信息传输。

评估指南：

通过设计文档验证，当非永久性共享存储释放回控制系统供不同用户使用时，所有的特有数据及特有数据的关联被清除，从而无法被其他用户访问，结果记录为“支持”或“不支持”。

6.5.3 SR4.3：密码的使用

如果需要密码，控制系统应根据普遍接受的工业实践和推荐来使用密码算法、密钥长度以及密钥创建和管理机制。

评估目标：

a) 识别工业实践所普遍接受的密码算法、密钥长度和机制；

b) 验证控制系统支持上述某些密码算法、密钥长度和机制。

评估指南：

通过设计文档验证控制系统根据普遍接受的工业最佳实践和推荐来使用密码算法、密钥长度以及密钥创建和管理机制，结果记录为“支持”、“不支持”或“不适用(未使用密码)”。

6.5.3.1 SR4.3 RE

无

6.6 FR5：限制的数据流

6.6.1 SR5.1：网络分区

控制系统应提供能力将控制系统网络与非控制系统网络进行逻辑分区，对关键控制系统网络和其他控制系统网络进行逻辑分区。

评估目标：

a) 验证控制系统网络能与非控制系统网络逻辑分区；

b) 验证关键控制系统网络能与其他控制系统网络进行逻辑分区。

评估指南：

a) 验证将控制系统网络与非控制系统网络进行逻辑分区的手段，结果记录为“支持”或“不支持”；

b) 验证将关键控制系统网络与其他控制系统网络进行逻辑分区的手段，结果记录为“支持”或

“不支持”。

6.6.1.1 SR5.1 RE(1):物理网络分区

控制系统应提供能力将控制系统网络与非控制系统网络进行物理分区,对关键控制系统网络和其他控制系统网络进行物理分区。

评估目标:

a) 验证控制系统网络能与非控制系统进行物理分区;

b) 验证关键控制系统网络能与其他控制系统网络进行物理分区。

评估指南:

通过用户文档验证,控制系统提供能力将控制系统网络与非控制系统网络进行物理分段以及将关键控制系统网络与其他网络进行物理分区,结果记录为“支持”或“不支持”。

6.6.1.2 SR5.1 RE(2):与非控制系统网络的独立性

控制系统能具有能力向控制系统网络(无论关键与否)提供网络服务,而不与非控制系统网络连接。

评估目标:

a) 验证控制系统能向控制系统网络提供网络服务;

b) 验证控制系统提供网络服务而不与非控制系统连接。

评估指南:

通过用户文档验证控制系统具有向控制系统网络提供网络服务的能力,而不与非控制系统连接,结果记录为“支持”或“不支持”。

6.6.1.3 SR5.1 RE(3):关键网络的逻辑和物理隔离

控制系统应提供能力,将关键控制系统网络与其他控制系统网络进行逻辑和物理隔离。

评估目标:

验证关键网络与其他控制系统网络逻辑隔离和物理隔离。

评估指南:

通过用户文档验证控制系统提供将关键控制系统网络和其他网络进行逻辑和物理分区的能力,结果记录为“支持”或“不支持”。

6.6.2 SR5.2:区域边界防护

控制系统应提供监视和控制区域边界通信的能力,以实现基于风险的区域和管道模型定义的划分。

评估目标:

a) 验证控制下能监视区域边界的通信;

b) 验证控制系统能控制区域边界的通信以实施划分。

评估指南:

验证控制系统通过适当的边界设备对所有区域边界的外部接口进行管理,结果记录为“支持”或“不支持”。

6.6.2.1 SR5.2 RE(1):默认拒绝,例外允许

控制系统应提供默认拒绝所有网络流量、例外允许网络流量(也称为拒绝所有,允许例外)的能力。

评估目标:

验证控制系统只能允许预先定义的流量。

评估指南:

验证控制系统边界设备的设置能够基于例外允许原则进行配置，结果记录为“支持”或“不支持”。

6.6.2.2 SR5.2 RE(2)：孤岛模型

控制系统应提供能力防止任何通过控制系统边界的通信(也称为孤岛模型)。

评估目标：

验证控制系统能孤立与非控制系统。

评估指南：

通过用户文档验证控制系统边界设备可以配置为当检测到安全事件时拒绝所有访问，结果记录为“支持”或“不支持”。

6.6.2.3 SR5.2 RE(3)：故障关闭

当边界防护机制出现操作故障时，控制系统应提供阻止所有控制系统边界通信(也称为故障关闭)的能力。故障关闭功能的设计应不干扰功能安全仪表系统或其他功能安全相关功能的运行。

评估目标：

a) 识别边界防护机制的操作故障；

b) 验证控制系统能在上述故障发生时防止所有控制系统边界的通信。

评估指南：

通过用户文档验证控制系统边界设备能被配置为故障发生时关闭所有访问，结果记录为“支持”或“不支持”。

6.6.3 SR5.3：一般目的的个人间通信的限制

控制系统应提供能力防止一般目的的个人间通信消息被控制系统外部的用户或系统接收到。

评估目标：

控制系统应提供能力，防止一般目的的个人间通信，如 email 系统、社交媒体(Twitter，facebook，等)，以及任何允许传输可执行文件的消息系统，被用于引入恶意软件、导致信息泄露或引入额外的网络负担从而造成安全问题或对控制系统进行攻击。

评估指南：

验证控制系统能够防止个人通信消息被控制系统以外的用户或系统收到，结果记录为“支持”或“不支持”。

6.6.3.1 SR5.3 RE(1)：禁止一般目的的个人间通信

控制系统应提供能力，禁止传输和接收一般目的的个人间通信消息。

评估目标：

验证控制系统能禁止一般目的的个人间通信。

评估指南：

验证控制系统边界设备的设置能够基于例外允许原则进行配置，结果记录为“支持”或“不支持”。

6.6.4 SR5.4：应用分离

控制系统应基于实现分区模型的关键程度提供对数据、应用和服务进行分离的能力。

评估目标：

a) 识别数据、应用和服务对于实现分区模型的关键程度；

b) 验证控制系统能提供物理或逻辑措施分离数据、应用和服务。

评估指南：

验证控制系统用户文档包含证据证明，具有应用分离能力来支持分区模型，结果记录为“支持”或“不支持”。

6.6.4.1 SR5.4 RE

无

6.7 FR6：对事件的及时响应

6.7.1 SR6.1：审计日志的可访问性

控制系统应为已授权的人和/或工具提供访问审计日志的能力。

评估目标：

验证发送到外部日志工具或系统的信息不会被篡改以隐藏对安全的违背（例如这种违背可通过比较系统之间的信息来发现）。

评估指南：

验证控制系统提供方法访问审计日志，结果记录为“支持”或“不支持”。

6.7.1.1 SR6.1 RE(1)：对审计日志的编程式访问

控制系统应使用应用编程接口 API 提供对审计记录的访问。

评估目标：

验证控制系统能使用应用编程接口 API 提供对审计记录的编程访问。

评估指南：

通过控制系统文档验证系统支持 API 对审计记录的编程访问，结果记录为“支持”或“不支持”。

6.7.2 SR6.2：持续监视

控制系统应使用普遍接受的安全工业实践和推荐来提供持续监视所有安全机制的性能的能力，以及时检测、特征化、削减和报告对安全的违背。

评估目标：

验证控制系统能提供工具或技术（例如，IDS、IPS、恶意代码保护软件和网络监视软件）来监视控制系统行为。

评估指南：

验证控制系统提供监视控制系统行为以检测攻击的工具，结果记录为“支持”或“不支持”。

6.7.2.1 SR6.2 RE

无

6.8 FR7：资源可用性

6.8.1 SR7.1：拒绝服务的防护

在拒绝服务攻击事件发生期间，控制系统应提供以降级模式运行的能力。控制系统的拒绝服务攻击事件不应对任何功能安全相关系统产生不利影响。

评估目标：

验证控制系统能限制、甚至消除拒绝服务攻击的后果，以防止对任何功能安全相关系统产生不利影响。

评估指南：

验证控制系统和文档提供了限制、某些情况下消除拒绝服务攻击后果的技术；

验证控制系统在拒绝服务攻击事件期间能以降级模式运行。

6.8.1.1 SR7.1 RE(1)：管理通信负荷

控制系统应提供管理通信负荷的能力(例如使用限速)来消减信息泛洪类的拒绝服务攻击事件。

评估目标：

a) 如果主控和功能安全控制共享通用网络，则对主控制器执行健壮性测试并验证不会影响功能安全系统；

b) 验证工业控制系 ICS 设计已考虑了 ICS 用户对其他相连的网络设备和系统的影响。

评估指南：

将流量风暴导向设备来执行通信健壮性测试，验证上行服务在测试结束后恢复正常，下行服务在测试期间不受不利影响。结果记录为“支持”或“不支持”。

6.8.1.2 SR7.1 RE(2)：限制拒绝服务攻击对其他系统和网络的影响

控制系统应提供能力限制所有用户(人、软件进程和设备)引发拒绝服务攻击事件的能力，这些事件可能影响其他控制系统和网络。

评估目标：

a) 验证边界设备可阻止或限制超出声明的通信速率的尝试；

b) 验证如果速率限制器位于单独的联网设备中，则超出声明的通信速率的尝试不影响基本服务。

评估指南：

验证超出声明的通信速率的尝试被边界设备阻止，结果记录为“支持”或“不支持”。

6.8.2 SR7.2：资源管理

控制系统应提供能力安全功能对资源的使用，防止资源耗尽。

评估目标：

验证控制系统可以限制安全功能对资源的使用。

评估指南：

通过用户或设计文档验证控制系统提供了限制安全功能(例如病毒扫描和补丁管理)对资源的使用的能力。结果记录为“支持”或“不支持”。

6.8.2.1 SR7.2 RE

无

6.8.3 SR7.3：控制系统备份

控制系统应在不影响正常工厂运行情况下，支持识别和定位关键文件、并有能力执行用户级和系统级备份(包含系统状态信息)。控制系统应提供以可配置的频率自动实现上述功能的能力。

评估目标：

a) 验证系统备份规程(包括恢复步骤)要求适当的授权；

b) 验证备份数据被充分加密以防止未授权的使用和发挥(例如攻击者应不能利用系统备份获取信息用于之后对安全的破坏)；

c) 验证控制系统备份功能不能干扰正常的控制系统功能(例如备份不能影响运行中的高优先级任务)。

评估指南：

验证用户文档对识别和定位关键文件以及备份规程进行了文档化。验证供货商执行测试，显示备份流程不影响正常的工厂运行。验证用户文档描述了自动化备份功能的流程。结果记录为“支持”或“不支持”。

6.8.3.1 SR7.3 RE(1)：备份验证

控制系统应提供能力验证备份机制的可靠性。

评估目标：

a) 验证备份数据的破坏可被检测；

b) 验证备份数据的破坏可在执行恢复操作之前被检测。

评估指南：

通过改变数据在数据文件中的任意位置来验证用户数据备份的完整性，结果记录为“支持”或“不支持”。

6.8.3.2 SR7.3 RE(2)：备份自动化

控制系统应提供能力按照可配置的频率自动备份。

评估目标：

a) 验证数据备份的频率可配置；

b) 验证数据可以按照设置的频率进行自动备份。

评估指南：

验证用户数据可以按照设置的频率自动备份，结果记录为“支持”或“不支持”。

6.8.4 SR7.4：控制系统恢复和重构

当中断或故障后，控制系统应提供恢复和重构到已知的安全状态的能力。

评估目标：

a) 验证系统备份恢复规程可在 ICS 运行中断后正确恢复 ICS 数据；

b) 验证在恢复操作之前检测备份数据的破坏情况；

c) 验证 ICS 备份规程允许选择恢复点。

评估指南：

验证用户数据存储功能，结果记录为“支持”或“不支持”。

6.8.4.1 SR7.4 RE

无

6.8.5 SR7.5：紧急电源

控制系统应在不影响现有安全状态条件下提供与紧急电源之间进行切换的能力。

评估目标：

a) 验证控制系统具备紧急电源设施，提供与紧急电源设施之间的切换；

b) 验证与紧急电源之间的切换不能影响现有安全状态。

评估指南：

审查供应商文献、声明和文档，记录结果为“支持—由设备供应商在设备和设施中的属性支持”或“不支持”。

6.8.5.1 SR7.5RE

无

6.8.6 SR7.6:网络和安全配置设置

控制系统应提供能力,按照控制系统提供商规定的指南中描述的推荐网络和安全配置进行配置。控制系统应提供与现有部署网络和安全配置设置之间的一个接口。

评估目标:

a) 验证控制系统能为配置设置提供可调节的参数。

b) 验证控制系统能根据安全策略和规程对配置变更进行监视和控制。

评估指南:

审查供应商文档,结果记录为"支持"或"不支持"。

6.8.6.1 SR7.6 RE(1):对当前安全设置的机器可读的报告

控制系统应提供能力生成机器可读格式的报告来列出当前部署的安全设置。

评估目标:

验证当安全配置设置变更时可正确更新安全配置报告。

评估指南:

验证能以机器可读格式生成列有当前部署的安全设置的报告。

6.8.7 SR7.7:最小功能化

控制系统应提供必要的能力,明确禁止和/或限制对非必要的功能、端口、协议和/或服务的使用。

评估目标:

验证控制系统能禁用超出基线配置的功能和服务(基线配置指支持基本功能的必要功能和服务)。

评估指南:

验证控制系统文档提供了如何禁止和/或限制使用非必要的功能、端口、协议和/或服务的指导,结果记录为"支持"或"不支持"。

6.8.7.1 SR7.7 RE

无

6.8.8 SR7.8:控制系统元器件清单

控制系统应提供报告当前已安装的元器件及其关联属性的列表的能力。

评估目标:

a) 验证控制系统提供报告已安装元器件及其关联属性的方法。

b) 验证已安装元器件在系统元器件清单目录中是正确的。

c) 验证当元器件增加、移除或元器件属性变革时,系统元器件清单目录可正确的更新。

评估指南:

验证控制系统提供能力报告当前已安装元器件及其属性的列表,结果记录为"支持"或"不支持"。

6.8.8.1 SR7.8 RE

无

7 评估程序

7.1 评估工作过程

评估的具体对象，因为其规模、性质、复杂程度等相关因素的原因，因此下面只是简要介绍其主要流程，见表 3。

表 3 评估的主要流程

评估准则与步骤	描　述	需　求
确定评估目标	根据满足组织机构业务持续发展在信息安全方面的需要、法律法规的规定等内容，识别本阶段工业控制系统及管理上的不足，以及可能造成的风险大小	分析组织机构资产的状况，商业理念以及计划如何进行风险识别、分类和评估
制定评估计划	双方签订评估协议书和系统评估规模，评估方组建评估项目组，从人员方面做好准备，并编制项目计划书	制定时间表以确定项目如何启动，信息如何收集和分析以及需要哪些的准备内容。项目计划书应包括项目概述，工作依据，技术思路和项目组织机构等
评估的实施	选择风险评估方法	组织机构应选择一个特定的风险评估和分析方式和方法，基于 ICS 资产相关的安全威胁、漏洞和后果对风险进行识别和优先排序
	提供风险评估背景信息	在识别风险之前，组织机构应为风险评估活动的参与者提供适当的信息，包括方法的培训
	执行高层次的风险评估	应进行高层次的系统风险评估来理解 ICS 的可用性、完整性或机密性被破坏带来的财务和 HSE 后果
	识别工业控制系统	组织机构应识别各种 ICS，收集设备数据来描述风险评估的性质并将设备归入逻辑系统中
	开发简单网络架构	组织机构应为每一个逻辑整合系统开发简单的网络架构，显示主要设备，网络类型和设备的通常位置
	系统优先排序	组织机构应为减少每个逻辑控制系统的风险制定标准并分配优先级
	执行详细的漏洞评估	组织机构应对每个逻辑 ICS 执行漏洞评估，范围可以基于高级别风险评估结果和 ICS 遭受这些风险的优先级
	识别详细的风险评估方法论	组织机构的风险评估方法应包含对详细漏洞进行优先排序的方法，详细漏洞通过详细漏洞评估识别
	执行详细的风险评估	组织机构应结合详细漏洞评估中识别出的漏洞进行详细的风险评估
	识别重评估频率和触发准则	组织机构应依据技术、组织机构和工业运行的变化，识别风险和漏洞重评估频率和重评估触发标准
	综合物理、HSE 和网络安全风险评估结果	应综合物理、HSE 和网络安全风险评估结果来理解资产的整体风险
	执行工业控制系统生命周期的风险评估	风险评估应在技术生命周期的所有阶段进行，包括规划、设计、实施、运行维护和废弃(退休)阶段

表 3（续）

评估准则与步骤	描　述	需　求
编写评估报告	文档化风险评估	风险评估方法和风险评估结果应被文档化
	维护漏洞评估记录	对所有包含工业控制系统的资产，应维护最新的漏洞评估记录
	整改的措施和建议	从组织机构管理方面提出信息安全的主要问题以及改进建议；从技术措施方面提出信息安全的主要问题以及改进建议

7.2 评估方法的确定

7.2.1 总则

选择正确的风险评估方法是很主观的，许多方法在市场上能够获得，其中有一些是免费的，其他方法在使用时需要验证。对这些方法进行评估，从而选取最有用的方法，这是一件困难的事情。多数方法有一个共同的前提：风险是事件发生与后果的可能性的组合。对一个特定的网络事故，设置适当的几率值并非易事，不仅是因为历史数据缺乏，还因为一旦一个脆弱性暴露，历史数据并不能预测将来可能发生的事情。因此，许多公司和商业联盟针对自身特点开发出一些方法，以解除对各公司重要问题的威胁和脆弱性。

一些方法充分支持高层次风险评估，一些则充分支持详细风险评估，还有基于场景或基于资产的评估等。这些方法允许输入易损性评估结果，也能够直接为相应的详细易损性评估提供指导。若一种方法能够同时支持高层次和详细风险评估，对一个机构而言是非常有效的。

因此，确定某种评估方法一般要进行以下 4 个步骤：

a） 筛选：评估方法有很多种，目的是确定适用于机构要求的理想方法；

b） 选择：根据机构要求从若干可用的评估方法中选取适用的方法；

c） 验证：本步骤仅仅提供了更加详细的评估数据，该步骤是可选的；

d） 确定：根据评估的对象不同，确定评估方法。

7.2.2 基于场景和基于资产的风险评估

基于具体场景的方法，倾向于利用实际的或者近乎实际的事故，但是，该方法不能深入发现风险对敏感资产的威胁，这些敏感资产之前并没有遭受过风险。

基于资产的方法倾向于利用组织机构对系统、工作方法和能够对经济产生影响的特殊资产的认识，然而，这种方法不能发现一些威胁和漏洞，这些威胁和漏洞能够将设备或者几台设备置于危险环境中。

示例：一机构将设备视作装备、应用软件和数据，认为这个机构整合了基于设备和基于场景的方法。下一步，该组织机构根据设备列举了可能的情景，并给出以下结论，应用情景与装备情景十分相似。

a） 装备情景

1） 情景：未授权用户本地进入 ICS 装备。

若有人靠近该装备，并进行了合法的任务操作，会产生什么结果？

2） 情景：未授权用户远程进入 ICS 装备。

当未授权用户获得远程进入该装备的途径，并对装备进行任意合法操作，会产生什么结果？

b） 数据情形

1） 情景：ICS 数据被窃。

若有人将数据盗窃，将会产生什么结果？

- 这些数据是否具有高智能性能价值？
- 对于竞争者而言，这些数据是否具有商业价值？
- 若数据公开，这些数据是否会对机构造成负面影响？
- 这些数据是否为法律所需？
- 这些数据是否处于诉讼期内？

2) 情景：ICS 数据被损害。

可能带来什么结果？

- 在传输过程中，这些数据被窃听或者被篡改；
- 在发送端，这些数据被窃听；这些数据是否为法律所需？这些数据是否在诉讼期内？

一个队伍可能采取基于场景的风险评估方法，首先是对事故场景的描述，然后决定该场景产生的结果，如示例中所示，或者首先列举不良结果，然后反推出可能的事故场景。也可以结合上述两种方法。

7.2.3 高层次风险评估

高层次风险评估过程，阐明了运用 ICS 产生的个别风险的性质，这需要从根本上选择最有效的方法和辨析配置的成本。它需要风险分析会议聚集利益关系者的意见，也要利用高级商业后果，这些后果在经营理念中已经阐述。风险分析会议中的文件列举了一些情景，这些情景描述了一个特定的威胁是怎样利用特定的漏洞，造成经济损失和负面的商业影响，该会议也设定了后果等级标准和抗风险等级优先顺序。

利益关系者在业务上使用过 ICS，在相关风险关系上负有责任，需要参与风险评估，进而增长他们的知识和经验。

为了成功举行风险分析会议，参与者须理解风险和漏洞的概念，否则，会议很可能只能找出漏洞而不能识别风险。例如，在控制系统 HMI 中，弱认证可能就是一个漏洞，相应的风险可能为，经验不足的雇员就能够在无监管的情况下，对控制系统 HMI 进行操作，设置不安全参数，因为安全控制问题，其后果为生产停止。组织机构机构列举出网络漏洞，然后修复这些漏洞，本身就是一个常见的缺陷。

7.2.4 详细风险评估

详细的风险评估集中在个体 ICS 网络和设备，同时要考虑到具体的财产上的技术漏洞评估和现有政策的有效性。他可能对组织机构一次性 ICS 资产执行详细的风险评估不是很实际。在这种情况下，组织机构将会收集足够的关于 ICS 的信息，允许对系统做优先级排序，决定哪些首先由具体漏洞和风险评估工作做分析。

在详细的风险评估中定义了风险，并进行优先级排序。风险应该是为每个 ICS 做定义。定义风险之后，组织机构可能会选择对所有的系统上的风险进行优先级排序，对每个系统的个体风险进行优先级排序，对研究的 ICS 子集上的风险进行优先级排序，比如说在某一个地方的所有的 ICS。由于优先级最终驱动着执行什么样的行动和投资改善计算机安全，因此优先权的范围要符合预算的范畴，组织机构才能到位做决定做这些投资。例如，如果 ICS 支持的特定的生产线作为一个集团，风险将通过 ICS 一起被优先级排序，保证经理的决定过程。

7.2.5 定性和定量风险评估

定性风险评估依赖有经验的雇员或者专家的意见，提供关于特定风险影响特定资产的可能性和严重性的信息。此外，不同层次的可能性和严重性通过一般级别如高、中、低来识别，而不是特定的可能结果和经济影响。在缺乏可靠信息时，定量风险评估更加实用，这些信息为特定风险对特定资产影响的可能性，或者特定资产损害带来影响的整体评估。

定量风险评估需要大量的数据，这些数据提供风险和脆弱性带来损失的概率，如果这些信息可用，就能够提供比定性风险评估更加精确的风险评估结果。根据最近 ICS 提供的关于系统安全威胁的数据，事故发生以及威胁迅速激化的现象相对较少发生，在这种情形下，定量风险评估在评价这些风险上更有效。

8 工业控制系统生命周期各阶段的风险评估

8.1 生命周期概述

风险评估应贯穿于工业控制系统生命周期的各个阶段中。工业控制系统生命周期各阶段中涉及的风险评估的原则和方法是一致的，但由于各个阶段实施的内容、对象、信息安全需求不同，使得风险评估的对象、目的、要求等各个方面也有所不同。具体而言，在规划设计阶段，通过风险评估以确定系统的安全目标；在建设验收阶段，通过风险评估以确定系统的安全目标达成与否；在运行维护阶段，要不断地实施风险评估以识别系统面临的不断变化的风险和脆弱性，从而确定安全措施的有效性，确保安全目标得以实现。因此，每个阶段风险评估的具体实施应根据该阶段的特点有所侧重地进行。有条件时，应采用风险评估工具开展风险评估活动。

8.2 规划阶段的风险评估

规划阶段风险评估的目的是识别系统的业务战略，以支撑工业控制系统信息安全需求及安全战略等。规划阶段的评估应能够描述信息系统建成后对现有业务模式的作用，包括系统能力（技术）、管理等方面，并根据其作用确定系统建设应达到的安全目标。

本阶段评估中，资产、脆弱性不需要识别；威胁应根据未来系统的应用对象、应用环境、业务状况、操作要求等方面进行分析。评估着重在以下几方面：

a) 是否依据相关规则，建立了与业务战略相一致的工业控制系统信息安全规划，并得到最高管理者的认可；

b) 工业控制系统规划中，是否明确该系统开发的组织机构、业务变更的管理、开发优先级；

c) 工业控制系统规划中，是否明确该系统开发的威胁、环境，并制定总体的信息安全方针；

d) 工业控制系统规划中，是否描述该系统预期使用的信息，包括预期的应用、信息安全资产的重要性、潜在的价值、可能的使用限制、对业务的支持程度等；

e) 工业控制系统规划中，是否描述所有与该系统信息安全相关的运行环境，包括物理和人员的安全配置，以及明确相关的法规、组织机构信息安全策略、专门技术和知识等。

规划阶段的评估结果应体现在工业控制系统规划或项目建议书中。

8.3 设计阶段的风险评估

设计阶段的风险评估需要根据规划阶段所明确的工业控制系统运行环境、系统（资产）重要性，提出信息安全功能需求。本阶段的风险评估结果应对设计方案中所提供的信息安全功能符合性进行判断，作为采购过程风险控制的依据。

本阶段的评估中，应详细评估设计方案中对系统面临威胁的描述，将使用的具体设备、软件等资产及其信息安全功能需求列表。对设计方案的评估着重在以下几个方面：

a) 设计方案是否符合工业控制系统建设规划，并得到最高管理者的认可；

b) 设计方案是否对系统程序建设后面临的威胁进行了分析，重点分析来自关键系统、物理环境、自然威胁以及内、外部分入侵等造成的威胁；

c) 设计方案中的信息安全需求是否符合规划阶段的信息安全目标，并基于威胁的分析，制定信息系统的总体安全策略；

d) 设计方案是否采取了一定的手段来应对系统可能的故障；

e) 设计方案是否对设计原型中的技术实现以及人员、组织机构管理等方面的脆弱性进行评估，包括设计过程中的管理脆弱性和技术平台固有的脆弱性；

f) 设计方案中是否考虑随着其他系统接入而可能产生的风险；

g) 系统性能是否满足用户需求，是否影响到工业控制系统其他的性能，是否在技术上考虑了满足系统性能要求的方法；

h) 应用系统(含数据库)是否根据业务需要进行了安全设计；

i) 设计方案是否根据开发的规模、时间及系统的特点选择开发方法，并根据设计开发计划及用户需求，对系统涉及的软件、硬件与网络进行分析和选型；

j) 设计活动中所采用的安全控制措施、安全技术保障手段对风险的影响。在安全需求变更和设计变更后，也需要重复这些评估。

设计阶段的评估可以以信息安全建设方案评审的方式进行，判定方案所提供的安全功能与工业控制系统安全技术标准的符合性。评估结果应体现在工业控制系统需求分析报告或建设实施方案中。

8.4 实施阶段的风险评估

实施阶段风险评估的目的是根据工业控制系统信息安全需求和运行环境对系统开发、实施过程进行风险识别，并对系统建成后的信息安全功能进行验证。根据设计阶段分析的威胁和制定的安全措施，在实施及验收时进行质量控制。

基于设计阶段的系统(资产)、安全措施，实施阶段应对规划阶段的安全威胁进行进一步细分，同时评估安全措施的实现程度，从而确定安全措施能否抵御现有威胁、脆弱性的影响。实施阶段风险评估主要对系统的开发与技术/产品获取、系统交付实施两个过程进行评估。

开发与技术/产品获取过程的评估要点包括：

a) 法律、政策、适用标准和指导方针：直接或间接影响工业控制系统信息安全需求的特定法律；影响工业控制系统信息安全需求的政府政策、国际或国家标准；

b) 工业控制系统的功能需要：信息安全需求是否有效地支持系统的功能；

c) 成本效益风险：是否根据工业控制系统的信息安全分析结果，确定在符合相关法律、政策、标准和功能需要的前提下选择最合适的安全措施；

d) 评估保护级别：是否明确系统建设后应进行怎样的测试和检查，从而确定是否满足项目建设、实施规范的要求。

系统实施过程的评估要点包括：

a) 根据实际建设的系统，详细分析系统(资产)、面临的威胁和脆弱性；

b) 根据系统建设目标和信息安全需求，对系统的信息安全进行验收测试；评价安全措施能否抵御安全威胁；

c) 评估是否建立了与整体安全策略一致的组织机构管理制度；

d) 对系统实现的风险控制效果与预期设计的符合性进行判断，如存在较大的不符合，应重新进行工业控制系统信息安全策略的设计与调整。

本阶段风险评估可以采取对照实施方案和标准要求的方式，对实际建设结果进行测试、分析。

8.5 运行维护阶段的风险评估

运行维护阶段风险评估的目的是了解和控制运行过程中的安全风险，是一种较为全面的风险评估。评估内容包括对真实运行的工业控制系统、系统(资产)、威胁、脆弱性等各个方面。

a) 系统(资产)评估：在真实环境下较为细致的评估。包括实施阶段采购的软硬件资产、系统运行过程中生成的信息安全相关的资产、相关的人员与服务等，本阶段系统(资产)识别是前期的补

充与增加；

b) 威胁评估：应全面分析威胁的可能性和影响程度。对非故意威胁导致信息安全事件的评估可以参照信息安全事件发生频率；对故意威胁导致安全事件的评估主要就威胁的各个影响因素做出专业判断；

c) 脆弱性评估：是全面的脆弱性评估。包括运行环境中物理、网络、系统、应用、信息安全保障设备、管理等各个方面的脆弱性。技术脆弱性评估可以采取核查、扫描、案例取证、渗透性测试的方式实施；信息安全保障设备的脆弱性评估，应考虑安全功能的实现情况和安全保障设备本身的脆弱性；管理脆弱性评估可以采取文档、记录核查等方式进行验证；

d) 风险计算：根据本标准的相关方法，对重要系统（资产）的风险进行定性或定量的风险分析，描述不同系统（资产）的风险高低状况。

运行维护阶段的风险评估应定期执行，当组织机构的业务流程、系统状况发生重大变更时，也应进行风险评估。重大变更包括以下情况（但不限于）：

a) 增加新的应用或应用发生较大变更；

b) 网络结构和连接状况发生较大变更；

c) 技术平台大规模的更新；

d) 系统扩容或改造；

e) 发生重大信息安全事件后，或基于某些运行记录怀疑将发生重大安全事件；

f) 组织机构结构发生重大变动时对系统产生了影响。

8.6 废弃阶段的风险评估

当工业控制系统信息安全不能满足现有要求时，信息安全系统进入废弃阶段。根据废弃的程度，又分为部分废弃和全部废弃两种。

本阶段的风险评估着重在以下几个方面：

a) 确保硬件和软件等资产及残留信息得到了适当的处置，并确保系统组件被合理地丢弃或更换；

b) 如果被废弃的系统是某个系统的一部分，或与其他系统存在物理或逻辑上的连接，还应考虑系统废弃后，与其他系统的连接是否被关闭；

c) 如果在系统变更中废弃，除对废弃部分外，还应对变更的部分进行评估，以确定是否会增加风险或引入新的风险；

d) 是否建立了流程，确保更新过程在一个安全、系统化的状态下完成。

本阶段应重点放在废弃资产对组织机构的影响方面进行分析，并根据不同的影响制定不同的处理方式。对由于系统废弃可能带来的新的威胁进行分析，并改进新系统或管理模式。对废弃资产的处理过程应在有效的监督之下实施，同时对废弃系统的执行人员进行安全教育。

工业控制系统的维护人员和管理人员均应参加此阶段的评估。

9 评估报告的格式要求

评估报告至少应包含下列内容：

a) 标题；

b) 负责评估或评定的机构和/或人员的资质；

c) 如果是为了系统的特定应用而进行评估，则过程的类型，输入输出的类型和数量要求的扫描速率，系统的使命任务和功能等应用特征都应包括在内；

d) 对被评估系统的说明和鉴定包括一张列出所使用的硬件包括型号和软件包括版本的表格；

e) 评估的目的；

f) 评估特征点及结论汇总表；

g) 程序方法、规范和试验项目的报表最好用矩阵表汇总，并用附件补充。以及特定选择矩阵表所列评估要素的汇总表，报告中同时应记录某些方面为什么不评估的原因；

h) 任何与评估计划的不一致之处增加或减少评估项目均应加以记录并说明原因；

i) 测量检查和分析得出的结果用合适的表格、图片、图纸或照片说明；

j) 观察到的故障描述；

k) 关于系统是否符合评估要求的说明；

l) 评估报告应附封面，封面注明报告标题统一编号，评估机构和发布日期，以便于不同系统评估的比较；

m) 评估报告发布后，若需改动或增补，只能采用补充报告的形式，报告上应标明原报告的标题和编号，补充报告的编写要求与原报告相同。

附 录 A
（规范性附录）
管理评估列表

管理评估的内容见表 A.1。

表 A.1 信息安全管理评估列表

	ML 1	ML 2	ML 3
5.1 安全方针			
5.1.1 信息安全方针			
要求：依据业务要求和相关法律法规提供管理指导并支持信息安全			
5.1.1.1 信息安全方针文件	✓	✓	✓
5.1.1.2 信息安全方针的评审	✓	✓	✓
5.2 信息安全组织机构			
5.2.1 内部组织机构			
要求：管理组织机构范围内信息安全			
5.2.1.1 信息安全的管理承诺	✓	✓	✓
5.2.1.2 信息安全协调	✓	✓	✓
5.2.1.3 信息安全职责的分配	✓	✓	✓
5.2.1.4 信息处理设施的授权过程	✓	✓	✓
5.2.1.5 保密性协议	✓	✓	✓
5.2.1.6 与政府部门的联系		✓	✓
5.2.1.7 信息安全的独立评审			✓
5.2.2 外部方			
要求：保持组织机构的被外部方访问、处理、管理或外部进行通信和信息处理设施的安全			
5.2.2.1 与外部方相关风险的识别	✓	✓	✓
5.2.2.2 处理与顾客有关的安全问题	✓	✓	✓
5.2.2.3 处理第三方协议中的安全问题			✓
5.3 资产管理			
5.3.1 对资产负责			
要求：实现和保持对组织机构资产的适当保护			
5.3.1.1 资产清单	✓	✓	✓
5.3.1.2 资产责任人	✓	✓	✓
5.3.1.3 资产的可接受使用			✓
5.3.2 信息分类			

表 A.1（续）

	ML 1	ML 2	ML 3
要求：确保信息受到适当级别的保护			
5.3.2.1 分类指南			✓
5.3.2.2 信息的标记和处理	✓	✓	✓
5.4 人力资源安全			
5.4.1 任用之前			
要求：确保雇员、承包方人员和第三方人员理解其职责，考虑对其承担的角色是适合的，以降低设施被窃取，欺诈和误用的风险			
5.4.1.1 角色和职责	✓	✓	✓
5.4.1.2 审查	✓	✓	✓
5.4.1.3 任用条款和条件			✓
5.4.2 任用中			
要求：确保所有的雇员、承包方人员和第三方人员知悉信息安全威胁和利害关系、他们的职责和义务，并准备好在其正常工作过程中支持组织机构的安全方针，以减少人为出错的风险			
5.4.2.1 管理职责	✓	✓	✓
5.4.2.2 信息安全意识、教育和培训	✓	✓	✓
5.4.2.3 纪律处理过程	✓	✓	✓
5.4.3 任用的终止或变更	✓	✓	✓
要求：确保所有的雇员、承包方人员和第三方人员以一个规范的方式退出一个组织机构或改变其任用关系			
5.4.3.1 终止职责	✓	✓	✓
5.4.3.2 资产的归还	✓	✓	✓
5.4.3.3 撤销访问权	✓	✓	✓
5.5 物理和环境安全			
5.5.1 安全区域			
要求：防止对组织机构场所和信息的未授权物理访问、损坏和干扰			
5.5.1.1 物理安全周边		✓	✓
5.5.1.2 物理入口控制	✓	✓	✓
5.5.1.3 办公室、房间和设施的安全保护	✓	✓	✓
5.5.1.4 外部和环境的安全防护		✓	✓
5.5.1.5 在安全区域工作	✓	✓	✓
5.5.1.6 公共访问、交换区安全	✓	✓	✓
5.5.2 设备安全			
要求：防止资产的丢失、损坏、失窃或危及资产安全以及组织机构活动的中断			

表 A.1（续）

	ML 1	ML 2	ML 3
5.5.2.1 设备安置和保护	√	√	√
5.5.2.2 支持性设施	√	√	√
5.5.2.3 布缆安全	√	√	√
5.5.2.4 设备维护	√	√	√
5.5.2.5 组织机构场所外的设备安全		√	√
5.5.2.6 设备的安全处置或再利用		√	√
5.5.2.7 资产的移动			√
5.6 通信和操作管理			
5.6.1 操作规程和职责			
要求：确保正确、安全的操作信息处理设施			
5.6.1.1 文件化操作规程	√	√	√
5.6.1.2 变更管理	√	√	√
5.6.1.3 责任划分		√	√
5.6.1.4 开发、测试和运行设施分离		√	√
5.6.2 第三方服务交付管理			
要求：实施和保持符合第三方服务交付协议的信息安全和服务交付的适当水准			
5.6.2.1 服务交付	√	√	√
5.6.2.2 第三方服务的监视和评审		√	√
5.6.2.3 第三方服务的变更管理			√
5.6.3 系统规划和验收			
要求：将系统失效的风险降至最小			
5.6.3.1 容量管理		√	√
5.6.3.2 系统验收	√	√	√
5.6.4 防范恶意和移动代码			
要求：保护软件和信息的完整性			
5.6.4.1 控制恶意代码	√	√	√
5.6.4.2 控制移动代码	√	√	√
5.6.5 备份			
要求：保持信息和信息处理设施的完整性及可用性			
5.6.5.1 信息备份	√	√	√
5.6.6 网络安全管理			
要求：确保网络中信息的安全性并保护支持性的基础设施			
5.6.6.1 网络控制	√	√	√

表 A.1（续）

	ML 1	ML 2	ML 3
5.6.6.2 网络服务安全	✓	✓	✓
5.6.7 介质处置			
要求：防止资产遭受未授权泄露、修改、移动或销毁以及业务活动的中断			
5.6.7.1 可移动介质的管理	✓	✓	✓
5.6.7.2 介质的处置	✓	✓	✓
5.6.7.3 信息处理规程		✓	✓
5.6.7.4 系统文件安全			✓
5.6.8 信息的交换			
要求：保持组织机构内以及与组织机构外信息和软件交换的安全			
5.6.8.1 信息交换策略和规程	✓	✓	✓
5.6.8.2 交换协议	✓	✓	✓
5.6.8.3 运输中的物理介质		✓	✓
5.6.8.4 电子消息发送	✓	✓	✓
5.6.8.5 业务信息系统			✓
5.6.9 监视			
要求：检测未经授权的信息处理活动			
5.6.9.1 审计记录	✓	✓	✓
5.6.9.2 监视系统的使用	✓	✓	✓
5.6.9.3 日志信息的保护	✓	✓	✓
5.6.9.4 管理员和操作日志	✓	✓	✓
5.6.9.5 故障日志	✓	✓	✓
5.6.9.6 时钟同步	✓	✓	✓
5.7 访问控制			
5.7.1 访问控制的业务要求			
要求：控制对信息的访问			
5.7.1.1 访问控制策略	✓	✓	✓
5.7.2 用户访问管理			
要求：确保授权用户访问信息系统，并防止未授权的访问			
5.7.2.1 用户注册	✓	✓	✓
5.7.2.2 特殊权限管理		✓	✓
5.7.2.3 用户口令管理	✓	✓	✓
5.7.2.4 用户访问权的复查			✓
5.7.3 用户职责			

表 A.1（续）

	ML.1	ML.2	ML.3
要求：防止未授权用户对信息和信息处理设施的访问、损害和窃取			
5.7.3.1 口令使用	✓	✓	✓
5.7.3.2 无人职守的用户设备	✓	✓	✓
5.7.3.3 清空桌面和屏幕策略		✓	✓
5.7.4 网络访问控制			
要求：防止对网络服务的未授权访问			
5.7.4.1 网络服务的策略	✓	✓	✓
5.7.4.2 外部连接的用户鉴别	✓	✓	✓
5.7.4.3 网络上的设备标识		✓	✓
5.7.4.4 远程诊断和配置端口的保护	✓	✓	✓
5.7.4.5 网络隔离	✓	✓	✓
5.7.4.6 网络连接控制	✓	✓	✓
5.7.4.7 网络路由控制		✓	✓
5.7.5 操作系统访问控制			
要求：防止对操作系统的未授权访问			
5.7.5.1 安全登录规程	✓	✓	✓
5.7.5.2 用户标识和鉴别	✓	✓	✓
5.7.5.3 口令管理系统	✓	✓	✓
5.7.5.4 系统实用工具的使用		✓	✓
5.7.5.5 会话超时			✓
5.7.5.6 联机时间的限定			✓
5.7.6 应用和信息访问控制			
要求：防止对应用系统中信息的未授权访问			
5.7.6.1 信息访问控制	✓	✓	✓
5.7.6.2 敏感系统隔离	✓	✓	✓
5.7.7 移动计算和远程工作			
要求：确保使用移动计算机和远程工作设施时的信息安全			
5.7.7.1 移动计算和通信	✓	✓	✓
5.7.7.2 远程工作	✓	✓	✓
5.8 信息系统获取、开发和维护			
5.8.1 信息系统的安全要求			
要求：确保安全是信息系统的一个有机组成部分			
5.8.1.1 安全要求分析和说明	✓	✓	✓

表 A.1（续）

	ML 1	ML 2	ML 3
5.8.2 应用中的正确处理			
要求：防止应用系统中的信息的差错、遗失、未授权的修改或误用			
5.8.2.1 输入数据确认	✓	✓	✓
5.8.2.2 内部处理的控制		✓	✓
5.8.2.3 消息完整性		✓	✓
5.8.2.4 输出数据确认			✓
5.8.3 密码控制			
要求：通过密码方法保护信息的保密性、真实性或完整性			
5.8.3.1 使用密码控制的策略	✓	✓	✓
5.8.3.2 密钥管理	✓	✓	✓
5.8.4 系统文件的安全			
要求：确保系统文件的安全			
5.8.4.1 运行软件的控制	✓	✓	✓
5.8.4.2 系统测试数据的保护	✓	✓	✓
5.8.4.3 对程序源代码的访问控制	✓	✓	✓
5.8.5 开发和支持过程中的安全			
要求：维护应用系统软件和信息的安全			
5.8.5.1 变更控制规程	✓	✓	✓
5.8.5.2 操作系统变更后应用的技术评审	✓	✓	✓
5.8.5.3 软件包变更的限制	✓	✓	✓
5.8.5.4 信息泄露	✓	✓	✓
5.8.5.5 外包软件开发		✓	✓
5.8.6 技术脆弱性管理			
要求：降低利用公布的技术脆弱性导致的风险			
5.8.6.1 技术脆弱性的控制	✓	✓	✓
5.9 信息安全事件管理			
5.9.1 报告信息安全事态和弱点			
要求：确保与信息系统有关的信息安全事态和弱点能够以某种方式传达，以便及时采取纠正措施			
5.9.1.1 报告信息安全事态	✓	✓	✓
5.9.1.2 报告安全弱点	✓	✓	✓
5.9.2 信息安全时间和改进的管理			
要求：确保采用一致和有效的方法对信息安全事件进行管理			
5.9.2.1 职责和规程	✓	✓	✓

表 A.1（续）

	ML 1	ML 2	ML 3
5.9.2.2 对信息安全事件的总结	✓	✓	✓
5.9.2.3 证据的收集		✓	✓
5.10 业务连续性管理			
5.10.1 业务连续性管理的信息安全方面			
要求：防止业务活动中断，保护关键业务过程免受信息系统重大失误或灾难的影响，并确保他们及时恢复			
5.10.1.1 在业务连续性管理过程中包含信息安全	✓	✓	✓
5.10.1.2 业务连续性和风险评估	✓	✓	✓
5.10.1.3 制定和实施包含信息安全的连续性计划	✓	✓	✓
5.10.1.4 业务连续性计划框架		✓	✓
5.10.1.5 测试、维护和再评估业务连续性计划			✓
5.11 符合性			
5.11.1 符合法律要求			
要求：避免违反任何法律、法令、法规或合同义务以及任何安全要求			
5.11.1.1 可用法律的识别	✓	✓	✓
5.11.1.2 知识产权	✓	✓	✓
5.11.1.3 保护组织机构的记录	✓	✓	✓
5.11.1.4 数据保护和个人信息的隐私	✓	✓	✓
5.11.1.5 防止滥用信息处理设施	✓	✓	✓
5.11.1.6 密码控制措施的规则		✓	✓
5.11.2 符合安全策略和标准以及技术符合性			
要求：确保系统符合组织机构的安全策略及标准			
5.11.2.1 符合安全策略和标准	✓	✓	✓
5.11.2.2 技术符合性核查	✓	✓	✓
5.11.3 信息系统审计考虑			
要求：将信息系统审计过程的有效性最大化，干扰最小化			
5.11.3.1 信息系统审计控制措施	✓	✓	✓
5.11.3.2 信息系统审计工具的保护	✓	✓	✓

附 录 B
（规范性附录）
系统能力（技术）评估列表

系统要求和增强要求见表 B.1。

表 B.1 系统要求和增强要求与安全等级的映射

SR 和 RE	CL1	CL2	CL3	CL4
FR 1 标识和认证控制				
SR 1.1 用户（人）的标识和认证	√	√	√	√
RE(1)唯一标识和认证		√	√	√
RE(2)非可信网络的多因子认证			√	√
RE(3)对所有网络的多因子认证				√
SR 1.2 软件进程和设备的标识和认证		√	√	√
RE(1)唯一标识和认证			√	√
SR 1.3 账号管理	√	√	√	√
RE(1)统一的账号管理			√	√
SR 1.4 标识符管理	√	√	√	√
SR 1.5 认证码管理	√	√	√	√
RE(1)软件进程标识凭证的硬件安全			√	√
SR 1.6 无线访问管理	√	√	√	√
RE (1) 唯一标识和认证		√	√	√
SR 1.7 口令认证的加强	√	√	√	√
RE (1) 对用户（人）的口令生成和口令有效期限制			√	√
RE (2) 对所有用户的口令有效期限制				√
SR 1.8 公钥基础设施证书		√	√	√
SR 1.9 公钥认证加强		√	√	√
RE (1)公钥认证的硬件安全			√	√
SR 1.10 认证反馈	√	√	√	√
SR 1.11 失败的登陆尝试	√	√	√	√
SR 1.12 系统使用通知	√	√	√	√
SR 1.13 经由非可信网络的访问	√	√	√	√
RE (1) 明确地对访问请求的批准		√	√	√
FR 2 使用控制				
SR 2.1 授权的执行	√	√	√	√
RE (1) 对所有用户执行授权		√	√	√
RE (2) 许可映射到角色		√	√	√

表 B.1（续）

SR 和 RE	CL1	CL2	CL3	CL4
RE (3) 主管越权			√	√
RE (4) 双授权				√
SR 2.2 无线使用控制	√	√	√	√
RE (1) 对未授权的无线设备进行识别和报告			√	√
SR 2.3 对便携和移动设备的使用控制	√	√	√	√
RE (1) 便携和移动设备的安全状态的实施			√	√
SR 2.4 移动代码	√	√	√	√
RE(1)移动代码的完整性检查			√	√
SR 2.5 会话锁	√	√	√	√
SR 2.6 远程会话终止		√	√	√
SR 2.7 并发会话控制			√	√
SR 2.8 可审计的事件	√	√	√	√
RE (1) 中央管理的、系统范围的审计跟踪			√	√
SR 2.9 审计存储容量	√	√	√	√
RE (1) 达到审计记录存储容量上限时发出警告			√	√
SR 2.10 审计处理失败的响应	√	√	√	√
SR 2.11 时间戳		√	√	√
RE (1) 内部时间同步			√	√
RE (2) 时间源的完整性保护				√
SR 2.12 不可否认性			√	√
RE (1)所有用户的不可否认性				√
FR 3 系统完整性				
SR 3.1 通信完整性	√	√	√	√
RE (1) 基于密码技术的完整性保护			√	√
SR 3.2 恶意代码保护	√	√	√	√
RE (1) 在入口和出口点防护恶意代码		√	√	√
RE (2) 恶意代码防护的中央管理和报告			√	√
SR 3.3 安全功能验证	√	√	√	√
RE(1)安全功能验证的自动化机制			√	√
RE(2)正常运行中的安全功能验证				√
SR 3.4 软件和信息完整性		√	√	√
RE (1) 对破坏完整性进行自动通知			√	√
SR 3.5 输入验证	√	√	√	√
SR 3.6 确定性的输出	√	√	√	√

表 B.1（续）

SR 和 RE	CL1	CL2	CL3	CL4
SR 3.7 错误处理		√	√	√
SR 3.8 会话完整性		√	√	√
RE (1) 会话终止后会话 ID 的失效			√	√
RE (2) 唯一会话 ID 的产生和承认			√	√
RE (3) 会话 ID 的随机性				√
SR 3.9 审计信息的保护		√	√	√
RE (1) 一次性写入介质上的审计记录				√
FR 4 数据保密性				
SR 4.1 信息机密性	√	√	√	√
RE (1) 静止和经由不可信网络传输的数据的机密性保护		√	√	√
RE (2) 区域边界的机密性保护				√
SR 4.2 信息存留		√	√	√
RE (1) 共享内存资源的清除			√	√
SR 4.3 密码的使用	√	√	√	√
FR 5 限制的数据流				
SR 5.1 网络分区	√	√	√	√
RE (1) 物理网络分区		√	√	√
RE (2) 与非控制系统网络的独立性			√	√
RE (3) 关键网络的逻辑和物理隔离				√
SR 5.2 区域边界防护	√	√	√	√
RE (1) 默认拒绝，例外允许		√	√	√
RE (2) 孤岛模型			√	√
RE (3) 故障关闭			√	√
SR 5.3 一般目的的个人通信的限制	√	√	√	√
RE(1)禁止所有的一般目的的个人通信			√	√
SR 5.4 应用分离	√	√	√	√
FR 6 对事件的及时响应				
SR 6.1 审计日志的可访问性	√	√	√	√
RE (1) 对审计日志的编程式访问			√	√
SR 6.2 持续监视		√	√	√
FR 7 资源可用性				
SR 7.1 拒绝服务的防护	√	√	√	√
RE (1) 管理通信负荷		√	√	√
RE (2) 限制拒绝服务攻击对其他系统和网络的影响			√	√

表 B.1（续）

SR 和 RE	CL1	CL2	CL3	CL4
SR 7.2 资源管理	√	√	√	√
SR 7.3 控制系统备份	√	√	√	√
RE（1）备份验证		√	√	√
RE(2)备份自动化			√	√
SR 7.4 控制系统恢复和重构	√	√	√	√
SR 7.5 紧急电源	√	√	√	√
SR 7.6 网络和安全配置设置	√	√	√	√
RE（1）对当前安全设置的机器可读的报告			√	√
SR 7.7 最小功能化	√	√	√	√
SR 7.8 控制系统元器件清单		√	√	√

附 录 C
（资料性附录）
风险评估工具和工业控制系统常见的测试内容

C.1 风险评估工具概述

风险评估工具是风险评估的辅助手段，是保证风险评估结果可信度的一个重要因素。风险评估工具的使用不但在一定程度上解决了手动评估的局限性，最主要的是他能够将专家知识进行集中，使专家的经验知识被广泛的应用。

根据在风险评估过程中的主要任务和作用原理的不同，风险评估的工具可以分成风险评估与管理工具、系统基础平台风险评估工具、风险评估辅助工具三类。虽然在评估中可以使用现场测试工具，但是现场测试并不能等同于风险评估，而且要对技术检测活动的安全风险，特别是现场检查中使用的自动化检测工具的安全风险进行评估，防止引入新的风险，并要求相关人员严格遵守操作规程。并对重要数据和配置进行备份，尽量避开业务高峰期进行工具测试。对工业控制系统的技术检测要慎重实施。

C.1.1 风险评估与管理工具

风险评估与管理工具大部分是基于某种标准方法或某组织机构自行开发的评估方法，可以有效地通过输入数据来分析风险，给出对风险的评价并推荐控制风险的安全措施。

风险评估与管理工具通常建立在一定的模型或算法之上，风险由重要资产（如 SIS 系统、SLC 系统等）、所面临的威胁以及威胁所利用的脆弱性三者来确定；也有的通过建立专家系统，利用专家经验进行分析，给出分析结论。这种评估工具需要不断进行知识库的扩充。

此类工具实现了对风险评估全过程的实施和管理，包括：被评估信息系统基本信息获取、重要系统获取、脆弱性识别与管理、威胁识别、评估过程与评估结果管理等功能。评估的方式可以通过问卷的方式，也可以通过结构化的推理过程，建立模型，输入相关信息，得出评估结论。通常这类工具在对风险进行评估后都会有针对性地提出风险控制措施。

根据实现方法不同，风险评估与管理工具可以分为三类：

a） 基于信息安全标准的风险评估与管理工具

目前，国际上存在多种不同的风险分析标准或指南，不同的风险分析方法侧重点不同，例如 ISA Secure、NIST SP800-30、BS7799、ISO/IEC 13335 等。以这些标准或指南的内容为基础，分别开发相应的评估工具，完成遵循标准或指南的风险评估过程。

b） 基于知识的风险评估与管理工具

基于知识的风险评估与管理工具并不仅仅限于某个单一的标准或指南，而是将各种风险分析方法进行综合，并结合实践经验，形成风险评估知识库，以此为基础完成综合评估。它还涉及来自类似组织机构（包括规模、商务目标和市场等）的最佳实践，主要通过多种途径采集相关的信息，识别组织机构的风险和当前的安全措施；与特定的标准或最佳实践进行比较，从中找出不符合的地方；按照标准或最佳实践的推荐选择安全措施以控制风险。

c） 基于模型的风险评估与管理工具

基于标准或基于知识的风险评估与管理工具，都使用了定性分析方法或定量分析方法，或者定性与定量相结合。定性分析方法是目前广泛采用的方法，需要凭借评估者的知识、经验和直觉，或者业界的标准和实践，为风险的各个要素定级。定性分析法操作相对容易，但也可能因为评估者经验和直觉的偏差而使分析结果失准。定量分析则对构成风险的各个要素和潜在损失水平赋值，通过对度量风险的所

有要素进行赋值，建立综合评价的数学模型，从而完成风险的量化计算。定量分析方法准确，但前期建立系统风险模型较困难。定性与定量结合分析方法是将风险要素的赋值和计算，根据需要分别采取定性和定量方法完成。这类工具是在对系统各组成部分、安全要素充分研究的基础上，对典型系统、威胁、脆弱性建立量化或半量化的模型，根据采集信息的输入，得到评价的结果。

C.1.2 系统基础平台风险评估工具

系统风险平台风险评估工具分析包括脆弱性扫描工具和渗透性测试工具。脆弱性扫描工具又称为安全扫描器、漏洞扫描仪等，主要用于识别网络、操作系统、数据库系统的脆弱性。通常情况下，这些工具能够发现软件和硬件中已知的脆弱性，以决定系统是否易受已知攻击的影响。

脆弱性扫描工具是目前应用最广泛的风险评估工具，主要完成操作系统、数据库系统、网络协议、网络服务等的安全脆弱性检测功能，目前常见的脆弱性扫描工具有以下几种类型：

a) 基于网络的扫描器：在网络中运行，能够检测如防火墙错误配置或连接到网络上的易受攻击的网络服务器的关键漏洞。

b) 基于主机的扫描器：发现主机的操作系统、特殊服务和配置的细节，发现潜在的用户行为风险，如密码强度不够，也可实施对文件系统的检查。

c) 分布式网络扫描器：由远程扫描代理、对这些代理的即播即用更新机制、中心管理点三部分构成，用于企业级网络的脆弱性评估，分布和位于不同位置、城市甚至不同的国家。

d) 数据库脆弱性扫描器：对数据库的授权、认证和完整性进行详细分析，也可以识别数据库系统中潜在的脆弱性。

渗透性测试工具是根据脆弱性扫描工具扫描的结果进行模拟攻击测试，判断被非法访问者利用的可能性。这类工具通常包括黑客工具、脚本文件。渗透性测试的目的是检测已发现的脆弱性是否真正会给系统或网络带来影响。

工业控制系统评估中，如果进行任何渗透测试，要慎重使用攻击性测试手段，并且测试系统的性能需要注明额外的渗透测试结果。最有可能有一些系统或组件由于渗透测试而性能退化。这些性能衰减应该被注明供今后使用。通常渗透性工具与脆弱性扫描工具一起使用。

C.1.3 风险评估辅助工具

科学的风险评估需要大量的实践和经验数据的支持，这些数据的积累是风险评估科学性的基础。风险评估过程中，可以利用一些辅助性的工具和方法来采集数据，帮助完成现状分析和趋势判断，如：

a) 检查列表：检查列表是基于特定标准或基线建立的，对特定系统进行审查的项目条款。通过检查列表，操作者可以快速定位系统目前的安全状况与基线要求之间的差距。

b) 入侵检测系统：入侵检测系统通过部署检测引擎，收集、处理整个网络中的通信信息，以获取可能对网络工主机造成危害的入侵攻击事件；帮助检测各种攻击试探和误操作；同时也可以作为一个警报器，提醒管理员发生的安全状况。

c) 安全审计工具：用于记录网络行为，分析系统或网络安全现状；其审计记录可以作为风险评估中的安全现状数据，并可用于判断被评估对象威胁信息的来源。

d) 病毒和恶意代码检测工具：该工具如同一个主动的侦查代理者，对上述迹象的非正常的活动目录进行侦查。病毒和恶意代码检测工具能够监查并运行在有恶意代码活动的主机上，或是网络服务器的层面上，如同一个邮件服务器。未来方向包括启发式、统计以及神经网络技术的病毒和恶意代码检测系统。

e) 资产信息收集系统：通过提供调查表形式，完成被评估信息系统数据、管理、人员等资产信息的收集功能，了解到组织机构的主要业务、重要资产、威胁、管理上的缺陷、采用的控制措施和安全策略的执行情况。此类系统主要采取电子调查表形式，需要被评估系统管理人员参与填写，

并自动完成资产信息获取。

f) 拓扑发现工具：通过接入点接入被评估网络，完成被评估网络中的资产发现功能，并提供网络资产的相关信息，包括操作系统版本、型号等。拓扑发现工具主要是自动完成网络硬件设备的识别、发现功能。

C.2 工业控制系统信息安全常见的测试内容

C.2.1 离线的安全测试

系统的安全测试重要，设备的安全测试也很重要，从而确保操作的完整性和健壮性能够实现。

如果 ICS 是一个新系统，应该在系统脱机环境下进行安全测试。这应该是在供应商的位置或最终场地离线分期步骤进行的工厂接受的测试。位置并不重要，重要的是执行的安全测试步骤。虽然这对安全测试的所有设备和应用于最后设备状态的对策很有意义，但是这也许支付不起且不适用。所以测试的设计应该更关注 ICS 设备的能力和不局限于安装位置的对策。安全测试应该不仅仅包括评估受试者遇到了典型的安全威胁的抵抗能力，也应该包括进行的系统安全支持的测试。这些包括但不限于：

a) 测试操作系统修补补丁和升级；

b) 测试 ICS 供应商的补丁和升级过程；

c) 测试离线系统的开发环境；

d) 测试恶意软件的部署和更新恶意软件的签名。

C.2.2 现场测试

如果这是新安装的 ICS，宜在 ICS 上线之前进行这些测试。如果这个活动是为了改造和替换现有的 ICS 设备或者实现一些新的 ICS 对策，也许不能获得机会去实现所有的离线安全测试。相反，这一挑战是实现新的设备或对策和现场测试，ICS 的基本操作功能在安全措施的冲击下不可能不受影响。

需要牢记的是系统性能测试应包括系统对正常和异常的工业操作类型事件和安全事故类型事件的反应。结合这些才能全面衡量系统的鲁棒性和完整性。由于每个工业操作稍有不同，宜确定一个测试流程手册。同时将需要大量的设计工作去决定最好的方法来保证测试，从而使得安全功能满足目标安全等级。

C.2.3 工业控制系统的测试类型

系统安全测试就像其他领域的测试一样包括验证测试和确认测试。根据能力成熟度，核查确认工作恰当地反应了符合要求。换句话说，验证保证“你证明他是正确的”。概括地说，验证决定了是否满足规范，而确认决定是否满足要求。

具体的测试将基于要求测试的等级、测试系统的组件以及系统或组件的测试要求类型。网络安全测试的表现分为三个典型的阶段：组件测试、集成测试以及系统测试。验证测试应在组件和集成阶段实现，确认测试都应该在系统测试阶段实现。

C.2.3.1 组件测试

组件测试应该由供应商和系统拥有者来完成。组件可以是软件、硬件或任何组合情况。组件需要被测试以验证他满足特定的操作和安全要求。组件测试是正常的工作台测试，有必要保证当组件集成到系统中，有信心每个组件都能按预期运行。

C.2.3.2 集成测试

集成测试应该由集成商和系统拥有者来验证。该测试包括可能来自不同供应商的各种组件的操作

和安全测试，这些组件是和工作台或辅助测试平台相连接，来检查所有的组件在投入 ICS 环境之前是否能一起正常的工作。集成测试包括使用额外的测试工具，如网络管理工具，但在组件测试阶段这些是不必要的。

测试平台很少对存在于操作设备中的控制系统有准确的配置。通常开发或试验阶段一个简化的或复制的系统在组件和集成测试阶段是最合适的。集成测试应该围绕测试平台进行设计。应注意将集成测试建立和 ICS 环境区别开来，需要的任何额外的工具否则组件就不能在集成测试和系统测试完全被测试。因为这个原因，也许很有用，尤其在集成测试阶段，在操作系统附近放置简化的或复制的系统。

在某些情况下，可能会执行非生产集成测试去检查安全对策是如何一起工作的，如何操作界面接口的。例如，安全对策通过实验室/试验平台网络连接离散的软件/硬件。其他情况下，这种集成也许不可能。该集成测试计划应该利用测试平台的方案，可以配置操作系统中可能出现的测试组件的运行条件。

C.2.3.3 系统测试

系统测试应该由拥有者验证。验证的目的是证明合适的技术、流程、细致的管理、运营和技术对策使得 ICS 能正确的完成，这在应用中是有效的，并确保新的安全对策，如采购和安装，满足要求。

系统测试可能包括系统的渗透测试来保证安全组件的能力，从而保护系统受到各种威胁满足每个区域的安全等级。渗透测试时一个已知的人试图在系统中渗透安全防御，寻找漏洞，被利用来获得访问或控制系统的权利。很多公司专注于渗透测试传统的 IT 系统，也许更难找到一组了解 ICS 特殊需求。

各种各样的测试工具，如测试脚本、数据库变量、于假定起始状态的基线配置、度量标准和校准工具可以协助实际的测试。商业和免费软件工具也可以进行与诊断路由和模拟网关以及连接设备。

如果进行任何渗透测试，测试中系统的性能需要注明额外的渗透测试结果。最有可能有一些系统或组件由于渗透测试而性能退化。这些性能衰减应该被注明供今后使用。

需要强调的是，安全对策也包括政策和过程，像手动检查安全。例如，一个对策可能由工程师安装安全补丁给硬件或软件来组成。测试计划可能通过运行补丁安装的序列，但注意其他因素的影响。

C.2.3.4 与开发环境分离的系统测试

开发和测试活动可以导致严重的问题，如不必要文件或系统环境或甚至是系统故障的没有预期的修改。进行信息安全测试在与操作系统分离的系统上很重要，因为这样，减少通过非法开发员路径意外改变的风险或未授权访问操作软件和商业数据。如果开发和测试人员有权限进入操作系统和获取信息，也可能导致未授权和未测试编码或改变运行数据。开发和测试人员也对操作信息的保密造成了威胁。如果他们使用同一个计算机，开发和测试活动可能导致对软件和信息意想不到的改变。

消除这些问题的首选方法是使用与操作系统分离的系统来运行初始开发和测试。如果这个不可能，应注意保证系统采用适当的变更管理器记录任何系统变化，提供撤销变化的能力。

参 考 文 献

[1] GB/T 15851—1995 信息技术安全技术带消息恢复的安全技术要求

[2] GB/T 17901 信息技术 安全技术 密钥管理 第1部分:框架(GB/T 17901—1999,idt ISO/IEC 11770-1:1996)

[3] GB/T 17902—1999 信息技术 安全技术 带附录的数字签名

[4] GB/T 18336—2001 信息技术 安全技术 信息技术安全性评估准则

[5] GB/T 19011—2003 质量和(或)环境管理体系审核指南(ISO 19011:2002,IDT)

[6] GB/T 28455—2012 信息安全技术 引入可信第三方的实体鉴别及接入架构规范

[7] ISO/IEC 9798 信息技术 安全技术 实体鉴别

[8] ISO/IEC 20009-2 信息技术 安全技术 匿名实体鉴别 第2部分:基于群组公钥签名的机制

[9] IEC 62443-1-1 工业过程测量和控制安全 网络和系统安全 第1-1部分:术语、概述和模型

[10] IEC 62443-1-3 工业过程测量和控制安全 网络和系统安全 第1-3部分:系统的安全性符合指标

[11] IEC 62443-2-1 工业过程测量和控制安全 网络和系统安全 第2-1部分:建立工业自动化和控制系统(IACS)安全程序

[12] IEC 62443 3-2 工业过程测量和控制安全 网络和系统安全 第3-2部分:用于区域和管道的安全保证等级(SAL)

[13] IEC 62443-4-1 工业过程测量和控制安全 网络和系统安全 第4-1部分:用于工业自动化和控制系统的产品开发要求

[14] IEC 62443-4-2 工业过程测量和控制安全 网络和系统安全 第4-2部分:用于工业自动化和控制系统组件的技术的安全要求