ICS 35.040
L 80

# 中华人民共和国国家标准化指导性技术文件

GB/Z 32916—2016/ISO/IEC TR 27008:2011

# 信息技术　安全技术
# 信息安全控制措施审核员指南

**Information technology—Security techniques—
Guidelines for auditors on information security controls**

(ISO/IEC TR 27008:2011,IDT)

2016-08-29 发布　　2017-03-01 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

本指导性技术文件按照 GB/T 1.1—2009 给出的规则起草。

本指导性技术文件使用翻译法等同采用国际技术报告 ISO/IEC TR 27008:2011《信息技术　安全技术　审核员信息安全控制措施审核指南》(英文版)。根据我国国情和 GB/T 1.1 的规定,做以下编辑性修改:

——盲测又称黑盒测试,加了标注"(黑盒测试)";

——透明盒测试又称白盒测试,加了标注"(白盒测试)"。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本指导性技术文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本指导性技术文件起草单位:中国电子技术标准化研究院、中国合格评定国家认可中心、工业和信息化部电子第五研究所、北京赛西认证有限责任公司、北京时代新威信息技术有限公司。

本指导性技术文件主要起草人:倪文静、董涛、刘健、张杰、刘晓红、韩硕祥、付志高、段森、刘小茵、王新杰、黄俊梅、魏军。

# 引　言

本指导性技术文件支持 GB/T 22080 和 ISO/IEC 27005 中定义的信息安全管理体系(ISMS)风险管理过程,以及 GB/T 22081 中包含的控制措施。

本指导性技术文件提供对组织信息安全控制措施进行评审的指南,例如,在组织、业务过程和系统环境下进行技术符合性检查等。

有关管理体系要素的审核,请参考 ISO/IEC 27007。有关认证目的的 ISMS 符合性评审,请参考 GB/T 25067。

# 信息技术　安全技术
# 信息安全控制措施审核员指南

## 1　范围

本指导性技术文件为评审控制措施的实现和运行提供指南，包括对信息系统控制措施的技术符合性检查，以符合组织所建立的信息安全标准。

本指导性技术文件适用于所有类型和规模的组织，包括公有和私营公司、政府机构、非营利组织开展信息安全评审和技术符合性检查。本指导性技术文件不适用于管理体系审核。

## 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 29246—2012　信息技术　安全技术　信息安全管理体系　概述和词汇(ISO/IEC 27000:2009，IDT)

## 3　术语和定义

GB/T 29246—2012 界定的以及下列术语和定义适用于本文件。

3.1

**评审对象　review object**

要评审的指定项。

3.2

**评审目的　review objective**

描述所要达到评审结果的陈述。

3.3

**安全实现标准　security implementation standard**

授权的安全实现方式的规范文件。

## 4　本指导性技术文件的结构

本指导性技术文件包含信息安全控制措施评审过程的描述，其中包括技术符合性检查。第 5 章为背景信息，第 6 章为信息安全控制措施评审的概述，第 7 章为评审方法，第 8 章为评审活动。

技术符合性检查参见附录 A，初始信息收集参见附录 B。

## 5　背景

组织信息安全控制措施的选择宜基于风险评估的结果，并作为信息安全风险管理过程的组成部分，以将风险降低到可接受的水平。但对于决定不实施信息安全管理体系(ISMS)的组织，可通过其他方式

选择、实现和维护信息安全控制措施。

通常，例如当信息资产包括信息系统时，组织的部分信息安全管控通过技术性的信息安全控制措施实现。

宜依据技术性的信息安全标准定义、文件化、实现和维护组织的技术性安全控制措施。随着时间的推移，信息安全控制措施的有效性可能会受到如下因素的负面影响，并最终影响组织的信息安全标准：

- 内部因素，诸如：信息系统改进、安全功能配置和信息系统环境的变化；
- 外部因素，诸如：攻击技能的提高。

组织宜制订严格的信息安全变更控制计划。组织宜定期评审是否适当地实现和运行了信息安全实现标准。技术符合性检查是 GB/T 22081—2008 中的控制措施之一，或手动或借助自动化工具的技术评审来执行。技术符合性检查可由未参与控制措施执行的角色（例如系统所有者），或者具体控制措施的责任人，或者内部或外部的信息安全专家（包括 IT 审核员）来执行。

技术符合性评审检查的输出将说明与组织的信息安全实现标准实际的技术符合程度。当技术控制措施符合信息安全标准时，为实际技术符合程度提供保证，否则作为改进的依据。审核开始时宜明确地建立审核报告链，并保证报告过程的完备性。宜采取相应的步骤，以确保：

a) 相关责任方直接从信息安全控制措施评审审核员（以下简称审核员）处收到未改动的报告副本；
b) 不适宜或未经授权方无法获得来自审核员的报告副本；
c) 审核员能够不受妨碍地开展其工作。

信息安全控制措施评审，尤其是技术符合性检查，可帮助组织：

a) 识别和理解组织在实现和运行信息安全控制措施、信息安全标准及相应的技术性信息安全控制措施方面潜在问题或不足的程度；
b) 识别和理解未充分消除的信息安全威胁和脆弱性对组织的潜在影响；
c) 确定降低信息安全风险活动的优先级；
d) 确认先前识别的或突发的信息安全弱点或不足已得到充分解决；和（或）
e) 支持与组织信息安全管理改进有关的投资过程中的预算决策和其他管理决策。

本指导性技术文件依据组织建立的信息安全实现标准关注信息安全控制措施评审，包括技术符合性检查。本指导性技术文件无意为 ISO/IEC 27004 规范的测量、ISO/IEC 27005 规范的风险评估和 ISO/IEC 27007 规范的 ISMS 审核方面的符合性检查提供具体指南。

作为制定信息安全控制措施评审规程的过程起点，本指导性技术文件可促进组织内信息安全具有更好的一致性。

使用本指导性技术文件为定制基于业务任务和目标、组织策略和要求、已知威胁和脆弱性信息、运行考虑、信息系统和平台依赖性以及风险承受度的评审提供所需的灵活性。

注：ISO 指南 73 将风险承受度定义为组织准备追踪、保持和接受的风险大小和类型。

## 6 信息安全控制措施评审概述

### 6.1 评审过程

当启动一个独立的信息安全评审时，信息安全控制措施评审审核员和与此评审相关的审核员通常先收集初步信息、评审工作计划的范围、联络组织相关部门的管理人员和其他联系人、开展对评审风险的评估，以制定指导实际评审工作的文件。

为了有效地进行评审，指定的审核员需要做好控制措施方面和测试方面的准备（例如：适用工具的操作，测试的技术目标）。在此阶段，各项评审工作可依据感知的风险来排列优先顺序，也可按照特定的业务流程或系统来计划，或者简单地按顺序来覆盖评审范围的所有领域。

初步信息收集的各种来源如下：

a) 该领域的书籍、互联网搜索、技术手册、标准和其他背景下研究的常见风险和控制措施，以及会议、研讨会、培训或论坛；

b) 以往的评审、测试和评估的结果，无论该评审、测试和评估是部分或完全符合本次评审范围，还是是否由审核员进行的(例如由信息安全专业人员进行的预发布安全测试可提供针对主要应用系统安全性的丰富信息)；

c) 从IT服务台、IT变更管理、IT事件管理流程和相类似的途径所搜集到的，与信息安全事件、事态、请求支持的问题和变更相关的信息；

d) 审核员或专业领域的信息安全人员通用的评审检查单和检查内容。

根据初始信息评审已策划的评审范围可能是适当的，尤其是在几个月之前就已经制定好的评审计划范围。例如，其他的评审活动未涉及值得深入探讨的关注点，或者已增加了保障则允许目前的工作重点转移到其他领域关注点。

在初期阶段，一项重要的活动是与管理者和评审联络人保持联系。因在评审结束时，他们需要了解评审发现，以便积极响应评审报告。彼此理解、相互尊重、充分解释评审过程，可显著改进评审结果的质量和影响。

每个审核员将其工作形成文件的方式有所不同，许多评审活动可利用工作文件模板来支持标准化的评审过程，如：评审检查单、内部控制措施调查问卷、测试计划、风险控制措施矩阵等。

评审检查单(或类似的文档)是一个关键文件，有以下几个原因：

a) 列出了评审工作已计划的范围，可详细到描述单个评审测试和预期/理想发现的程度；

b) 提供了评审工作的结构，有助于确保评审工作能充分地涵盖所策划的范围；

c) 必要的分析最初编写的检查表可使审核员为后续的现场评审工作做好准备。随着评审进展开始分析过程、逐步填写检查表、再根据分析过程生成评审报告；

d) 提供了记录前期和现场评审结果的框架，例如，检查表里可以引用和评价收集到的评审证据；

e) 审核管理人员或其他审核员可以评审检查表，作为评审工作质量保障过程的一部分；

f) 检查单一旦完成，连同评审证据作为产生的结果和发现构成一个评审工作合理的详细历史记录，用于证实或支持评审报告，向管理层报告和/或帮助策划以后的评审。

审核员宜谨慎避免简单使用他人编写的通用评审检查单。这样也许会节省时间，但可能会丧失上面提到的几个好处。(对于明确的符合性评审或认证评审，因为需要满足的要求通常很明确，简单使用他人编写的检查表可能不会造成问题。)

大部分的现场评审工作是由审核员实施或其要求实施的一系列测试组成，以收集评审证据并对其评审，评审经常通过与相关符合性法规、标准或获得广泛认可的良好实践的预期或期望结果进行对比来实现。例如，检测恶意软件控制措施的测试评审，可能检查是否所有适用的计算机平台安装反病毒软件。此类评审测试经常使用抽样技术，因为很少会有足够的评审资源以进行全面的测试。不同的审核员和实际情况会有不同抽样实践，可能包括随机选择、分层选择和其他更复杂的统计抽样技术(例如，为了证实控制措施不足的程度，在初始结果不令人满意时采取额外的抽样)。通常来说，以电子的方式收集和测试证据时可进行更全面的测试，例如使用SQL查询语句从系统和资产管理数据库中整理出评审证据数据库。审核抽样方法至少部分宜以被审核运行区域的风险为导向。

通常宜在评审工作文件中标注、引用或存储评审过程中收集到的证据。在评审分析、发现、建议和报告的过程中，审核员需充分保护评审证据，特别是一些很可能是非常敏感和/或有价值的证据。例如，从生产数据库中提取的用于评审的数据，宜通过访问控制措施、加密等手段使其达到和生产数据库相同程度的保护。自动评审工具、查询、实用程序/数据提取程序等也宜严格控制。同样，由审核员打印的或提供给审核员的打印资料，一般宜通过加锁等措施保护其物理安全，以防止未经授权的泄露或修改。对于特别敏感的评审，宜在评审的早期阶段识别风险和必要的信息安全控制措施并做好准备。

随着评审检查的完成、一系列评审测试、评审证据地充分收集，审核员宜对评审证据进行检查，确定信息安全风险被处置的程度，并评审所有残余风险的潜在影响。在这个阶段，审核员可以起草某种形式的评审报告，对评审工作的质量进行评审，以及与管理层讨论，特别是对直接被评审的业务单位、职能部门或团队的讨论，也可能涉及组织的其他部门。

审核管理人员宜公正地对评审证据进行检查：

a) 有充分的评审证据来提供事实依据支持所有评审发现；

b) 所有评审发现及建议宜与评审范围相关，无关事项排除在外。

如果对评审发现需要策划进一步的评审工作，宜在报告中注明。

与评审计划一样，分析过程本质上是基于风险的，在评审工作中收集的证据能为分析过程提供有用的信息。简单的符合性评审通常可以产生一系列相对简单的具有明确意见的符合/不符合的结果。信息安全评审通常会带来一些需要管理层在决定采用何种适当的行动(如果有)之前需考虑和讨论的事项。在有些情况下，管理层可能有选择性地接受一定的信息安全评审确定的风险；另外一些情况下，管理层有权决定不采纳评审的建议，但是这需要承担相应的责任。从这个意义上说，尽管审核员拥有重大影响力并且有丰富的评审实践和事实证据做支撑，但他们只是作为建议而非执行的角色。

审核员宜通过合理的评审来证实组织的信息安全活动(并非单指管理体系)达到了既定目标。评审宜提供实际情况与准则之间的差距说明。当一个内部策略作为准则的时候，宜明确该策略足以作为准则。为确保这一点，可参考附录 B 所列的准则。审核员宜在评审范围内考虑内部策略和规程。未考虑的相关准则仍可能被非正式地应用于组织内。已识别的关键准则未被应用可能会导致潜在的不符合。

### 6.2 资源配备

信息安全控制措施的评审需要客观分析和专业报告的技能。针对技术符合性检查，还需要额外的专业技能，他们需具备了解信息安全策略如何在软件、硬件、通信链路及其相关技术过程中执行的具体技术知识。审核员宜具备：

a) 基于对信息系统框架概念的理解，对信息系统风险和安全结构的评价能力；

b) 良好的信息安全实践的知识，例如由 GB/T 22081—2008 和其他安全标准给出的信息安全控制措施；

c) 深入检查复杂技术信息的能力，以识别任何重大的风险和改进的机会；

d) 评价评审信息安全和信息技术局限性的实用方法。

强烈建议任何没有审核经验的人在分派去执行信息安全控制措施审核前，需正式地掌握审核专业基础知识，具备职业道德、独立性、客观性、保密性、责任心和判断力；了解访问记录授权的权限来源、职能、资产、人员和信息；具有处理与保护所获得的信息、评审发现与建议以及随之而来的后续过程等的责任。

为实现评审目的，评审小组可由拥有各相关专业能力的审核员组成。当要求范围内实施评审的相关专业技术和能力尚未具备时，宜安排专家和资源(无论内部还是外部的)并考虑风险和利益。

审核员还宜确认组织及其负责信息安全的人员能够参与，并且具备足够的信息安全知识、具体任务和必要的资源。

作为组织反欺诈工作的一部分，审核员可能需要在每个审核策划、审核实现和审核评审阶段中与财务审计师进行密切合作。

## 7 评审方法

### 7.1 概述

评审控制措施典型的基本概念包括：评审规程、评审报告和评审跟踪。评审规程的设计和内容包

括:评审目的和评审方法。

审核员在信息安全控制措施评审过程中可以采用以下三种评审方法:

a) 检查;

b) 访谈;

c) 测试。

下面相应章节采用一组属性和属性值来定义每种评审方法。对于深度属性,属性值"重点的"包括属性值"一般的"所定义的评审严格度和详细度,并建立在其上;属性值"详尽的"包括属性值"重点的"所定义的评审严格性和详细度,并建立在其上。对于广度属性,属性值"特定的"包括属性值"典型的"所定义的评审对象数量和类型,并建立在其上;属性值"全面的"包括属性值"特定的"所定义的评审对象数量和类型,并建立在其上。

"检查"和"测试"方法可以使用被广泛认可的自动化工具来支持。审核员宜同时评审这种工具的运行对评审对象正常运行的影响。当评审的某部分依赖于这种工具时,审核员宜证明或者提供证据来说明这种工具提供可靠结果。

## 7.2 评审方法:检查

### 7.2.1 概要

核查、检验、评审、观察、研究或者分析一个或多个评审对象以便理解、澄清或获取证据的过程及其结果,以用来确定评审区间内存在的控制措施,及其功能性、正确性、完备性和潜在改进的可能性。

评审对象通常包括:

a) 规范(例如,策略、计划、规程、系统需求、设计);

b) 机理(例如,在硬件、软件和固件中执行的功能);

c) 过程(例如,系统的操作、监管、管理、演练)。

典型的审核员的评审活动可能包括:

a) 评审信息安全策略、计划和规程;

b) 分析系统设计文档和接口规范;

c) 观察系统备份操作和评审应急预案演练的结果;

d) 观察事件响应过程;

e) 研究技术手册和用户/管理员指南;

f) 核查、研究或观察信息技术机制在信息系统的硬件/软件中的运行;

g) 核查、研究和观察信息系统的变更管理和活动日志;

h) 核查、研究或观察与信息系统操作有关的物理安全措施。

### 7.2.2 属性

#### 7.2.2.1 一般检查

一般性检查通常包含对评审对象的通盘审视、核查、观察和检验。这种类型的检查只使用有限的证据或文档(例如,机理功能级别的描述;过程中高级过程的描述;实际规格说明书)。一般性检查为确定必要的控制措施是否实现和无明显错误提供了一定程度的了解。

#### 7.2.2.2 重点检查

重点性检查通常包含对评审对象的通盘审视、核查、观察、检验和更深入的研究/分析。这种类型的检查需要大量的证据或文件(例如,机理的功能说明、适用及可用时其概要设计信息;过程的概要信息及其实现规程;规范及与其相关的文档)。重点检查帮助审核员了解必须的安全控制措施是否实现且无明

显错误。检查同样为该控制措施被正确的实现且按预期运行提供更多的证明。

#### 7.2.2.3 详尽检查

详尽检查通常包含对评审对象的通盘审视、核查、观察、检验和更深入、详尽、彻底地研究/分析。实现这类检查使用广泛的证据或文件(例如,机理的功能说明、适用及可用时其概要设计、详细设计及实现信息;过程的概要信息及其详细的实现规程;规范及与其相关的文档)。详尽检查帮助审核员了解必须的安全控制措施是否实现且无明显错误,同时为该控制措施被正确的实现且按预期持续、一致的运行提供更多证明,且对控制措施的有效性提供持续改进的支持。

#### 7.2.2.4 典型检查

典型检查使用达到必要覆盖率的评审对象的抽样样本(类型和数量),以确定其相关的控制措施是否实现且无明显错误。

#### 7.2.2.5 特定检查

特定检查使用评审对象的抽样样本(类型和数量)和其他对达到评审目的起重要作用的特定评审对象。特定检查也提供必要的覆盖率,以确定其相关的控制措施是否实现且无明显错误、是否能进一步证明控制措施正确实现且按预期运行。

#### 7.2.2.6 全面检查

全面检查使用充足的评审对象样本(类型和数量)和其他对达到评审目的起重要作用的特定评审对象。全面检查提供必要的覆盖率,以确定其相关的控制措施是否实现且无明显错误、是否能进一步证明控制措施正确实现且按预期持续一致的运行,且对控制措施的有效性提供持续改进的支持。

### 7.3 评审方法:访谈

#### 7.3.1 概要

访谈是指与组织内的个人或者小组进行讨论,以便于理解、澄清或者找到证据出处的过程。访谈结果用于支持确定信息安全控制措施的存在、功能性、正确性、完备性以及潜在的持续改进。

评审对象通常包括个人或小组。

典型的审核活动可能包括与以下人员访谈:

a) 管理者;
b) 信息资产和任务的负责人;
c) 信息安全主管;
d) 信息安全管理员;
e) 人事主管;
f) 人力资源管理员;
g) 设施管理员;
h) 培训主管;
i) 信息系统操作员;
j) 网络和系统管理员;
k) 站点管理员;
l) 物理安全主管;
m) 用户。

#### 7.3.2 深度属性

##### 7.3.2.1 一般访谈

与个人或小组进行的广泛的、通盘讨论。这种访谈通过一组通用的、高层次的问题来完成。一般访谈帮助审核员了解必须的安全控制措施是否实现且无明显错误。

##### 7.3.2.2 重点访谈

重点访谈除了一般访谈的要求以外，还包括与个人或小组进行的某个特定领域的深入讨论。这种类型的访谈是在有迹象表明需要更深入调查的特定领域里额外地询问更深入的问题。重点访谈帮助审核员了解必须的安全控制措施是否实现且无明显错误、是否能进一步证明控制措施正确实现且按预期运行。

##### 7.3.2.3 详尽访谈

详细访谈除了重点访谈的要求以外，还包括在有迹象表明需要更深入调查的或评审规程有要求的特定领域里询问更深入、更具探究性的问题。详细访谈帮助审核员了解必须的安全控制措施是否实现且无明显错误、是否能进一步证明控制措施正确实现且按预期运行，且对控制措施的有效性提供持续改进的支持。

#### 7.3.3 广度属性

广度属性指的是访谈过程的范围或者广度，它包括被访谈的人员类别(按其相关的组织角色和责任来分)，被访谈的人的数量(按类别分)，以及某些特定的被访谈的人。

##### 7.3.3.1 典型访谈

典型访谈指的是与组织的关键角色有代表性的个人进行的访谈，达到必要的覆盖率，以确定其相关的控制措施是否实现且无明显错误。

##### 7.3.3.2 特定访谈

特定访谈指的是与组织的关键角色、有代表性的个人，和其他对达到评审目标起重要作用的特定人员进行的访谈。特定访谈提供必要的覆盖率，以确定其相关的控制措施是否实现且无明显错误、是否能进一步证明控制措施正确实现且按预期的运行。

##### 7.3.3.3 全面访谈

全面访谈指的是与组织足够数量的关键角色的人员，和其他对达到评审目标起重要作用的特定人员进行的访谈。全面访谈提供必要的覆盖率，以确定其相关的控制措施是否实现且无明显错误、是否能进一步证明控制措施正确实现且按预期持续一致的运行，且对控制措施的有效性提供持续改进的支持。

### 7.4 评审方法：测试

#### 7.4.1 概要

测试是指在规定条件下对一个或多个评审对象进行演练，并将实际情况与期望的行为进行对比的过程。其结果用来支持确定信息安全控制措施的存在、功能性、正确性、完备性以及潜在的持续改进。测试应由有能力的专家来执行，且需谨慎，测试对组织的运行可能造成的影响应在测试开始前得到考虑并经过管理层的批准。并且需要考虑选择在非运行窗口或低负荷的环境，甚至在复制的测试环境中进

行测试。测试造成的系统故障或不可用可能会给组织的正常业务运行造成重大影响，可能会造成经济损失或影响组织的声誉。因此，在测试策划以及签约时(包括考虑法律方面的事宜)需要特别注意。

在做出任何推断之前，审核员应仔细调查测试结果中存在的误报和漏报。

典型的评审对象包括机理(如硬件、软件、固件)和过程(如系统的操作、实现、管理以及演练)。

审核员的典型活动可包括：

a) 测试访问控制、身份鉴别、授权以及审查机制；
b) 测试安全配置设置；
c) 测试物理访问控制措施设备；
d) 执行关键信息系统组件的渗透测试；
e) 测试信息系统的备份操作；
f) 测试事件响应能力；
g) 演练应急策划能力；
h) 测试安全系统入侵检测、报警和响应的能力；
i) 测试加密机制和哈希算法；
j) 测试用户 ID 和特权管理机制；
k) 测试授权机制；
l) 验证安全措施的级联恢复能力。

注：测试不适用于属性。

### 7.4.2 测试类型

#### 7.4.2.1 盲测(黑盒测试)

盲测(黑盒测试)是指审核员事先未掌握评审对象除公开信息以外的任何其他特性的情况下进行的测试，盲测(黑盒测试)的评审对象已经为评审做好准备，并且提前知道评审的详细细节。盲测(黑盒测试)主要测试审核员的技能。盲测(黑盒测试)的广度和深度也只是体现了审核员知识的广度和工作效率。这种测试在安全评审中的作用是有限的，应该避免使用。该方法通常也被称为红客测试。

#### 7.4.2.2 双盲测试

双盲测试是指审核员事先未掌握评审对象除公开信息以外的任何其他特性的情况下进行的测试。双盲的评审对象在评审前也不知道评审的范围以及将使用的测试向量。双盲评审测试了评审对象对未知扰动变量的准备程度。

#### 7.4.2.3 灰盒测试

灰盒测试是指审核员对审查对象的防御能力和资产有限的了解，但是对可用的测试向量完全掌握的情况下进行的测试。评审对象已经为评审做好准备，并且提前知道评审的详细细节。灰盒评审测试了审核员的技能。这种测试的本质是效率。测试的广度和深度取决于测试前提供给审核员的信息的质量，以及审核员的适用知识。这种测试在安全评审中的作用是有限的，宜避免使用。这种类型的测试经常称作脆弱性测试，通常由自我评估活动的对象发起。

#### 7.4.2.4 双灰盒测试

双灰盒测试是指审核员对审查对象的防御能力和资产有限的了解，但是对可用的测试向量完全掌握的情况下进行的测试。评审对象对评审的范围以及评审的时间框架已经了解，但测试向量是未知的。双灰盒评审测试了评审对象对未知扰动变量的准备程度。测试的广度和深度取决于测试前提供给审核

员的信息的质量，以及审核员的适用的知识。

#### 7.4.2.5 透明盒测试(白盒测试)

透明盒测试(白盒测试)是指审核员和评审对象都已经为评审做好了准备，并都提前知道了评审的细节。透明盒测试(白盒测试)评审了对目标的保护和控制情况，但它不能测试未知扰动变量目标的准备程度。当审核员对所有的测试以及响应有全面的评审，这种测试的本质是全面的。测试的广度和深度取决于测试前提供给审核员的信息的质量，以及审核员的适用知识。这种测试常用于内部评审，审核员往往在全部安全过程中起到积极的作用。

#### 7.4.2.6 逆向测试

逆向测试是指审核员完全了解评审对象的过程和安全操作，但是评审对象不知道审核员将测试什么、如何测试以及何时测试。这种测试真正的本质是评审目标对未知扰动变量和向量的准备程度。测试的广度和深度取决于测试前提供给审核员的信息的质量，以及审核员的适用知识和创造力。这常被称为红队演练。

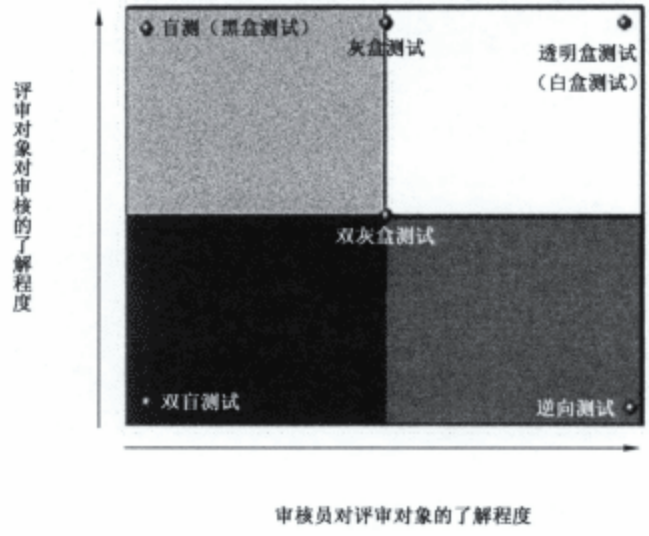


图 1 测试类型

### 7.4.3 扩展的评审规程

除了应用于单个控制措施的评审规程，扩展的评审规程可以适用于整体评审。扩展的评审规程被设计用于和评审规程一起使用并补充该规程，以便为控制措施有效性提供证明。

扩展的评审规程和相关的评审目的也与信息系统的风险级别密切相关。

## 8 活动

### 8.1 准备

为获得可接受的结论，在评审前、评审中和评审后建立并保持一组适当的期望很重要。这意味着为管理层提供信息，使其能够针对如何最佳地实现和运行信息系统做出合理的、基于风险的决策。组织和审核员的充分准备是进行有效评审的重要环节。准备活动宜关注一系列与成本、进度、专业知识的可用性和评审绩效等相关的问题。

从组织的角度看，评审准备包括以下关键活动：

a) 确保具备覆盖评审的适当的策略，并且被组织所有的成员所理解；
b) 确保为实现控制措施所策划的所有步骤在评审之前已经成功完成，并接受适当的管理评审（仅适用于被标记为“全面运行”的控制措施，而不是筹备/实现阶段的控制措施）；
c) 确保所选择的控制措施已分配给适当的组织实体进行开发和实现；
d) 建立评审的目的和范围（即评审的目的和内容）；
e) 通知组织主要的管理者即将进行的评审并分配实现评审所需的必要资源；
f) 在与评审有关的组织管理者中建立适当的沟通渠道；
g) 为有效地管理评审，建立组织所需要的评审时间框架和关键决策点；
h) 识别和选择一个胜任的审核员或审核小组负责实现评审，并考虑审核员的独立性；
i) 收集组织文件（例如，包括组织结构图、策略、规程、计划、规范、设计、记录、管理员/操作员手册、信息系统文档、互联协议、以往评审结果等信息安全控制文件）并提供给审核员；
j) 在组织和审核员之间建立一种机制，最小化评审期间发现的控制措施实现或控制措施弱点/缺陷的歧义或误解。

除了组织为评审准备所实现的策划活动之外，审核员宜从以下方面为评审做准备：

a) 理解组织的总体运作（包括任务、职能和业务流程）和评审范围内的信息资产如何支持这些组织运作；
b) 了解信息资产结构（即系统架构）；
c) 充分了解所有被评审的控制措施；
d) 研究这些控制措施中所引用的相关出版物；
e) 识别负责开发和实现评审范围内支持信息安全控制措施的组织实体；
f) 建立实现评审所需的适当的组织联络点；
g) 获得评审所需组织文件（例如策略、规程、计划、规范、设计、记录、管理员/操作员手册、信息系统的文档、互联协议）；
h) 获得以往的可适当再次用于评审的评审结论（例如报告、评审、漏洞扫描、物理安全检查、开发测试和评估）；
i) 与组织中相关的管理者会面，确保对评审目的、建议的评审严格度和范围达成一致；
j) 制定评审计划。

为信息安全控制措施评审做准备时，宜收集必要的背景信息供审核员使用。为支持特定评审组织宜识别组织中相关的个人或小组，并安排对其的访问。这些个人或小组负责开发、编制、分发、评审、运行、保持、更新所有的安全控制措施、安全策略和有关实现符合性策略控制措施的规程。审核员也需要获得信息系统的安全策略和相关的实现规程、与控制措施实现和运行及评审对象相关的材料（例如安全计划、记录、日程安排、评审报告、改进后报告、协议和认可包）。

必需文件的可用性、关键组织人员与被评审信息系统的可访问性对一个成功的信息安全控制措施评审来说是非常重要的。

## 8.2 制定计划

### 8.2.1 概述

制定评审控制措施计划的审核员宜确定控制措施评审的类型（例如，完整评审或部分评审），以及基于评审的范围和目的确定评审中将包含哪些控制措施/控制措施增强。审核员宜评估和降低评审活动对组织正常运营的风险和影响（可能时），并基于评审中所涉及的控制措施和控制措施增强以及它们关联的深度和覆盖范围，选择合适的评审规程。

审核员宜根据信息系统风险水平和组织的实际运行环境来对所选择的评审规程进行裁剪。必要时,审核员还宜针对本技术规范中未覆盖的安全控制措施、控制措施增强和额外保障需求制定附加的评审规程。

计划中宜设计一个阶段来确定背景、生成所确定背景下的期望行为的基线以及测试/评价规范和对评价中的发现进行确认的方法。计划宜包括制定应用扩展评审规程的策略,必要时优化评审规程以减少重复工作,并提供有成本效益的评审方案。审核员宜最终确定评审计划,并获得执行计划的必要批准。

### 8.2.2 范围

文件宜提供信息资产安全需求的概述,并描述为满足这些安全需求现有的或计划的控制措施。审核员以信息安全文档中所描述的控制措施为起点并考虑评审目的。评审可以是对组织内所有信息安全控制措施的完整评审或对信息资产保护措施的部分评审(例如,在连续监视期间,持续评审信息资产控制措施的子集)。对于部分评审,信息资产负责人宜与评审相关的组织管理者共同确定需要评审哪些控制措施。控制措施的选择依赖于所建立的连续监测计划、活动计划中的项目和适当的里程碑。宜对不稳定的控制措施实施更频繁的评审。

### 8.2.3 评审规程

评审规程包含一组评审目的,每个评审规程都可能有一组关联的评审方法和评审对象。评审目的的明确性陈述与控制措施内容(即控制措施功能)紧密关联。这确保了评审结果可追溯至基本控制措施要求。评审规程应用于某一控制措施后产生评审发现。这些评审发现随后将有助于确定控制措施的整体有效性。评审对象识别了要评审的特定项,包括了规范的说明、机制、过程和人员。

附录A提供了技术符合性检查和控制措施增强评审规程的示例。附录A中的实践指南用于收集证据,这些证据将用来确定控制措施是否正确实现、按预期运行,并产生与满足信息资产安全需求相关的预期输出。对于评审中所包括的每一个控制措施和控制措施增强,审核员可参照附录A制定相应的评审规程。在不同的评审中,根据当时的评审目的选择不同评审规程(例如控制措施年度评审,连续监测)。附录A提供了一个基于特定的评审关注点选择适宜的评审规程的工作表。

可以通过下列方式裁剪评审规程:

a) 选择能够最有效做出适当判定并满足评审目的所需的评审方法和评审对象;
b) 根据被评审的控制措施的特征和需做出的具体判定来选择评审方法的深度和覆盖范围的特征值,以满足评审期望;
c) 如果某些控制措施已被其他评审过程充分评审,则可删除相应的评审规程;
d) 修订适用于特定的信息系统/平台和特定组织的评审规程,以便成功地实施评审;
e) 在评审结论中引用以往合适的评审结果;
f) 如需从外部供应商获得必要的评审证据,则适当调整评审规程;
g) 在确保满足实现评审目的情况下,选择的评审方法宜考虑其对组织的影响。

### 8.2.4 与对象有关的考虑

组织可以通过多种方式来描述、记录和配置他们的信息资产,因此现有评审证据的内容和适用性会有所不同。这可能会需要对不同的评审对象应用不同的评审方法,以形成用于确定控制措施在应用中是否有效地评审证据。因此,每个评审规程所提供的评审方法和评审对象的列表,可能为特定的评审选择最合适的方法和对象。选用的评审方法和对象是为产生评审证据所必须的。评审规程中的潜在方法和对象是作为一种资源协助选择适当的方法和对象,而不是为了限制选择。因此,在从潜在的评审方法中选择评审方法以及从已选方法相关的评审对象清单中选择评审对象时,审核员宜有自己的判断。

审核员宜只选择那些有助于最有效地做出与评审目的相关的决定的方法和对象。测量评审结论的质量是基于所提供的选择评审方法和对象理由的合理性，而不是所采用的特定的方法和对象本身。在大多数情况下，没有必要为了达到理想的评审结果而对每一个评审对象使用各种评审方法。而对于特定评审和全面评审，使用目前未列入的潜在方法或者不采用已列入的方法都可能是适宜的。

### 8.2.5 以往的发现

#### 8.2.5.1 概述

审核员宜利用现有的控制措施评审信息以促进更有效地评审。

宜将先前已接受或批准的信息系统评审结论的重用作为确定所有控制有效性证据的一部分。

当考虑再次使用以往的评审结论和这些结论对当前评审的价值时，审核员宜确定：

a) 证据的可信性；

b) 以往分析的合理性；

c) 证据对当前信息资产状况的适用性。

当考虑再次使用以往的评审结果时，在某些情况下可能有必要通过附加的评审活动对其进行补充，以完全满足评审目的。例如，如果一个信息技术产品的独立第三方评价没有测试某信息系统中组织所采用的某特定配置的设置，那么审核员可能需要通过附加的测试来覆盖这种配置的设置，以补充原有的测试结果。

在确认以往的评审结果能否在当前评审中再次使用时，宜考虑以下章节。

#### 8.2.5.2 环境变化

在以往的评审中被视为有效的控制措施可能由于与信息资产或者周围环境相关的条件改变而变得无效，因此之前被认为是可以接受的评审结论可能不再提供可信的证据来确定控制措施的有效性，故需要一次新的评审。将之前的评审结论应用于当前的评审，需要识别自上次评审以来发生的任何变更和这些变更对以往评审结果的影响。例如，如果确定已识别的策略、规程和风险环境没有显著变化，就可重用之前的评审结果检查组织的安全策略和规程。

#### 8.2.5.3 重用评审结果的可接受性

在控制措施评审中使用以往的评审结果是否可接受(在控制措施评审时是否可使用以往的评审结果)，宜与评审结论的使用者协调并获得其批准。在确定使用之前的评审结果时，信息资产所有者有必要与相应的组织管理者(例如，首席信息官、首席信息安全官、任务/信息所有者)配合。决定重新使用评审结果的决定宜记录在评审计划和最终报告中。

只要符合以下条件，安全评审可以包括以往的安全评审发现：

a) 审核计划中明确允许；

b) 审核员有很好的理由相信审核发现仍然有效；

c) 当前评审对这些运用于控制措施和过程中的任何技术或者规程上的审核发现的改变给予了充分的安全考虑；

d) 审核报告中明确表述了使用以往的审核发现和使用这些审核发现对风险管理潜在的影响。

#### 8.2.5.4 时效

一般情况下，随着当前和以往评审之间的时间间隔增加，以往评审结果的可信性/可用性就会下降。主要是因为信息资产或者信息资产运行的环境更可能随着时间的推移而改变，可能会使之前评审依据的原始条件或者设想失效。

#### 8.2.6 工作分配

审核员的独立性在某些类型的评审中是关键因素，尤其是对中等和高风险的信息资产。每次评审需要的独立性程度宜保持一致。例如，在当前更高独立性的评审中，不适合重新使用以往未要求审核员自我评估独立性的结论。

#### 8.2.7 外部系统

为适应外部信息系统的评审，需适当调整附录 A 中的评审方法和规程。因为组织并不能总是直接控制外部信息系统中所使用的安全控制措施，或对这些控制措施的开发、实现和评审上并不总是充分的了解，这可能需要裁剪附录 A 中描述的评审规程。信息系统所需要的保障或已协定的控制措施需被记录在合同或服务级别协议中。审核员宜评审这些合同或协议，并在适当的情况下调整评审规程来评审按这些协议提供的控制措施或控制措施评审结果。此外，对于运行外部信息系统对被评审的信息资产进行保护的组织，审核员宜对组织已进行或正在进行的评审予以考虑。宜将评审中认为可信的可用信息纳入报告中。

#### 8.2.8 信息资产和组织

评审规程可做调整以适应系统/平台特定的或组织特定的依赖关系。在技术性信息安全控制措施（即访问控制、审核与责任追究、标识与鉴别、系统和通信保护）相关的评审规程中常有这种情况。如果这些测试方法提供较透明度高（例如，测试了什么、何时测试、如何测试），最近的测试结果也可能适用于当前的评审。基于标准的测试协议可为组织如何帮助达到这种程度的透明提供范例。

#### 8.2.9 扩展的评审规程

在达到信息安全控制措施的保障要求时组织有很大的灵活性。例如，保障缺陷及时处理的要求，组织可以基于具体控制、控制类型、具体系统甚至组织级别来满足要求。

考虑到这种灵活性，7.4.3 中扩展的评审规程要基于逐个评审的基础加以应用，通常依照组织选择如何对评审中信息资产实现保障的方式。应用的方法宜记录在评审计划中。此外，组织根据信息资产风险水平为扩展的评审规程选择适当的评审目的。扩展的评审规程的应用是为了补充其他评审规程，以增加对控制措施正确实现、按预期进行操作、对符合适用的信息安全需求产生所期望结果的信心。

#### 8.2.10 优化

审核员可以有一定程度的灵活性来组织所需的评审计划。因此，这就提供了一种在获取安全控制措施有效性必要证据的同时降低整体评审成本的机会。

审核员在设计一个满足组织需求的评审计划上有一定的灵活性。在评审期间，评审方法可多次应用于信息安全控制措施特定区域内的各种评审对象。

为节省时间、降低评审成本、并最大限度地提高评审结果的可用性，审核员在可能或可行的情况下，宜评审选定的控制措施领域的评审规程，和联合或整合程序（或规程的一部分）。

例如，审核员可能希望合并与组织内负责处理各种信息安全相关主题的关键管理者的访谈。审核员可通过同时检查所有适用的安全策略和规程，或组织相关策略和规程组（可作为一个统一实体进行检查），获得重大合并和节约成本的机会。获取并检查相关信息系统内相似的硬件和软件组件的配置设置是另一个可明显提高评审效率的示例。

优化评审过程中，另外需要考虑的一个问题是评审安全控制措施的顺序。

先对一些控制措施评审可能会提供一些有利于了解和评审其他控制措施的信息。例如，控制措施领域可能会对信息资产进行一般性描述。在评审过程的早期对这些安全控制措施进行的评审可提供对

信息资产的基本了解以帮助评审其他安全控制措施。许多控制措施的附加指南同样能识别在组织评审规程中提供有用信息的相关控制措施。换句话说，评审实施的顺序可能有助于将一个控制措施的评审信息在评审其他相关控制措施中再利用。

#### 8.2.11 定稿

选择评审规程(包括开发不包含在本文中的必要规程)后，根据信息特定资产和组织特定的条件调整规程，使规程在效率上最优化，在必要时应用扩展的评审规程，并解决可能影响评审的意外事件，评审计划的完成和进度表的建立包含评审过程的关键里程碑。

一旦完成评审计划，相应的组织管理者要评审和认可该计划以确保计划是完整的、符合组织的安全目的和组织的风险评审，以及为评审而分配的资源的成本效益。如果评审可能干扰组织的正常运作[例如由于渗透测试阻碍了关键人员通信或可能的(临时)系统故障]，评审计划需要突出显示这些干扰的程序和时间范围。

### 8.3 实施评审

组织批准评审计划后，审核员根据商定的里程碑和日程执行计划。

针对已选择的评审对象应用设定的评审方法，并收集/形成与每个评审目的决策相关的必要信息，以此实现评审目的。审核员执行评审规程中作出的每一个判定陈述，宜为下列发现之一：

- 满足(S)；
- 部分满足(P)；
- 不满足(O)。

满足的评审发现表明，对于由判定申明所涉及的部分控制措施，获得的评审信息(即评审证据)表明控制措施的评审目的已经达到并产生完全可以接受的结果(S)。部分满足的评审发现表明在评审时，针对其目的，部分控制措施并未完全达到，或控制措施的实现仍在进行中，且保证控制措施将达到一个满意的结果(P)。不满足的发现表明，对于判定申明所涉及的部分安全控制措施，获得的评审信息表明控制措施在操作或实现中有潜在的异常情况，可能需要组织解决相关问题(O)。不满足的发现也可能表明在评审报告中说明的理由，审核员无法获得足够的信息来作出在判定申明中需要的特殊判定。

审核员宜根据控制措施评审中的发现形成公正的、基于事实的评审发现(即所做的判定)。对于每个不满足的发现，审核员宜说明评审发现的情况影响了哪一部分的控制措施(即，那些被认为不满足的或不能够进行评审的控制措施)，并描述控制措施与计划和期待的状态有何不同。审核员也宜注意那些不满足的发现记录对保密性、完备性和可用性的潜在影响。如果评审发现了可能会显著增加组织风险的严重不符合项(即那些严重偏离计划的状况、“不满意”的调查发现)，审核员宜立即通知负责人和管理层，使其立即启动风险降低程序。

### 8.4 分析并报告结果

评审计划提供了评审目的和如何进行评审的详细引导。评审报告作为评审输出和最终评审结果，记录了基于已实现的信息安全控制措施的信息安全保障水平。报告内容包括审核员作出的判断所使用控制措施有效性的必要信息以及基于其发现所作出的组织在实施所选择和适当的控制措施时的整体有效性的信息。该报告是确定组织的业务运作(即任务、职能)、组织资产、个人和组织其他信息安全风险等的一个重要因素。

评审结果宜按照组织策略规定的评审报告格式，以适宜的详细程度来记录。该报告的格式也宜与控制措施评审的类型相适应(如信息系统负责人的自我评估、独立的验证和确认、审核员实施的独立控制措施评审等)。

信息系统的负责人依赖审核员的信息安全专业知识和技术判断对安全控制措施进行评审，并就如

何纠正控制措施的弱点和缺陷以及减少或消除已识别的脆弱性提出具体的建议。

在安全评审报告初稿中，审核员将把评审有关的信息(既满意或者不满意的评审发现/关于部分未产生令人满意的安全控制措施的鉴定/对危及信息资产的潜在危害的描述)提供给管理层。在评审报告定稿前，如果有机会纠正控制措施的脆弱性、或者纠正/澄清对评审结果的误解和解释，信息资产负责人可以依据审核员的建议采取相应措施。审核员宜在评审报告定稿前把在此过程中被修改过的、增强的或者新增的控制措施重新评审一遍。将最终报告提交给管理层意味着信息安全控制措施评审的正式结束。

因为评审结果最终影响信息安全控制措施的内容、行动计划和里程碑，信息资产负责人要核对审核员的发现，并与管理层共同确定改正评审中已确定的脆弱性的适当步骤。通过使用满意和不满意的标记，报告评审发现的形式为管理层提供了关于特定弱点和信息安全缺陷信息，有助于按照信息安全风险管理的规程采取制度化和结构化的方法来降低风险。例如，信息资产负责人经与管理层协商可决定某些标记为不满足的评审发现是不重要的，并不会给组织带来重大的风险。反之，信息资产负责人和管理者可能决定某些标记为不满足的评审发现是重要的，需要立即采取补救措施。总之，组织核对审核员发现的不满足证据，并就评审发现的严重程度和重要性(即，对组织的业务、资产、个人或其他组织的潜在不利影响)进行判断，并判定该评审发现是否值得进一步调查或需要采取补救措施。高级管理层参与降低风险的过程可能是必要的，以确保组织资产按照组织优先级来分配，将资源首先分配给组织中支持最多关键业务的信息资产，或者分配给纠正导致最大风险缺陷的信息资产。最后根据评审发现，由信息资产负责人与组织指定的负责人协商发起的降低风险的措施，使得信息安全风险管理过程和信息安全控制措施得以更新。于是，管理人员更新用于判定信息资产安全状态的关键文件以反映新的评审结果。

在预先确定的里程碑或评审后的固定周期，例如最终报告完成后的三个月，通常会进行一次跟踪评审，重点关注那些待解决的或“没有定论”的问题。包括验证以往评审发现实施方案的有效性。组织也可选择在下次评审时执行跟踪评审，特别是针对那些非关键或不紧急的问题。

# 附 录 A
（资料性附录）
技术符合性检查实践指南

本附录使用 GB/T 22081—2008 中描述的典型控制措施为技术符合性检查提供一套实践指南。

本附录中的每一种控制措施基本上按照以下陈述和指南的结构来组织。

“技术控制措施”(带“附加技术信息”)

1 安全实现标准(带“安全实现标准技术注解”)

1.1 实践指南、设想的证据、方法

1.2 实践指南、设想的证据、方法

1.3

2 安全实现标准(带“安全实现标准技术注解”)

2.1 实践指南、设想的证据、方法

2.2 实践指南、设想的证据、方法

2.3

每个技术控制措施都有附加的技术信息，以便为审核员提供更多的支持。它基本上由一系列“安全实现标准”组成，这些标准宜由组织定期评审以证实适用的标准是否被适当地实现和运行。

每个“安全实现标准”有补充的“安全实现标准技术注解”，以便为评审过程提供更多的技术信息。它还提供了一系列的“实践指南”“设想的证据”和“方法”。

“实践指南”为安全实现标准提供了符合性检查规程。“设想的证据”给出了一些系统、文件、文档或其他项目的例子，可被作为符合性检查规程中的“证据”来接受。请注意组织中证据的名称可能会不同。然而，本附录中使用的名称可被认为在技术符合性检查领域中普遍接受的。“方法”提供了一种与以上实践指南一致的合适的技术符合性检查方法。

本附录不提供全部的技术符合性检查实践指南，但仍将尽最大可能帮助组织评审安全实现标准是否被适当地实现、运行。

| A.1 防范恶意代码控制措施的技术性检查 | |
|---|---|
| 控制措施 | GB/T 22081—2008 10.4.1 控制措施恶意代码<br>宜实现防范恶意代码的检测、防御和恢复控制措施以及适当的用户意识规程 |
| 附加技术信息 | 恶意代码(恶意软件)是一个通用术语，用来指包括软件、程序、脚本在内的，旨在通过信息窃取、欺诈、间谍、破坏及恶意毁坏计算机系统的代码。<br>当恶意软件被植入计算机系统后，该系统可能被破坏，或系统中的信息被窃取。这种行为也可能危害其他系统。<br>恶意软件包括计算机病毒、蠕虫、木马、僵尸、间谍软件、欺诈广告和其他恶意和非期望的软件。<br>在组织网络接入互联网的情况下，审核员宜评审安置在互联网边界的检测/预防恶意软件的功能是全面有效的，且这些功能适当地工作。<br>特别说明，评审检测/预防功能是否适当工作，审核员必须确认用来检测恶意软件的模式文件或者电子签章已经更新。<br>其中一些检测/预防系统被设计为使用模式文件和电子签章来检测恶意软件，另外一些被设计为不使用模式文件和电子签章的系统来检测计算机系统异常行为。<br>因为有一些连接互联网模式，例如通过网关，组织的网络连接到国际互联网，或者每台个人电脑直接连接到互联网，审核员宜确保检测/防御系统在每个情况下适当工作。<br>注：审核员宜意识到检测/预防系统的能力对于未知恶意软件的如 Zero day 的攻击是有限的。 |

| | | | |
|---|---|---|---|
| 1 | 安全实现标准 | 安装和定期更新恶意代码检测和修复软件以扫描计算机和介质文件作为预防性或常规性控制措施;实施的检查宜包括:<br>a) 在使用前检查所有电子或者光媒体文件和从网络接收的文件是否含有恶意代码。<br>b) 使用前检查电子邮件附件和下载文件是否含有恶意代码;这个检查宜在不同地方进行,例如,电子邮件服务器、桌面计算机和接入组织网络时。<br>c) 检查网页是否含有恶意代码 | |
| | 安全实现标准技术注解 | 在网关中,组织网络入口处,检测/预防恶意软件系统宜相适当地支持跨越网络边界的服务或协议,如 WWW、Mail 和 FTP 等 | |
| | 1.1 | 实践指南 | 以下实践指南分别适用于安全实现标准中的 a)、b)、c)。<br>a) 通过系统规范和网络图解的评审,检查恶意代码和修复系统对电子和光媒体文件和通过网络接收的文件都是全面和有效地存在。<br>审核员宜通过审计系统规范和网络图解来检查检测/预防系统是否全面和有效地存在。<br>b) 通过系统规范和网络图解的评审(包括电子邮件服务器、台式计算机和网关)来检查所有电子邮件附件和下载文件的检测恶意代码和修复系统是否全面和有效地部署。<br>系统规范有时清晰描述作为专用设备的检测恶意代码和修复系统,但是,审核员关注同样被安装在旨在提供一些其他功能/服务(WWW、Mail 和 FTP)的服务器中的信息,而它本身就未在系统规范中清楚说明。<br>对于台式个人计算机,审核员关注系统规范中没有清楚说明的检测恶意代码和修复系统。<br>c) 通过包括 web 服务器的系统规范和网络图解的评审检查检测恶意代码和修复系统对 web 页面全面和有效。<br>对于用于检查和浏览 web 页面的台式个人计算机,审核员关注本身就在系统规范中没有清楚说明的检测恶意代码和修复系统。在这种情况下,检测恶意代码和修复系统可能固化在浏览器中。<br>对于 web 服务器来说,检测恶意代码和修复系统作为专用设备有时在系统规范中被清楚描述,然而,审核员宜关注安装在 web 服务器中并未在系统规范中清楚说明的这些专用设备 |
| | | 设想的证据 | 系统规范,网络图解 |
| | | 方法 | 检查/评审 |
| | 1.2 | 实践指南 | 以下实践指南分别适用于安全实现标准中的 a)、b)、c)。<br>a) 通过观察信息处理设施来检查检测恶意代码和修复系统已被部署,并且正常检测所有电子或光媒体文件和通过网络接收的文件。<br>检查管理软件在管理检测恶意代码和修复系统的集成系统中是否正常的工作。<br>b) 通过观察信息处理设施如抽样的台式机和网关,检查安装的病毒防护和修复系统,并确认其正常防护任何电子邮件附件、下载的文件。<br>对于电子邮件,检查检测系统的工作不仅仅针对附件,同样针对 html 邮件中的恶意代码。<br>c) 通过观察信息处理设施来检查对检测 web 页面正常的工作的检测恶意代码和修复系统是存在的。<br>对于用于检查和浏览 web 页面的桌面个人计算机,检查针对未授权的 Active X 控件,脚本的检测系统。<br>对于 web 服务器,检查检测系统不仅仅针对 html 文件,同样针对 web 服务中的恶意代码,如 apache、IIS 等 |

| | | | |
|---|---|---|---|
| 1 | 1.2 | 设想的证据 | 检测恶意代码和修复系统设施是存在的，例如：<br>a) 文件服务器；<br>b) 电子邮件服务器；<br>c) 抽样台式个人计算机；<br>d) 手提电脑；<br>e) 安装了专用的检测恶意代码和修复系统的网关(组织内网和互联网边界间)；<br>f) Web 服务器；<br>g) 代理服务器；<br>h) Web 浏览器；<br>i) 其他设备(物理上阻止 USB 适用的设备) |
| | | 方法 | 检查/观察 |
| | 1.3 | 实践指南 | 收集检测和修复系统的日志文件，并且检查日志的记录以证明当检测出恶意软件时候系统已运行且必要的功能已执行。<br>注：对于台式个人计算机，检测和修复系统的输出日志被存储在个人计算机中。对于服务器和外部设备，日志有时通过传输协议(如 syslog)传送并存储于其他系统。<br>对于用于检查和浏览 web 页面的台式个人计算机，web 浏览器中检测功能可能不能生成表明这些功能已经运行的日志记录，相反，大多数浏览器都能显示检测到未授权的脚本的消息 |
| | | 设想的证据 | a) 运行的检测系统；<br>b) 检测系统输出的日志文件；<br>c) 检测系统报警记录；<br>d) 检测系统在 web 浏览器中的信息 |
| | | 方法 | 检查/观察 |
| 2 | 安全实现标准 | 扫描计算机和媒体的恶意代码检测和修复软件作为预防控制措施，宜定期更新和正常工作 | |
| | 安全实现标准技术注解 | 在大部分情况下，应该有自动升级模式文件或者电子签章的功能 | |
| | 2.1 | 实践指南 | 检查自动或规则的恶意代码检测和升级软件补丁文件或电子签章的设计 |
| | | 设想的证据 | 检测系统的设计或说明书 |
| | | 方法 | 检查/评审 |
| | 2.2 | 实践指南 | 检查自动或规则的恶意代码检测和升级软件补丁文件或电子签章的设置 |
| | | 设想的证据 | 检测系统的设置 |
| | | 方法 | 检查/观察 |
| | 2.3 | 实践指南 | 通过观察产品名称、版本和模式文件或者电子签章的更新日志，以检查模式文件或者电子签章是否已经更新。<br>注：可能会在产品的帮助文件中观察到检测和修复系统的产品名称和版本的信息。 |
| | | 设想的证据 | 检测/预防系统信息，例如：<br>a) 产品名称；<br>b) 产品版本；<br>c) 模式文件/电子签章版本 |
| | | 方法 | 检查/观察 |

| A.2 审计记录控制措施的技术性检查 | | |
|---|---|---|
| 控制措施 | GB/T 22081—2008 10.10.1 审计记录<br>宜产生记录用户活动、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措施监视 | |
| 附加技术信息 | 检测未授权的信息处理活动，记录审核日志对追踪用户活动、系统运行、安全事件和系统是非常重要的。<br>审核日志宜包括以下信息以分析是否为未授权活动、安全事件：<br>a) 用户 ID；<br>b) 日期和时间；<br>c) 关键事件，如登录和退出；<br>d) 终端标识；<br>e) 网络地址和协议。<br>为生成包含上述信息的必要记录，产生这些日志的设备宜被调整或设置一些规则。<br>产生日志的方法取决于系统的结构、架构和实现的应用程序。<br>审核员宜考虑不同的系统结构使用不同的记录日志方法，例如服务器和 PC。<br>注：<br>相关系统结构例子：<br>a) 客户机/服务器系统(C/S 系统)；<br>b) 服务器/浏览器系统；<br>c) 瘦客户端系统；<br>d) 虚拟化；<br>e) ASP 应用(应用服务提供商)，SaaS(软件即服务)或云计算。<br>相关的系统架构例子：<br>a) UNIX、Linux；<br>b) Windows；<br>c) 大型机。<br>相关的日志类型例子：<br>a) 系统日志；<br>b) 应用日志。 | |
| 1 | 安全实现标准 | 审核日志记录用户行为、异常和信息安全事件。审核日志宜包括：<br>a) 用户 ID；<br>b) 关键事件的日期、时间和细节，例如登录和退出；<br>c) 终端身份与位置的信息。(若有可能)；<br>d) 成功的和被拒绝的对系统尝试访问的记录；<br>e) 成功的和被拒绝的对数据以及其他资源的尝试访问记录；<br>f) 系统配置的变更；<br>g) 特殊权限的使用；<br>h) 系统实用工具盒应用程序的实用；<br>i) 访问的文件和访问类型；<br>j) 网络地址和协议；<br>k) 访问控制措施系统引发的警报；<br>l) 保护系统的激活和停用，例如防病毒系统和入侵检测系统 |
| | 安全实现标准技术注解 | 为找出安全事件和发生原因，审核员检查和分析操作系统的状态，使用和改变日志记录。为调查研究事件和事故因果关系，需要结合多系统的审核日志。为此目的，从系统结构/架构/配置来理解日志文件的位置和类型是非常重要 |

| | | | |
|---|---|---|---|
| 1 | 1.1 | 实践指南 | 检查系统日志的设计基于安全实现准则 |
| | | 设想的证据 | a) 文档规范；<br>b) 需求定义文档；<br>c) 软件设计文档 |
| | | 方法 | 检查/评审 |
| | 1.2 | 实践指南 | 检查系统配置文件设置的日志是否与系统设计文件中所描述的相一致 |
| | | 设想的证据 | a) 软件设计文档；<br>b) 系统配置文件 |
| | | 方法 | 检查/观察 |
| | 1.3 | 实践指南 | 检查实际审核日志文件的记录是否与系统设计文档中所描述的相一致。<br>注：在审核日志中，有些记录经常性出现，有些记录则不，例如错误记录。为了检查系统是否对特殊情况进行记录，审核员可能需要使用各种测量方法，包括产生测试案例，检查系统设计文档。 |
| | | 设想的证据 | 日志文件 |
| | | 方法 | 检查/观察 |
| | 1.4 | 实践指南 | 检查审核日志的记录完整性以判断日志是否适当。<br>注：即使日志设置适当，也会有一些宜记录在审核日志中的记录因为性能不足、系统能力或其他的原因而丢失。 |
| | | 设想的证据 | 日志文件 |
| | | 方法 | 检查/观察 |
| 2 | 安全实现标准 | 审核日志宜按约定周期保存，以便将来调查研究和访问控制措施监控 | |
| | 安全实现标准技术注解 | 在一些情况下，审核日志的保存周期设定依据业务目的、合同和法律法规。例如，包括系统访问控制措施警报信息的审核日志宜保存到对事件和事故的调查完成。<br>注：对于刚运行的相对新的系统，审核日志未按约定周期保存。这种情况下，需完成下面的实践指南 2.3，需检查实践指南 2.1、2.3。 | |
| | 2.1 | 实践指南 | 检查审核日志的保存期是否与系统设计文档中所描述的相一致 |
| | | 设想的证据 | a) 日志文件；<br>b) 系统设计文档 |
| | | 方法 | 检查/观察 |
| | 2.2 | 实践指南 | 检查系统的审核日志的保存期设置是否与系统设计文档中所描述的相一致，或存储周期未应用前，设置覆盖不擦除审核日志 |
| | | 设想的证据 | a) 日志文件；<br>b) 系统设计文档 |
| | | 方法 | 检查/观察 |
| | 2.3 | 实践指南 | 通过观察日志文件的时间戳或日志中记录的时间，检查存储周期是否长于协议的周期 |
| | | 设想的证据 | a) 日志文件；<br>b) 系统设计文档 |
| | | 方法 | 检查/观察 |

<table>
<tr><td colspan="4">A.3　特殊权限管理控制措施的技术性检查</td></tr>
<tr><td>控制措施</td><td colspan="3">GB/T 22081—2008 11.2.2 特殊权限管理<br>宜限制和控制特殊权限的分配及使用</td></tr>
<tr><td>附加技术信息</td><td colspan="3">特殊权限管理是重要的，因为特殊权限的不当使用会对系统造成重大影响。<br>特殊权限的分配状态宜在定义特殊权限的文档（特殊权限定义文件）中予以描述。因为每个系统产品（操作系统、数据管理系统和每个应用程序）中相关的访问权限是不同的。<br>不同类型的特殊权限的示例有：<br>a)　超级用户（UNIX、LINUX）；<br>b)　管理员（Windows）；<br>c)　备份操作员（Windows）；<br>d)　高级用户（Windows）；<br>e)　系统管理员（数据库管理系统）；和<br>f)　数据库管理员（数据库管理系统）。<br>特殊权限的分配宜在使用需求的基础上最小化。此外，也没有必要不断地分配特殊权限。<br>不同系统的特殊权限管理方法不同。基于系统的特殊权限管理例子：<br>a)　操作系统中，ACL（访问控制措施列表）定义特殊权限；<br>b)　数据库管理系统中，定义各种默认权限；<br>c)　在应用程序中，可能会定义各种应用程序管理功能的默认权限，所以审核员宜提前确定检查级别；<br>d)　安全操作系统中有强制访问控制措施的功能</td></tr>
<tr><td rowspan="6">1</td><td>安全实现标准</td><td colspan="2">每个系统产品相关的访问权限（例如：操作系统。数据库管理系统和每个应用程序）及需要分配这些权限的用户宜予识别</td></tr>
<tr><td>安全实现标准技术注解</td><td colspan="2">宜对特殊权限用户的活动进行监控，因为特殊权限的不当使用会对系统造成显著的影响。如果系统架构不同，则检测不当使用特殊权限的方法也不同。<br>注：有代表性的系统架构是：<br>a)　大型机；<br>b)　Windows；<br>c)　UNIX、Linux；<br>d)　安全操作系统。</td></tr>
<tr><td rowspan="3">1.1</td><td>实践指南</td><td>检查特殊权限定义文档中已描述的特殊权限的分配</td></tr>
<tr><td>设想的证据</td><td>特殊权限定义文档</td></tr>
<tr><td>方法</td><td>检查/观察</td></tr>
<tr><td rowspan="3">1.2</td><td>实践指南</td><td>检查系统配置的设置是否与特殊权限定义文档中所描述的相一致。不同系统架构中检查特殊权限操作的方法不同。<br>特殊权限操作检查方法示例：<br>a)　（大型机例子）通过检查 RACF（资源访问控制措施程序）报告检查特殊权限应用状态是否适宜。<br>b)　（UNIX、LINUX 或 Windows）通过调查现实使用特殊权限的日志检查特殊权限使用状态是否适宜。<br>注：<br>a)　RACF（资源访问控制措施程序）是大型机的安全管理中间件。<br>b)　在 UNIX 或 LINUX，仅通过超级用户的登录来调查超级用户不当使用是危险的。因为一般用户在登录 UNIX 或 Linux 后通过使用“su”命令转变成超级用户。</td></tr>
<tr><td>设想的证据</td><td>特殊权限定义文档；<br>访问控制措施列表；<br>RACF（资源访问控制措施程序）报告</td></tr>
<tr><td>方法</td><td>检查/观察</td></tr>
</table>

| | | | |
|---|---|---|---|
| 2 | 安全实现标准 | 分配了特殊权限的用户 ID 宜与一般业务使用所用的 ID 不同 | |
| | 安全实现标准技术注解 | 对于特殊权限的访问，有可能是未经授权的操作，因而有规律地使用特殊权限就成了未经授权进行访问的温床。<br>如果操作不需要特殊权限，用户宜使用普通账户。如果允许使用“超级用户”权限登录，那就不能通过日志识别哪个用户登录了系统 | |
| | 2.1 | 实践指南 | 通过观察系统的 ACLs 检查特权用户在特权账户外是否有普通用户账户 |
| | | 设想的证据 | 访问控制措施列表 |
| | | 方法 | 检查/观察 |
| | 2.2 | 实践指南 | 根据观察日志文件检查特殊权限使用不同的用户账号用于正常业务。<br>在使用 UNIX 或 Linux 的情况下，检查系统配置提示系统拒绝以“超级用户”的身份登录。<br>注：<br>当日志表明特殊权限仅使用特权账号时，审核员宜尝试通过访谈来检查特殊权限使用不同用户账号用于正常业务。 |
| | | 设想的证据 | a) 日志文件；<br>b) “超级用户”登录系统配置 |
| | | 方法 | 检查/观察 |

| A.4 备份控制措施的技术性检查 | |
|---|---|
| 控制措施 | GB/T 22081—2008 10.5.1 信息备份<br>宜按照已设的备份策略，定期备份和测试信息和软件 |
| 附加技术信息 | 进行适当备份，宜按备份策略定义组织标准，并宜在备份设计文档中体现组织标准。<br>备份用于在出现数据损失（如灾难或媒介失效）时恢复核心信息或软件。<br>当组织设计备份时，宜依照组织备份策略选择备份地点、备份路径和备份方法。<br>就备份地点而言，组织宜选择现场或异地作为备份地点。一般认为现场备份在进行备份操作和恢复操作时比异地备份迅速。一般选用异地备份以预防本地灾难的影响，例如火灾、洪水或地震。<br>就备份路径而言，要选择离线还是在线。在线备份的数据是通过网络或通信线路备份的。离线备份的备份数据是通过移动介质以物理形式转移的，例如 DLTs 或 CD/DVD。<br>备份方法被分为几种方式，例如全数据备份、增量备份和差异备份。<br>全数据备份对所有选择备份的数据进行备份。全数据备份比其他备份方式需要更多的时间和数据存储容量，但它是数据恢复最简单和容易的方法。<br>增量备份是对上次备份后所有发生变化的数据进行备份。增量备份比其他方法需要更少的时间和数据存储容量，但它的数据恢复方式最复杂。<br>差异备份对上一次全数据备份发生变化的数据进行备份。它比全数据备份需要更少的时间和数据存储容量，比增量备份对数据的恢复更简单和容易 |

| | | | |
|---|---|---|---|
| 1 | 安全实现标准 | 备份范围(如全数据备份或差异备份)和频率宜反映组织业务需求、所涉及的信息安全要求和组织持续运行的关键性信息 | |
| | 安全实现标准技术注解 | 依据业务需求,组织宜选择充分备份/恢复时间和数据存储容量用于备份。评估人员宜对满足组织业务需求的备份方法进行评估。<br>相关的备份频率的示例:<br>a) 镜像或实时复制(当信息的关键程度最高级时);<br>b) 每天(当需要对至少一天内备份的数据进行恢复时);<br>c) 每周;<br>d) 每月 | |
| | 1.1 | 实践指南 | 检查备份的设计是基于安全实现标准 |
| | | 设想的证据 | a) 备份规范文档;<br>b) 业务需求和安全需求定义文档;<br>c) 备份设计文档 |
| | | 方法 | 检查/评审 |
| | 1.2 | 实践指南 | 检查用于备份的系统配置文件的设置是否与设计文档中关于备份所描述的相一致 |
| | | 设想的证据 | a) 备份设计文档;<br>b) 备份系统配置文件 |
| | | 方法 | 检查/评审 |
| | 1.3 | 实践指南 | 检查已按备份设计文档的说明进行备份 |
| | | 设想的证据 | a) 备份设计文档;<br>b) 日志文件;<br>c) 备份介质 |
| | | 方法 | 检查/观察 |
| 2 | 安全实现标准 | 宜定期检查和测试数据恢复程序以确保其有效并能在操作程序分配恢复的时间内完成 | |
| | 安全实现标准技术注解 | 所采取的备份方式不同,数据恢复的复杂程度和需要的时间也不同;例如全数据或者差分备份。<br>测试和检查恢复程序的计划宜予编制并形成文件 | |
| | 2.1 | 实践指南 | 检查测试和检查的计划得到定期检查 |
| | | 设想的证据 | 检查测试和检查计划的记录 |
| | | 方法 | 检查/评审 |
| | 2.2 | 实践指南 | 检查测试和检查计划已经定期测试以确保其有效的且能在操作程序分配恢复的时间内完成 |
| | | 设想的证据 | a) 恢复测试的记录;<br>b) 测试和检查计划 |
| | | 方法 | 检查/评审 |

| A.5 网络安全管理控制措施的技术性检查 | | | |
|---|---|---|---|
| 控制措施 | | GB/T 22081—2008 10.6.2 网络服务安全<br>安全特性、服务级别以及所有网络服务的管理要求宜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 | |
| 附加技术注解 | | 网络服务是一种在网络计算环境中提供的服务，无论是组织内部提供的还是外包的。当一个组织使用网络服务时，可能会通过外包的网络服务方式传送组织的机密信息。因此，评审人员宜关注外包网络服务商提供的如加密和/或身份认证等必要的安全功能。<br>用于网络服务的系统的示例：<br>a) 域名系统(DNS)；<br>b) 动态主配设置协议(DHCP)；<br>c) 防火墙/虚拟专用网络(Firewall/VPN)；<br>d) 反病毒检测器(Anti Virus detector)；<br>e) 入侵检测系统/入侵防护系统(IDS/IPS) | |
| 1 | 安全实现标准 | 宜确定对于特定服务所必要的安全准备工作，例如安全特性、服务级别和管理要求。组织宜确保网络提供商实现了这些措施 | |
| | 安全实现标准技术注解 | 使用网络服务时，安全准备工作对保护网络上传输的信息是重要的。<br>与安全特性相关的需求通常包含在业务需求中。<br>以下给出了与网络服务相关的安全特性的示例：<br>a) 加密，防止窃听；<br>b) 网络接入控制措施，以防止未经授权的访问；<br>c) IDS/IPS，打击恶意活动；<br>d) URL 过滤，以防止未经授权的 web 访问；<br>e) 针对突发安全事件的事件响应 | |
| | 1.1 | 实践指南 | 检查服务提供商提供的包括 SLA(服务级别协议)的合同文件是否满足业务、法律和安全要求 |
| | | 设想的证据 | a) 合同文件；<br>b) 需求定义文档 |
| | | 方法 | 检查/评审 |
| | 1.2 | 实践指南 | 组织内部提供网络服务时，检查网络服务的系统设置是否与网络服务设计文档中所描述的相一致 |
| | | 设想的证据 | a) 系统配置；<br>b) 网络服务设计文档 |
| | | 方法 | 检查/评审 |
| | 1.3 | 实践指南 | 组织内部提供网络服务时，检查网络服务系统的实际日志文件记录是否与网络服务设计文档中的描述相一致。<br>网络服务的记录的例子：<br>a) 身份鉴别；<br>b) 加密；<br>c) 网络连接控制措施；<br>d) 网络速度；<br>e) 响应(使用在线系统时)；<br>f) 宕机时长 |
| | | 设想的证据 | a) 日志文件；<br>b) 报警信息；<br>c) 网络服务设计文档 |
| | | 方法 | 检查/观察 |

| A.6 用户职责控制措施技术性检查 | | | |
|---|---|---|---|
| 控制措施 | | | GB/T 22081—2008 11.3.1 口令使用<br>宜要求用户在选择及使用口令时，遵循良好的安全习惯 |
| 附加技术注解 | | | 为防止对计算机资源的未授权访问，宜建立口令，且口令对那些无权限访问资源的人保密。<br>口令验证是对多个资源所使用的一种用户验证的方法，如操作系统、程序、数据库、网络或 web 站点。口令的质量取决于字符的长度和类型，如字母、数字和符号。<br>一些操作系统可能会为用户配置口令策略的参数，如 Windows。此外，应用开发商可开发验证功能以配置口令策略。<br>评审员宜评估口令验证功能被有效地部署在计算机资源中，并且这些功能发挥了适当的作用 |
| 1 | 安全实现标准 | | 选择有足够最小长度的有质量的口令：<br>a) 易于记忆；<br>b) 不能基于那些别人通过运用与个人相关信息便可轻易猜测出或获得的信息，如：名字、电话号码和生日等；<br>c) 不易遭受字典攻击(即，不是由字典中的单词所组成的)；<br>d) 无连续相同，全数字的或者全字母的字符 |
| | 安全实现标准技术注解 | | 通常，容易被其他的用户记住的口令对都是脆弱的 |
| | 1.1 | 实践指南 | 检查组织口令策略中描述的选择口令的原则 |
| | | 设想的证据 | 组织口令策略 |
| | | 方法 | 检查/评审 |
| | 1.2 | 实践指南 | 检查系统配置的设置(系统口令策略)是否与组织口令策略中所描述的相一致 |
| | | 设想的证据 | a) 系统配置(系统口令策略)；<br>b) 组织的口令策略 |
| | | 方法 | 检查/观察 |
| | 1.3 | 实践指南 | 检查日志文件是否显示用户更改过口令 |
| | | 设想的证据 | 日志文件 |
| | | 方法 | 检查/观察 |

# 附 录 B
（资料性附录）
初始信息收集（除信息技术以外）

信息安全审核组组长宜在相应信息安全领域分配有相应能力和经验的信息安全控制措施评审审核员。

相关职员的初始问题包括但不限于以下例子。

## B.1 人力资源和安全

a) 相关人员是否能对其行为负责或承担义务？
b) 相关人员是否具有信息和信息安全常识、并能解答相关问题，激励他人并提供必要的指导？
c) 申请策略和规程是否清晰，是否明确、可测量、可接受、可实现？
d) 已受聘雇员是否具备组织期望的“运行”知识？
e) 组织是否信任接触可能危及组织生存的信息和系统的相关人员？
f) 相关人员是否值得信任？
g) 这种信任是如何被组织进行定义和测量的？

## B.2 策略

a) 分层次
   i. 信息安全方针是否与组织业务目标和总体安全策略保持一致？
   ii. 如何使信息技术、人力资源和获取方针联系在一起？
b) 综合
   i. 这些方针是否能够覆盖组织所有业务活动区域的信息安全（人力资源、物理环境、信息技术、销售、制造、研发和合同安全等）？
   ii. 这些方针是否被设计成能够完整涵盖组织战略、战术和运营？
c) 规划
   i. 这些方针是直接使用了 GB/T 22081—2008 的相关内容，还是针对特定的背景对控制措施目标和控制措施进行了剪裁？
   ii. 这些方针是否以书面形式明确了执行者的职责？
   iii. 在一个策略中有一个期望活动，或者有一套考虑谁、何时、为什么、什么、哪里、如何等的基础性问题的规程：
      1) 如果没有定义执行活动人员的职责，由谁来负责达成这组目标？
      2) 如果没有定义何时执行活动，是否能保证其按时启动和完成？
      3) 如果一个活动的目的和目标没有被定义，这个活动为什么会被正确理解，其重要性为什么会被充分考虑到？
      4) 如果没有定义活动的内容，如何知道应该做什么？
      5) 如果一个活动没有定义目标、执行地点、操作规程和信息资产，或者没有定义其效果控制措施，如何使它有效（地点）？
      6) 一个规程中的活动如果没有明确定义如何被完成，如何保证其能被正确执行（方式）？
      7) 如果一个活动没有定义指标和控制措施点，以验证其是否正确包含并且达到其既定目

标，如何确保或能够达成组织目标？

ⅳ. 是否有控制措施和检测环境，以鉴定组织策略声明强制执行、实现和可达成既定目标？

ⅴ. 在策略声明中的目标陈述宜考虑 SMART 准则，否则：

1） 没有明确目标则不容易被清晰地辨识，并且未达成目标的责任也无法落实到人；

2） 如果目标不可测量，组织一般无法验证目标的达成程度；

3） 如果目标没有在组织内进行充分沟通并达成共识，则可能造成对控制措施的被误解、被规避或被中断；

4） 如果组织不是根据自身的实际能力来确定目标，很可能因不切合实际而不能达到；

5） 如果组织没有确认实现方针目标的预期起始和结束时间点，就很可能无法确保组织能够采取实际的行动，达成目标也难以实现。

## B.3 组织

a） 是否考虑了在组织的特定环境和限制条件的情况下对组织人员角色和职责进行充分且必要定义和分配，以满足组织的业务目标？

b） 是否与外部机构保持联系？

c） 组织是否对自身没有能力承担的安全管理责任进行了外包？

d） 合同是否阐述信息安全的相关要求？

## B.4 物理和环境安全

### B.4.1 工作场所能否保证信息的安全？

a） “区域”

ⅰ. 业务区与公众访问区是否充分隔离？

ⅱ. 是否在定义了敏感信息处置的范围（通过人员和信息通信技术系统）？

ⅲ. 这些“安全区”是否被恰当地隔离，以避免其相互间的敏感信息交换？

b） 位置

ⅰ. 不同安全级别的区域是否被明确标识，并合理部署？

ⅱ. 保护信息资产的边界（墙、天花板、地板等）和适当保护强度是否被清晰地定义？

ⅲ. 区域是否被适当地进行了标识，且关键区域标识对“外部”不可见？

c） “出入口”

ⅰ. 当门窗或其他非固定边界处于关闭状态时，能否提供与固定边界相当的防护能力？

ⅱ. 是否对这些位置的进出采取适当的访问控制措施？

ⅲ. 是否有防入侵系统？

ⅳ. 是否有“紧急出口”，以保证信息、人和设备具有充足的移动性？

d） 走廊和“通道”

ⅰ. 去往固定区域或位置的通道是否得到识别？

1） 人员的通道；

2） 缆线的通道（传输信息）。

ⅱ. 是否有供选择的通道？

ⅲ. 这些“通道”是否受到保护和监控？

e） 监控

ⅰ. 监控设备能否在不被发现的情况下正常工作？

ii. 监控设备能否发现远处的入侵?
iii. 监控何时启动?
iv. 监控记录在何地和如何保存和分析?

f) 装置
i. 适合于信息存储?
ii. 是否被放置在正确的地方?
iii. 实际运行是否和预期的结果一致?

### B.4.2 工作场所能否保证信息通信技术(ICT)的安全?(环境方面)

a) 电力设施
i. 足够/适当?
ii. 备用?
b) 空调设施
i. 足够/适当?
ii. 备用?
c) 防火设施
i. 足够/适当?
ii. 备用?

### B.4.3 工作场所能否保证人员的安全?

a) 有紧急出口(并且采取了适当的控制措施)?
b) 是否存在电、水、气体、液体的泄漏等造成人员伤害的潜在风险?
c) 是否存在在温度、湿度、材料和震动的潜在风险?
d) 是否配备了避免区域内人员受伤的器材?
e) 是否安装了避免区域内人员受伤的"门"?
f) 是否安装和维护了避免区域内人员受伤的器材?

## B.5 事件管理

a) 是否定义了信息安全事件?
b) 是否有响应信息安全事件的能力:
i. 指南或手册?
ii. 职责和角色?
iii. 处理方式和资源?

## 参 考 文 献

[1] GB/T 19011—2003 质量和(或)环境管理体系审核指南(ISO 19011:2002,IDT)

[2] GB/T 22080—2008 信息技术 安全技术 信息安全管理体系 要求(ISO/IEC 27001:2005,IDT)

[3] 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)

[4] GB/T 25067—2010 信息技术 安全技术 信息安全管理体系审核认证机构的要求(ISO/IEC 27006:2007,IDT)

[5] ISO/IEC 27004:2006 信息技术 安全技术 信息安全管理 测量(Information technology—Security techniques—Information security management—Measurement)

[6] ISO/IEC 27005:2011 信息技术 安全技术 信息安全风险管理(Information technology—Security techniques—Information security risk management)

[7] ISO/IEC 27007:2011 信息技术 安全技术 信息安全管理体系审核指南(Information technology—Security techniques—Guidelines for intormation security management systems auditing)

[8] ISO 指南 73:2009 风险管理 词汇(Risk management—Vocabulary)

[9] NIST 特定出版物(SP)800-53A,联邦信息系统控制措施评审指南,2008 年 7 月,http://csrc.nist.gov/publications/PubsSPs.html

[10] 安全与开放方法研究会(ISECOM),开源安全测试方法手册,http://www.isecom.org/osstmm/

[11] 联邦信息安全办公室(BSI),德国,标准 100-1,信息安全管理系统(ISMS);100-2,IT-Grundschutz 方法;100-3,基于 IT-Grundschutz 和 IT-Grundschutz 目录的风险分析(德语版和英语版),https://www.bsi.bund.de/cln_174/EN/Publications/publications_node.html

[12] 信息安全论坛(ISF),信息安全最佳实践标准,2007,https://www.securityforum.org/services/publicresearch/