国际标准

ISO/IEC 27003

第二版

2017-03-01

信息技术-安全技术-信息安全管理体系-指南

参考编号
ISO/IEC 27003:2017(E)

目录

前言

ISO（国际标准化组织）和 IEC（国际电工委员会）形成了全球标准化专业系统。作为 ISO 或 IEC 成员的国家机构通过由各自组织设立的技术委员会来参与国际标准的制定，以处理特定的技术活动领域。ISO 和 IEC 技术委员会在共同关心的领域进行合作。其他国际组织、政府和非政府组织，通过联络 ISO 和 IEC 也参加了这项工作。在信息技术领域，ISO 和 IEC 建立了联合技术委员会 ISO/IEC JTC 1。

用于开发本文件的程序和用于进一步维护的程序在 ISO/IEC 准则第 1 部分中有所描述。特别是应注意不同类型文件所需的不同批准标准。本文件是根据 ISO/IEC 准则第 2 部分的编辑规则（见 www.iso.org/directives）起草的。

请注意本文件的某些内容可能是专利权的主题的可能性。ISO 和 IEC 不负责确定任何或所有这些专利权。在文件开发过程中确定的任何专利权利的细节将在引用和/或 ISO 所收到的专利声明列表中（见 www.iso.org/patents）。

本文档中使用的任何商品名称是为了方便用户而提供的信息，不构成背书。

对于标准的自愿性质的解释、与合格评定有关的 ISO 特定术语和表达的含义、以及关于 ISO 在技术性贸易壁垒（TBT）中遵守世界贸易组织（WTO）原则的信息，请参阅以下 URL：www.iso.org/iso/foreword.html。

负责本文件的委员会是 ISO/IEC JTC 1 信息技术，小组委员会 SC 27 IT 安全技术。

本第二版的 ISO/IEC 27003 取消并取代第二版（ISO/IEC 27003：2010），这是一个较小的修订。

相比以前的版本，主要的变化如下：

— 范围和标题已经改为涵盖 ISO/IEC 27001：2013 的要求的解释和指南，而不是以前的版本（iso / iec 27001：2005）；

— 结构现在与 ISO/IEC 27001:2013 的结构一致，使用户更容易与 ISO/IEC 27001:2013 一起使用；

— 之前的版本有一个带有活动顺序的项目方法。这个版本反而提供对要求的指南，而不考虑它们实现的顺序。

引言

本文件就 ISO/IEC 27001 中规定的信息安全管理体系（ISMS）的要求提供指南，并提供有关它们的建议（“should”）、可能性（“can”）和许可（“may”）。本文档的意图不是要提供关于信息安全所有方面的通用指南。

本文件的第 4 至 10 章映射了 ISO/IEC 27001：2013 的结构。

本文件不增加对 ISMS 及其相关术语和定义的新要求。有关要求和定义，组织宜参考 ISO/IEC 27001 和 ISO/IEC 27000。实施 ISMS 的组织没有义务遵守本文档中的指南。

ISMS 强调以下几个阶段的重要性：

— 理解组织的需求和建立信息安全方针和信息安全目标的必要性;

— 评估组织与信息安全相关的风险;

— 实施和运行信息安全过程、控制和其他措施来处理风险;

— 监视和评估 ISMS 的性能和有效性;和

— 实践持续改进。

ISMS 与任何其他类型的管理体系类似，包括以下关键组件：

a) 方针;

b) 有明确责任的人员;

c) 有关以下内容的管理过程：

1) 方针制定;

2) 意识和能力的规定;

3) 规划;

4) 实现;

5) 运行

6) 绩效考核

7) 管理评审;和

8) 改进;及

d) 文件化信息

ISMS 还有其他关键组件，如：

e) 信息安全风险评估;和

f) 信息安全风险处置，包括控制措施的确定和实施。

本文件是通用的，旨在适用于所有组织，不论其类型、大小或性质。组织宜根据其特定的组织环境来确定本的哪一部分适用于自己(见 ISO/IEC 27001:2013，条款 4)。

例如，某些指南可能更适合于大型组织，而对于非常小的组织（例如少于 10 人），某些指南可能是不必要的或不适当的。

条款 4 至 10 的描述结构如下：

— **要求的活动**：介绍在 ISO/IEC 27001 的相应条款中要求的关键活动;

— **解释**：讲解 ISO/IEC 27001 的要求意味着什么;

— **指南**：提供更详细的或支持性的信息来执行“要求的活动”，包括实施的例子

— **其他信息**：提供可以考虑的进一步的信息。

ISO/IEC 27003，ISO/IEC 27004 和 ISO/IEC 27005 形成了一套文件支持 ISO/IEC 27001：2013，并提供指南。在这些文件中，ISO/IEC 27003 是为 ISO/IEC 27001 的所有要求提供指南的基本和全面的文件，但没有关于“监视、测量、分析和评价”以及信息安全风险管理的详细描述。ISO/IEC 27004 和 ISO/IEC 27005 侧重于具体内容和对“监视、测量、分析和评价”以及信息安全风险管理给予更为详细的指南。

在 ISO/IEC 27001 中有几处明确提及的文件化信息。然而，组织可以保留额外的文件化信息，当其确定对管理体系的有效性以及作为响应 ISO/IEC 27001：2013,7.5 b)的一部分是必要的。在这种情况下，本文件使用惯用语“有关此活动和它的结果的文件化信息，只有在形式和程度上该组织确定对其管理体系的有效性是必要的才是强制性的（见 ISO/IEC 27001：2013，7.5.1 h))

信息技术-安全技术-
信息安全管理体系-指南

1. 范围

本文件提供有关 ISO/IEC 27001:2013 的解释和指南。

2. 规范性引用文件

以下文件在本文件中被引用，其部分或全部内容构成本文件的要求。凡是注明日期的引用文件，仅注明日期的版本适用。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用。

ISO/IEC 27000：2016，信息技术-安全技术-信息安全管理系统-概述和词汇

ISO/IEC 27001：2013，信息技术-安全技术-信息安全管理体系-要求

3. 术语和定义

ISO/IEC 27000：2016 给出的术语和定义适用于本文件。

国际标准化组织和国际电工委员会维护用于标准化的术语数据库，地址如下：

- IEC Electropedia：http://www.electropedia.org/

- ISO 在线浏览平台：http://www.iso.org/obp

4. 组织背景

4.1.理解组织及其背景

需要的活动

组织确定关于其目标和影响其实现信息安全管理体系（ISMS）预期成果的能力的外部和内部问题。

解释

作为 ISMS 的一个必须功能，组织不断地分析自己和周围的世界。这种分析涉及外部和内部问题，这些问题在某种程度上影响信息安全,以及信息安全如何管理，并且与组织目标有关。

这些问题的分析有三个目的：

- 理解背景以决定 ISMS 的范围;
- 分析背景以确定风险和机会;和
- 确保 ISMS 适应变化中的外部和内部问题。

外部问题是那些超出组织控制范围的问题，这通常被称为组织的环境。分析这个环境可能（can）包括以下几个方面：

a) 社会和文化;
b) 政治，法律，规范和监管;
c) 财务和宏观经济;
d) 技术;
e) 自然; 和
f) 竞争力。

组织环境的这些方面不断出现影响信息安全和信息安全如何管理的问题。相关的外部问题取决于组织的具体优先事项和情况。

例如，特定组织的外部问题可能（can）包括：

g) 使用外包 IT 服务的法律影响（法律方面）;
h) 在火灾、洪水和地震等灾害的可能性方面的自然特征（自然方面）;
i) 黑客工具的技术进步和密码学的使用（技术方面）;和

j）对组织服务的普遍要求（社会，文化或财务方面）。

内部问题受制于组织的控制，分析内部问题可能（can）包括以下几个方面：

k）组织的文化;
l）方针、目标和实现它们的战略;
m）管理方式、组织结构、角色和责任;
n）组织采用的标准、准则和模型;
o）可能直接影响 ISMS 范围内的组织过程的合同关系;
p）过程和规程;
q）资源和知识（例如资本，时间，人员，流程，系统和技术）方面的能力;
r）物理基础设施和环境;
s）信息系统、信息流和决策过程（正式和非正式）;和
t）以前的审计和以前的风险评估结果。

这个活动的结果在 4J，61 和 9.3 中使用。

指南

基于对组织目标（例如使命声明或经营计划）以及组织 ISMS 的预期成果的理解，组织宜（should）：

- 审查外部环境，识别相关的外部问题;和
- 审查内部方面，识别相关的内部问题。

为了找出相关问题，下面的问题可能（can）被提问：某个类别的问题（见上面的 a）到 t））如何影响信息安全目标？内部问题的三个例子可以作为例证：

例子 1，关于治理和组织结构（见条款 m））：在建立 ISMS 时，宜（should）考虑已有的治理和组织结构。例如，组织可能（can）基于其他已有的管理体系的结构对其 ISMS 的结构进行建模，并且可能（can）整合共同的功能，例如管理评审和审计。

例子 2，关于方针、目标和战略（见条款 1)）：对现有方针、目标和战略的分析可以表明该组织打算实现什么，以及如何使信息安全目标与业务目标保持一致，以确保成功的结果。

例子 3，关于信息系统和信息流（见条款 s)）：在确定内部问题时，组织宜（should）在足够的详细程度上确定其各个信息系统之间的信息流。

此活动及其结果的文件化信息仅在形式上或是到了组织确定对其管理体系有效性是必要的程度时是强制性的（见 ISO/IEC 27001：2013,7.5.1 b))

其他信息

在 ISO/IEC 27000 中，“组织”的定义有一个注释：“组织概念包括但不限于独资经营者、公司、有限责任公司、商行、企（事）业单位、行政权力机构、合营公司、慈善机构或社会事业机构，或其部分或组合，不论其是否法人组织，不论是公有还是私有。”其中一些例子是完整的法律实体，而另一些则不是。

有四种情况：

1) 组织是一个法律或行政实体（例如独资经营者、公司、有限责任公司、商行、企（事）业单位、行政权力机构、合营公司、慈善或社会事件机构，无论是否法人，公立或私立）；
2) 组织是法律或行政实体的子集（例如公司、有限责任公司、企（事）业单位的一部分）；
3) 组织是一组法律或行政实体(例如独资经营者、大公司、有限责任公司、商行的组合)。 和
4) 组织是一组法律或行政实体（如俱乐部，行业协会）的子集。

4.2.理解相关方的需要和期望

需要的活动

组织确定与 ISMS 相关的相关方及其与信息安全相关的要求。

解释

相关方是一个已定义的术语（参见 ISO/IEC 27000：2016,2.41），指的是可能影响、被影响、或意识到自己受到组织的决策和活动影响的个人或组织。相关方可能（can）在组织外部和内部找到，并且可能(can)对组织的信息安全有特定的需要、期望或要求。

外部相关方可能（can）包括：

a) 监管者和立法者;
b) 股东，包括所有者和投资者;
c) 供应商，包括分包商、顾问和外包合作伙伴;
d) 行业协会;
e) 竞争者;
f) 顾客和消费者;和
g) 维权组织。

内部相关方可能（can）包括：

h) 决策者，包括最高管理者;
i) 过程所有者、系统所有者和信息所有者;
j) 支持职能，如：IT 或人力资源等;
k) 员工和用户;和
l) 信息安全专业人员。

这个活动的结果在 43 和 6.1 中使用。

指南

宜（should）采取以下步骤：

- 识别外部相关方;
- 识别内部相关方; 和

- 识别相关方的要求。

随着相关方的需要、期望和要求随着时间的推移而变化，这些变化及其对 ISMS 范围、约束和要求的影响宜（should）定期审查。

此活动及其结果的文件化信息仅在形式上或是到了组织确定对其管理体系有效性是必要的程度时是强制性的（见 ISO/IEC 27001：2013,7.5.1 b））。

其他信息

没有其他信息。

4.3.确定信息安全管理体系的范围

需要的活动

组织确定 ISMS 的边界和适用性，以确立其范围。

解释

这个范围定义了 ISMS 到底适用于哪里和什么，以及哪里和什么是不适用的。

因此，确立范围是为实施 ISMS 的所有其他活动确定必要基础的关键活动。例如，风险评估和风险处置，包括控制的确定，如果对 ISMS 究竟适用于哪里没有准确的理解，就不会产生有效的结果。准确认识 ISMS 的边界和适用性以及组织与其他组织之间的接口和依赖关系也是至关重要的。对范围的任何后期修改都可能导致大量额外的工作量和成本。

以下因素可能（can）影响范围的确定：

a) 4A 中描述的外部和内部问题;
b) 根据 ISO/IEC 27001：2013,4.2 确定的相关方及其要求;
c) 业务活动的准备作为 ISMS 覆盖范围的一部分包括在内;

d) 所有支持职能，即支持这些业务活动所必要的职能（例如人力资源管理、信息技术服务和软件应用、建筑设施管理、物理区域，公共基础服务和公用事业）;和

e) 被外包给组织内的其他部门或独立供应商的所有职能。

从一个实施到另一个实施，ISMS 的范围可能非常不同。例如，范围可以包括：

- 一个或多个特定过程;
- 一个或多个特定职能;
- 一项或多项特定服务;
- 一个或多个特定部门或场所;
- 整个法律实体;和
- 整个行政实体和一个或多个供应商。

指南

为了确立 ISMS 的范围，可能采取多步骤的方法：

f) 确定初步范围：这项活动宜（should)由一小组有代表性的管理者代表指挥;

g) 确定精细范围：宜（should)审查初步范围内外的职能单位，也许随后包括或排除某些职能单位，以减少边界接口的数量。在提炼初步范围时，宜（should)考虑范围内支持业务活动所必要的所有支持职能;

h) 确定最终范围：精细范围应由所有管理层在精细范围内进行评价。若有必要，应进行调整，然后进行精确描述;和

i) 批准范围：描述范围的文件化信息宜(should)由最高管理层正式批准。

组织还宜(should)考虑对 ISMS 或对组织内的其他部门或独立供应商的外包活动产生影响的活动。对于这些活动，宜（should)识别接口（物理、技术和组织）和它们对范围的影响。

描述范围的文件化信息宜（should)包括：

j） 组织范围、边界和接口;

k） 信息和通信技术的范围、边界和接口;和

l） 物理范围、界限和接口。

其他信息

无其他信息。

4.4.信息安全管理体系

需要的活动

组织建立、实施、维护和持续改进 ISMS。

解释

ISO/IEC 27001：2013 4.4 规定了建立、实施、维护和持续改进 ISMS 的核心要求。ISO/IEC 27001 的其他部分描述了 ISMS 的要求要素，4.4 要求组织确保满足为了建立、实施、维护和持续改进 ISMS 的所有要求要素。

指南

无具体指南

其他信息

无其他信息。

5. 领导

5.1.领导和承诺

需要的活动

最高管理层证实重视 ISMS 的领导和承诺。

解释

领导和承诺对于有效的 ISMS 至关重要。

最高管理层（见 ISO/IEC 27000）被定义为指导和控制 ISMS 最高层组织的个人或群体，即最高管理层对 ISMS 负总体责任，这意味着最高管理层指导 ISMS 与组织中的其他领域类似，比如分配和监控预算的方式，最高管理层可以代表组织的权力，为实际执行有关信息安全和 ISMS 的活动提供资源，但仍然保留总体责任。

例如，实施和运营 ISMS 的组织可以是更大组织内的业务单位。在这种情况下，最高管理层是指导和控制该业务部门的个人或群体。

最高管理层也参与管理评审（见 9.3）和促进持续改进（见 10.2），

指南

最高管理层宜（should)通过以下方式提供领导和展示承诺：

a) 最高管理层宜（should)确保信息安全方针和信息安全目标的确立，并与组织的战略方向相一致;
b) 具有指定的流程责任人的组织可以将实施适用的要求的职责授权给这些个人或群体。克服组织改变过程和控制的阻力也可能(can）需要最高管理层的支持;
c) 最高管理层宜(should)确保有效的 ISMS 的资源的可用性。资源是 ISMS 的建立、及其实施、维护和改进，以及实施信息安全控制所需要的。ISMS 所需的资源包括：

    1) 财务资源;
    2) 人员;
    3) 设施; 和

4) 技术基础设施。

所需资源取决于组织的背景，如规模、复杂性以及内部和外部的要求。管理评审宜（should）提供信息指明资源对组织是否是充足的;、

d) 最高管理层宜（should)传达组织的信息安全管理需要以及符合 ISMS 要求的需要。这可以通过给出实际的例子来说明在组织背景下的实际需要是什么，以及通过传达信息安全要求来完成;
e) 最高管理层宜（should）通过支持所有信息安全管理过程的实施，特别是通过要求和审查 ISMS 的状态和有效性的报告来确保 ISMS 实现其预期结果（参见 5.3b))。 这些报告可以从测量（见 6.2 b）和 9.1 a))、管理评审和审计报告中得出。最高层管理层可能还要为参与 ISMS 的关键人员设定绩效目标;
f) 最高管理层宜指导和支持组织内直接参与信息安全和 ISMS 的人员。如果不这样做，可能会对 ISMS 的有效性有负面影响。最高管理层的反馈可能包括计划的活动如何与组织的战略需求相一致，也可以为 ISMS 中的不同活动划分优先顺序;
g) 最高管理层宜在管理评审期间评估资源需求，并为持续改进和监视计划活动的有效性设定目标;和
h) 最高管理层宜支持已被分配涉及信息安全管理角色和责任的人员，以便他们有动力并能够指导和支持他们领域内的信息安全活动。

如果实施和运营 ISMS 的组织是一个更大的组织的一部分，领导和承诺可以通过接触控制和指导更大组织的人员或群体来改善。如果他们理解实施 ISMS 所涉及的内容，他们可以在 ISMS 范围内为最高管理层提供支持，并帮助他们提供领导力和证实对 ISMS 的承诺。例如，如果 ISMS 范围之外的相关方参与有关信息安全目标和风险准则的决策，并且保持对 ISMS 产生的信息安全结果的警觉，则他们关于资源分配的决定可以与 ISMS 的要求保持一致。

其他信息

无其他信息

5.2.方针

需要的活动

最高管理层建立信息安全方针

解释

信息安全方针描述了 ISMS 对组织的战略重要性，并作为文件化信息是可用的。该方针指导组织的信息安全活动。

方针规定了在组织的实际背景下，信息安全的需求是什么。

指南

信息安全方针宜包含有关信息安全的意图和方向的简要、高层次的声明。它可以是一个 ISMS 的特定的范围，也可以有更广泛的覆盖范围。

有关信息安全的所有其他方针、过程、活动和目标宜与信息安全方针一致。

信息安全方针宜反映组织的业务状况、文化、问题以及与信息安全有关的关注点。信息安全方针的程度宜符合组织的宗旨和文化，并宜在便于阅读和完整性之间寻求一个平衡点。重要的是，方针的用户能够认同方针的战略方向。

信息安全方针可能包括组织的信息安全目标，或者描述如何设定信息安全目标的框架(即，谁为 ISMS 设置它们，以及它们应该如何在 ISMS 范围内被部署)。例如，在非常大的组织中，高层次的目标应该由整个组织的最高管理层设定，然后根据信息安全方针中建立的框架，目标宜在一定程度上详述，以给所有相关方以方向感。

信息安全方针宜括来自最高管理层的对其满足信息安全相关的要求的承诺的明确声明。

信息安全方针宜包括最高管理层支持所有活动的持续改进的明确声明。在方针中阐明这一原则是很重要的，以便 ISMS 范围内的人员都意识到这一点。

信息安全方针宜传达给 ISMS 范围内的所有人。因此，它的格式和语言宜是适当的，以便所有的接受者都能容易理解。

最高管理层宜决定应向哪些相关方传达方针。信息安全方针可以用将其与组织外部的相关方联系起来的方式来写。这些外部相关方的例子有：客户、供应商、承包商、分包商和监管机构。如果信息安全方针向外部相关方提供，则不宜包括机密信息。

信息安全方针可以是单独的独立方针，也可以包括在一个涵盖组织内的多个管理体系主题的全面的方针中，（例如质量、环境和信息安全）。

信息安全方针宜作为文件化信息提供。ISO/IEC 27001 中的要求并不意味着这些文件化信息有任何特定的形式，因此由组织决定哪种形式是最合适的。如果组织有一个方针的标准模板，信息安全方针的形式宜使用此模板。

其他信息

有关信息安全政策的进一步信息可以在 ISO/IEC 27002 中找到。

有关信息安全方针与方针框架内其他方针之间关系的进一步信息可以在附录 A 中找到。

5.3.组织角色、责任和权力

需要的活动

最高管理层确保与信息安全相关的角色的责任和权限分配和传达至整个组织。

解释

最高管理层确保与信息安全相关的角色和责任以及必要的权力得到分配和传达。

这个要求的目的是分配责任和权限，以确保 ISMS 符合 ISO / IEC 27001 的要求，并确保向最高管理层报告 ISMS 的性能。

指南

最高管理层宜有条不紊地确保 ISMS 的责任和权限得到分配，以使管理体系满足 ISO/IEC 27001 中规定的要求。最高管理层不需要指定所有的角色、责任和权力，但是宜充分授权去做这个。最高管理者宜批准 ISMS 的主要角色、职责任和权力。

与信息安全活动有关的责任和权力宜被分配。活动包括：

a) 配合 ISMS 的建立、实施、维护、绩效报告和改进;
b) 就信息安全风险评估和处置提供建议;
c) 设计信息安全过程和制度;
d) 制定有关信息安全控制的确定、配置和运行的标准;
e) 管理信息安全事件;和
f) 审查和审计 ISMS。

除了有关信息安全的特有角色之外，有关的信息安全责任和权力宜包含在其他角色之中。例如，信息安全责任可以被纳入以下角色：

g) 信息所有者;
h) 过程所有者;
i) 资产所有者（例如应用程序或基础设施所有者）;
j) 风险所有者;
k) 信息安全协调职能或人员（这个特定角色通常是 ISMS 的支持角色）;
l) 项目经理;
m) 部门经理;和

n) 信息使用者。

此活动及其结果的文件化信息仅在形式上或是到了组织确定对其管理体系有效性是必要的程度时是强制性的[见 ISO/IEC 27001：2013,7.5.1 b))。

其他信息

无其他信息。

6. 规划

6.1.应对风险和机会的行动

6.1.1. 总则

概述

ISO/IEC 27001：2013 6.1 是关于应对有关 ISMS 的所有类型的风险和机会的行动规划。这包括风险评估和风险处置计划。

规划过程中，构成 ISO/IEC 27001 的细分风险分为两类：

a) 与 ISMS 整体的预期成果相关的风险和机会;和
b) 与 ISMS 范围内信息的机密性、完整性和可用性的损失相关的信息安全风险。

第一类宜按照 ISO/IEC 27001：2013，6.1.1（总则）中规定的要求进行处理。属于这一类的风险可能是与 ISMS 本身、ISMS 范围定义、最高管理层对信息安全的承诺、ISMS 运营资源等相关的风险。属于这一类的机会可能是与 ISMS 成果、ISMS 的经济价值，运行 ISMS 过程和信息安全控制的功效等。

第二类由与 ISMS 范围内信息的机密性、完整性和可用性的损失直接相关的所有风险组成。这些风险宜根据 6.1.2（信息安全风险评估）和 6.1.3（信息安全风险处处置）进行处理。

组织可以（may)选择对每个类别使用不同的技术。

应对风险的要求分支可解释如下：

- 鼓励兼容组织整合了不同主题（如：质量，环境和信息安全）的管理体系中的其他管理体系标准;
- 要求组织明确并应用完整和详细的信息安全风险评估和处置过程;和
- 强调信息安全风险管理是 ISMS 的核心要素。

ISO/IEC 27001：2013 6.1.1 使用“确定风险和机会”和“处理这些风险和机会”的表述。“确定（determine)”一词可以被认为等同于 ISO/IEC 27001：2013 中 6.1.2 中使用的“评估(assess)”一词（即:识别、分析和评价)。同样，“处理（address)”一词可以被认为等同与 ISO/IEC 27001：2013 6.1.3 中使用的“处置（treat）”一词。

需要的活动

规划 ISMS 时，组织就 4.1 中提到的问题和 4.2 中提到的要求确定风险和机会。

解释

对于在关 ISMS 预期成果的风险和机会，组织基于内部和外部问题（见 4.1）和相关方的要求（见 4.2）来确定它们。然后组织规则划它的 ISMS：

a) 确保 ISMS 实现预期的成果，例如，信息安全风险为风险所有者所知悉，并被处置至可接受的水平;
b) 防止或减少有关 ISMS 的预期成果的非期望的风险影响;和
c) 实现持续改进（见 10.2)。例如，通过适当的机制来检测和纠正管理过程中的弱点或者抓住改进信息安全的机会。

与上述 a）相关的风险可能是流程和责任不明确、员工意识淡薄、管理层参与不力等。与上述 b）相关的风险可能是风险管理不力或风险意识不足。与上述 c）相关的风险可能是对 ISMS 文件和过程的管理不善。

当组织在其活动中寻求机会时，这些活动就会影响组织的背景（ISO / IEC 27001：2013,4.1）和相关方的需求和期望（ISO / IEC 27001：2013,4.2），以及改变对组织的风险。这样的机会的例子可能是：将其业务集中在产品或服务的某些领域、为某些地理区域建立营销策略，或扩大与其他组织的业务伙伴关系。

机会也存在于 ISMS 过程和文件的持续改进，以及 ISMS 实现的预期结果的评估中。例如，考虑一个相对较新的 ISMS，往往会通过澄清接口、减少管理开销、消除不具成本效益的部分过程，通过细化文件和引入新的信息技术，来识别改进过程的机会。

6.1.1 中的计划包括确定：

d) 应对风险和机遇的行动;和
e) 下面的方法：

1) 将这些行动整合并实施到 ISMS 过程中;和
2) 评价这些行动的有效性。

指南

组织宜：

f) 考虑 4.1 中提到的问题和 4.2 中提到的要求，确定可能影响 a)、b）和 c）中描述的目标的实现的风险和机会;和
g) 制定计划来执行确定的行动并评价这些行动的有效性；宜考虑规划行动将信息安全过程和文件整合进现有的体系;所有这些行动都与信息安全目标（6.2）联系在一起，对信息安全风险进行评估和处理（见 6.1.2 和 6.1.3）的。

ISO/IEC 27001：2013 10.2 中规定的持续改进 ISMS 的总体要求被 6.1.1 给出的实现持续改进和 ISO/IEC 27001：2013，5.1 g)、5.2 d)、9.1、9.2 和 9.3 中的其他相关要求所支持。

6.1.1 所要求的行动在战略层面、战术层面和操作层面、不同地点、不同服务或系统都可能有所不同。

可以采取数种方法来满足 6.1.1 的要求。其中两种是：

- 分别从信息安全风险角度考虑与规划、实施和运行 ISMS 相关联的风险和机会，和
- 同时考虑所有风险。

将 ISMS 整合到已建立的管理体系中的组织可能发现，组织现有的业务规划方法论能满足 6.1.1 的要求。在这种情况下，宜仔细核实该方法论覆盖了 6.1.1 的所有要求。

此活动及其结果的文件化信息仅在形式上或是到了组织确定对其管理体系有效性是必要的程度时是强制性的（见 ISO/IEC 27001：2013,7.5.1 b)）

其他信息

关于风险管理的进一步信息可以在 ISO 31000 中找到。

注：术语“风险”被定义为“不确定性对目标的影响”（见 ISO/IEC 27000：2016,2.68)。

6.1.2. 信息安全风险评估

需要的活动

组织定义并应用信息安全风险评估过程。

解释

该组织定义信息安全风险评估过程：

a) 建立和维护：

1) 风险接受准则;和
2) 执行信息安全风险评估的准则，其中可能包括评估后果和可能性的准则，以及确定风险级别的规则;和

b) 确保重复的信息安全风险评估产生一致的、有效的和可比较的结果。

然后，信息安全风险评估过程将在以下子过程中进行定义：

c) 信息安全风险的识别：

1) 识别与 ISMS 范围内信息的机密性、完整性和可用性损失相关的风险;和
2) 识别与这些风险相关的风险所有者，即，识别并指定具有管理已识别风险的适当权力和责任的人员。

d) 信息安全风险分析：

1) 评估所识别的风险成为现实时的潜在后果，例如，直接的业务影响，如金钱损失，或间接的业务影响，如声誉损害。评估后果可以用定量或定性的值来报告;
2) 用定量（即机率或频率）或定性的值，评估已识别的风险发生的现实可能性;和
3) 将已识别的风险的级别确定为一个评定的后果和评定的可能性的预定义组合;

e) 信息安全风险评价：

1) 将风险分析的结果与之前建立的风险接受准则进行比较;和
2) 优先对风险处置进行分析风险，即确定被认为是不可接受的风险的处置紧迫性，以及如果多个风险需要处置，则进行排序。

然后应用信息安全风险评估过程。

信息安全风险评估过程（6.1.2a）至 e））的所有步骤及其应用结果均由组织作为文件化信息保留。

指南

关于建立风险准则的指南（6.1.2a））

信息安全风险准则宜根据组织的背景和利益相关方的要求来建立，一方面宜根据最高管理层的风险偏好和风险认知来定义，另一方面宜允许一个可行的和适当的风险管理过程。

信息安全风险准则宜联系 ISMS 的预期结果来建立。

根据 ISO/IEC 27001：2013 6.1.2 a），宜建立考虑可能性和后果评估的关于信息安全风险评估的准则。并且，宜建立风险接受准则。

在建立评估信息安全风险的后果和可能性的准则之后，组织还宜建立一种将它们结合起来以确定风险等级的方法。后果和可能性可以（may）以定性、定量或半定量的方式表示。

风险接受准则涉及风险评估（在评价阶段，此时，组织宜了解风险是否可以接受）和风险处置活动（此时，组织宜理解提议的风险处置是否足以达到可接受的风险水平）。

风险接受准则可能是基于可接受风险的最高级别、成本效益考虑或对组织的后果。

风险接受标准宜由负有责任的管理者批准。

产生一致的、有效的和可比较的评估结果的指南（6.1.2 b））

风险评估过程应基于设计的足够详细的方法和工具，以便得出一致的、有效的和可比较的结果。

无论选择何种方法，信息安全风险评估过程应确保：

- 所有的风险都在需要的细节层面上被考虑;
- 其结果是一致的和可重复的（即风险的识别，其分析和评估可以被第三方理解，并且当不同的人在相同情况下评估风险时结果是相同的)。和
- 重复的风险评估的结果是可比较的（即可以了解风险水平是增加的还是减少的)。

当整个或部分信息安全风险评估过程重复时，结果前后矛盾或不一致，可能表明所选择的风险评估方法是不适当的。

信息安全风险识别指南（6.1.2c))

风险识别是发现、辨别和描述风险的过程。这包括识别风险来源、事态、其原因和其潜在后果。

风险识别的目的是基于那些可能引起、提高、阻碍、降低、加速或延迟实现信息安全目标的事态，形成全面的风险清单。

通常使用两种方法来识别信息安全风险：

- 基于事态的方法：以通用的方式考虑风险来源。考虑的事态可能发生在过去，或者可预见的未来。第一种情况可能涉及历史数据，第二种情况可能基于理论分析和专家意见
- 基于资产、威胁和脆弱性识别的方法：考虑两种不同类型的风险来源：具有内在脆弱性的资产和威胁。这里考虑的潜在事态是威胁来如何利用资产的某些脆弱性来影响组织的目标。

这两种方法都符合 ISO 31000 中关于风险评估的工作原理和通用指导原则。

其它风险识别方法也可以被使用，如果其被证明具有类似的实际作用，并且能够确保 6.1.2 b)）中的要求。

注：基于资产、威胁和脆弱性的方法符合和兼容 ISO/IEC 27001 中要求的信息安全风险识别方法，以确保以前的风险识别投资不会浪费。

不建议在第一轮风险评估中风险识别过于详细。对信息安全风险有一个高层次的清晰的画像远比根本没有画像好。

信息安全风险分析指南（6.1.2 d)）

风险分析的目标是确定风险级别。

ISO 31000 在 ISO/IEC 27001 中作为通用模型被引用。ISO/IEC 27001 要求，对于每个已识别的风险，风险分析是基于风险导致的后果的评估并评估这些后果发生的可能性来确定风险级别。

基于后果和可能性的风险分析技术可能是：

1) 定性，使用一个限定属性的尺度（如高、中、低）;
2) 定量，使用一个数值尺度（如货币成本、发生频率或机率）;或者
3) 半定量，使用具有指定值的定性尺度。

无论使用哪种风险分析技术，都宜考虑其客观性水平。

有多种分析风险的方法。提到的两种方法（基于事态的方法和基于资产、威胁和脆弱性识别的方法）可能对信息安全风险分析是适合的。当有关风险的讨论在专家的帮助下进行时，风险识别和分析过程可能是最有效的。

信息安全风险评价指南（6.1.2e)）

对已分析的风险的评价涉及使用组织的决策过程来比较每个风险已评估的风险级别与预先确定的接收准则，以确定风险处置选项。

风险评估的最后一步是根据 6.1.2a）所定义的接受准则，验证前一步分析过的风险是否可以接受，还是需要进一步的处置。 6.1.2 d）中的步骤提供了关于风险重要程度的信息，但没有提供有关实施风险处理选项的紧迫性的直接信息。依据据风险发生的条件，他们可能有不同的处置优先级。因此，这一步骤的输出宜是按优先顺序排列的风险清单。这有利于保留来自风险识别和风险分析步骤中的进一步信息，以支持风险处置的决策。

其他信息

ISO/IEC 27005 为执行信息安全风险评估提供指导。

6.1.3. 信息安全风险处置

需要的活动

组织定义和应用信息安全风险处置过程。

解释

信息安全风险处置是选择风险处置选项、确定适当的控制去实施这些选项、确切地描述风险处置计划，以及获得风险所有者对风险处置计划的批准的整体过程。

信息安全风险处置过程（6.1.3a）至 f））的所有步骤及其应用结果由组织作为文件化信息保留。

指南

信息安全风险处置选项的指南（6.1.3a））

风险处置选项是：

a) 通过决定不开始或不继续引起风险的活动或移除风险来源（例如：关闭电子商务门户）来规避风险;

b) 冒额外的风险或增加风险以谋求业务机会（例如：开设电子商务门户）;
c) 通过改变可能性（例如减少脆弱性）或后果（例如多元化资产）或这两者来缓解风险;
d) 通过保险、分包或风险融资与其他方分担风险;和
e) 基于风险接受准则或通过知情决定（例如维持现有的电子商务门户）保留风险。

为了满足风险接受准则，每个单独的风险宜通过一个或多个这些选项处理至与信息安全目标一致。

确定必要的控制的指导（6.1.3 b））

宜给予确定必要的信息安全控制特别的关注。任何控制宜基于之前评估的信息安全风险来确定。如果组织的信息安全风险评估是糟糕的，那么它选择信息安全控制的基础也是糟糕的。

适当的控制决定确保：

f) 包括所有必要的控制，并且没有不必要的控制被选择;和
g) 必要的控制的设计达到适当的广度和深度。

糟糕的控制选择的后果是，所提出的信息安全风险处置可能是：

h) 无效的;或者
i) 效率低下和不合理地昂贵。

为确保信息安全风险处置的有效性和高效性，能够证明从必要的控制到风险评估和风险处置过程的结果之间的关系是非常重要的。

使用多个控制来实现对信息安全风险处置的要求可能是必要的。例如，如果选择改变特定事态的后果的选项，则可能需要控制以及时检测事态，以及需要控制以响应事态并从事态中恢复。

当确定控制时，组织还应顾及到来自外部供应商的服务（例如应用、过程和功能）所需的控制。通常，这些控制是通过写入与这些供应商的协议中的信息安全要求来委托的，包括获取有关这些要求被满足到什么程度的信息的方法（如审计权}。可以有这样的情况，即组织希望确定和描述详细的控制作为其自己的ISMS 的一部分，即使这些控制是由外部供应商执行的。

独立于所采取的方法，组织总是宜在确定对其 ISMS 的控制时考虑其供应商所需的控制。

比较控制与 ISO/IEC 27001：2013 附录 A（6.1.3 c））中的控制的指导。

ISO/IEC 27001：2013，附录 A 包含了控制目标和控制的综合清单。这个文件的使用者被引导到 ISO/IEC 27001：2013 附录 A 中的控制的通用陈述，以确保没有忽略必要的控制。与 ISO/IEC 27001：2013 附录 A 对照，还可能识别出哪些可能在缓解信息安全风险上更有效的替代 6.1.3 b）中确定的控制的替代控制。

控制目标隐含在控制选择中。ISO/IEC 27001：2013 附录 A 中列出的控制目标和控制并不是详尽无遗的，宜根据需要增加额外的控制目标和控制。

并不是 ISO/IEC 27001：2013 附录 A 中的每一项控制都需要被包括在内。任何 ISO/IEC 27001：2013 附录 A 中无助于缓解风险的控制都宜被排除，并宜给出排除的正当理由。

产生适用性声明（SoA）（6.1.3 d））的指南

SoA 包含：

- 所有必要的控制（在 6.1.3 b）和 6.1.3 c）中所确定的），并对每一个控制：
  - 控制被包含进来的正当理由;和
  - 控制是否得到执行（例如，全面执行、正在进行、尚未开始）；
- 排除 ISO/IEC 27001：2013 附录 A 中任何控制的正当理由。

将一个控制包含在内的正当理由部分依赖于控制在缓解信息安全风险方面的作用。信息安全风险评估结果和信息安全风险处置计划的引用宜是充分的，连同必要的控制的实施所预期的信息安全风险缓解。

排除一个包含在 ISO/IEC 27001：2013 附录 A 中的控制的理由，可能包括以下内容：

- 已经确定控制对实施选择的信息安全风险处置选项控制是不必要;
- 控制是不适用的，因为它在 ISMS 的范围之外（例如如果所有组织的系统开发都是在内部进行的，则 ISO/IEC 27001：2013，A.14.2.7 外包开发是不适用的）。和
- 它是被自定义的控制消除的（例如，如果自定义控制阻止使用可移动媒体，ISO/IEC 27001：2013 A.8.3.1 可移除媒体的管理能够被排除）。

注：自定义控制是不包含在 ISO/IEC 27001：2013 附录 A 中的控制。

一个有用的 SoA 可能是作为一个表格来生成，其中包含 ISO/IEC 27001：2013 附录 A 中的所有 114 个控制，以及在 ISO/IEC 27001：2013 附录 A 中未提及的额外控制（如果需要的话）。表中的一列可能表明一个控制对实施风险处置选项是否是必要的或者是可以排除的。下一列可能包括包含或排除一个控制的理由。表中的最后一列可能表明控制的当前的实现状态。可以使用更多列，例如 ISO/IEC 27001 中未要求的但常常用于随后的评审的细节;这些细节可能是对如何实施控制的更详细的描述，或者是对更详细的描述和文件化信息的交叉引用，或者是与实施控制相关的策略。

虽然它不是 ISO/IEC 27001 的具体要求，但是组织可能发现它对包含在 SoA 中的每个控制的操作责任是有用的。

制定信息安全风险处置计划（6.1.3e））的指南

ISO/IEC 27001 没有规定信息安全风险处理计划的结构或内容。不管怎样，宜从 6.1.3 a）至 c）的输出中制定计划。因此，该计划应记录每一个处理过的风险：

- 选定的处置选项;
- 必要的控制;和
- 执行状态。

其他有用的内容可能包括：

- 风险所有者;和
- 实施行动后的预期残余风险。

如果风险处置计划要求采取任何行动，那么宜规划指出责任和期限（见 6.2）：这些行动计划可能用这些行动的清单来表示。

一个有用的信息安全风险处置计划可能被设计成一个按风险评估期间风险识别分类的表格，显示所有确定的控制。作为一个例子，在这个表格中可能有一列标明负责提供控制的人员的姓名。更多的列可以标明控制的实施日期、关于控制（或过程）打算如何操作的信息以及关于目标实施状态的列。

作为风险处理过程的一部分的一个例子，考虑盗窃手机。后果是可用性的丧失和潜在的不受欢迎的信息披露。如果风险的评估显示风险水平超出了接受范围，组织可能决定改变可能性或者改变风险的后果。

为了改变手机丢失或被盗的可能性，组织可能确定一个合适的控制是强制员工通过移动设备策略来保管手机，并定期检查是否有损失。

为了改变手机丢失或被盗的后果，组织可能确定像这样的控制：

- 用户可以报告丢失的事件管理过程;
- 移动设备管理（MDM）解决方案，用于删除丢失手机中的内容;和
- 用于恢复手机内容的移动设备的备份计划。

在准备 SoA （6.1.3 d)）时，组织可能纳入其选择的控制（移动设备策略和 MDM, Mobile Device Management)，基于其改变手机丢失或盗窃可能性和后果的影响对将其纳入做出解释，从而减少剩余风险。

将这些控制与 ISO/IEC 27001：2013 附录 A（6.1.3c）中列出的控制进行比较，可以看出移动设备策略与 ISO/IEC 27001：2013，A.6.2.1 一致，但是 MDM 控制不直接一致，其宜被视为一个额外的自定义控制。如果将 MDM 和其他控制被确定为组织的信息安全风险处置计划中的必要的控制，则宜将其纳入 SoA（参见“生成 SoA 指南”（6.1.3d))。

如果组织想要进一步降低风险，它可能从 ISO/IEC 27001：2013，A.9.1.1（访问控制策略）考虑它缺乏对移动电话的访问的控制，并修改其移动设备策略以强制使用所有手机上的 PIN 码。这宜是改变手机丢失或被盗的后果的进一步的控制。

在制定信息安全风险处理计划（6.1.3e）时，组织宜纳入实施移动设备策略和 MDM 的行动，并分配责任和时间计划。

获得风险所有者批准的指南（6.1.3 f))

在制定信息安全风险处置计划时，组织宜获得风险所有者的授权。这种授权宜基于已定义的风险接受准则或任何偏离的有正当理由的让步。

通过其管理过程，组织宜记录风险所有者对残余风险的接受和管理层对风险处置计划的批准。

作为一个例子，可以通过标明控制的效用、残余风险和风险所有者的批准的列来改良在 6.1.3 e 指导中描述的风险处置计划，使风险所有者的批准是有案可查的。

其他信息

关于风险处置计划的进一步信息可以在 ISO/IEC 27005 和 ISO 31000 中找到。

6.2.信息安全目标和实现目标的计划

需要的活动

组织建立信息安全目标和在相关的职能和层级实现这些目标的计划。

解释

信息安全目标有助于实现组织的战略目标，以及实现信息安全方针。因此，ISMS 中的目标是关于信息的机密性、完整性和可用性的信息安全目标。信息安全目标也有助于按照信息安全方针（见 5.2）来规定和测量信息安全控制和过程的性能。

组织计划、建立和发布相关职能和层级的信息安全目标。

ISO/IEC 27001 中关于信息安全目标的要求适用于所有的信息安全目标。如果信息安全方针包含目标，那么这些目标就要达到 6.2 的标准。如果方针包含设定目标的框架，则该框架产生的目标需要满足 6.2 的要求。

确定目标时需要考虑的要求是那些在了解组织及其背景（见 4.1）以及相关方（见 4.2）的需求和期望时确定的要求。

风险评估和风险处置的结果被用作对目标进行持续审查的输入，以确保它们保持适合于组织的境况。

信息安全目标是风险评估的输入：风险接受准则和执行信息安全风险评估的准则（见 6.1.2）考虑了这些信息安全目标，从而确保风险水平与其一致。

依据 ISO / IEC 27001 的信息安全目标是：

a) 与信息安全方针保持一致;
b) 如果切实可行，可以测量;这意味着能够确定是否达到目标是重要的;
c) 连接适用的信息安全要求和风险评估与风险处置的结果;
d) 沟通;和

e） 酌情更新。

组织保留有关信息安全目标的文件化信息。

当计划如何实现其信息安全目标时，组织确定：

f） 将要做什么;
g） 将需要什么资源;
h） 谁负责;
i） 何时完成;和
j） 如何评价结果。

以上关于计划的要求是通用的,并且适用于 ISO/IEC 27001 要求的其他计划。为 ISMS 考虑的计划包括：

- 如 6.1.1 和 8.1 所述的改进 ISMS 的计划;
- 如 6.1.3 和 8.3 所述的处置已识别的风险的计划;和
- 有效运行所需的任何其他计划（如开发能力和提高认识、沟通、绩效评价、内部审计和管理评审的计划)。

指南

信息安全方针宜申明信息安全目标或为设定目标提供一个框架。

信息安全目标可以用各种方式表示。该表示宜适合于满足可测量的要求（如果可行）（ISO/IEC 27001：2013，6.2b))。

例如，信息安全目标可以用下列方式表示：

- 有界限的数值，例如“不超过一定限度”、“达到四级”;
- 信息安全绩效测量指标;
- 衡量 ISMS 有效性的指标（见 9.1）;
- 遵从 ISO/IEC 27001;
- 遵从 ISMS 程序;

- 完成行动和计划的需要;和
- 要符合的风险准则。

以下指南适用于解释中提到的编号条目：

- 见上面的 a)。信息安全方针指定组织中信息安全的要求。其他相关职能和层级的具体要求宜与其相一致。如果信息安全方针具有信息安全目标，那么其他任何具体的信息安全目标宜与信息安全方针中的信息安全目标联系起来。如果信息安全方针只提供了设定目标的框架，那么宜遵循这个框架，并宜确保更具体的目标与更通用的目标挂钩。
- 见上面的 b)。并不是每一个目标都可以测量，但可以使目标所支持的成绩和改进可测量。能够定性或定量描述目标达到的程度是非常理想的。例如，如果目标未得到满足，则为额外的努力指导优先级，或者，如果目标是过度的，则提供对提高效益的机会的见解。目标是否被实现，目标的实现是如何确定的，以及是否有可能使用定量测量来确定目标达成的程度宜是可以被理解的。目标实现的定量描述宜详细说明如何进行相关的测量。要定量确定所有目标的实现程度可能是不可能的。ISO/IEC 27001 要求目标在可行的情况下可以测量;
- 见上面的 c)。信息安全目标宜与信息安全需求相一致;因此，在设定信息安全目标时，宜将风险评估和处置结果作为输入;
- 见上面的 d)。信息安全目标宜被传达给相关的组织内部相关方。它们也可以被传达到外部相关方，例如：客户、利益相关者、他们需要知道的程度、受到信息安全目标的影响;和
- 参见上面的 e)。当信息安全需要随时间变化时，相关信息安全目标宜相应地更新。其更新宜根据 d)的要求酌情传达至内部及外部相关方。

组织宜计划如何实现其信息安全目标。组织可以使用它选择的任何方法或机制来实现其信息安全目标。可以是单个信息安全计划、一个或多个项目计划或包含在其他组织计划中的行动。不管计划采取何种形式，最终的计划都应该至少（见上面的 f）到 j））定义为：

- 要完成的活动;
- 保证执行活动所需的资源;
- 责任;
- 活动的时间表和里程碑;和
- 评价结果是否实现目标的方法和量度，包括此评价的时间安排。

ISO/IEC 27001 要求组织保留有关信息安全目标的文件化信息。这些文件化信息可能包括：

- 计划、行动、资源、责任、最后期限和评价方法;和
- 要求、任务、资源、责任、评价频率和方法。

其他信息

无其他信息。

7. 支持

7.1.资源

需要的活动

组织确定并提供建立、实现、维护和持续改进 ISMS 的资源。

解释

资源是进行任何形式的活动的基础。资源类别可能包括：

a) 推动和操作活动的人员;
b) 执行活动的时间和在进行新的步骤之前让结果落地的时间;
c) 获取、开发和实施所需的财务资源;
d) 用于支持决策、测量行动的性能和提高知识的信息;和
e) 基础设施和其他可以被获取或建造的财富，如技术、工具和物料，不管它们是否是信息技术产品。

这些资源应与 ISMS 的需求保持一致，并因此在需要时进行调整。

指南

组织宜：

f) 在数量和质量上（容量和能力）估算与 ISMS 相关的所有活动所需的资源;
g) 根据需要获取资源;
h) 提供资源;
i) 维护跨越整个 ISMS 过程和具体活动的资源;和
j) 审查针对 ISMS 的需要所提供的资源，并根据需要进行调整。

此活动及其结果的文件化信息仅在形式上或是到了组织确定对其管理体系有效性是必要的程度时是强制性的（见 ISO/IEC 27001：2013,7.5.1 b））

其他信息

无其他信息。

7.2.能力

需要的活动

组织决定信息安全绩效所需人员的能力，并确保人员胜任。

解释

能力是应用知识和技能来实现预期结果的才能。它受知识、经验和智慧的影响。

能力可以是特定的（例如，关于技术的或者特定的管理（如风险管理））或常规的（例如软件技能、可靠性、基础技术和管理科目）。

能力与在组织的控制下工作的人员有关。这意味着组织的员工和其他需要的人员的能力宜被管理。

获得更高的或新的能力和技能可能是在内部和外部通过实践、培训（例如课程、研讨会和讲习班）、辅导、聘用或签约外部人员实现。

对于只是暂时需要的能力-为了特定的活动或短暂的时间，例如弥补意想不到的内部人员的临时短缺-组织可能聘用或签约其能力是可看到的和被验证的外部资源。

指导

该组织宜：

a) 确定 ISMS 中每个角色的预期能力，并决定是否需要文件化（例如在职位描述中）；
b) 通过以下方式将 ISMS 中的角色（见 5.3）分配给具有所需能力的人员：

   1) 识别组织内有能力的人员（基于如他们的教育、经历或认证）；
   2) 规划和实施组织内人员获得能力的行动（例如通过提供培训、辅导、现有员工的重新分配）;或者
   3) 聘用有能力的新人（例如通过聘用或签约）；

c) 评价上述 b）中的行动的有效性;

例 1：考虑人员在培训后是否已获得能力。

例 2：分析新近聘用或签约的人员到达组织后的一段时间的能力。

例 3：验证是否按预期完成了获取新人的计划。

d) 核实这些人是否有能力担任其角色;和
e) 确保能力随着时间发展，并符合预期。

适当的文件化信息需要作为能力的证据。因此，组织宜保留关于影响信息安全绩效的必要能力和这种能力如何被有关人员满足的文件。

其他信息

无其他信息。

7.3.意识

需要的活动

在组织的控制下工作的人员意识到信息安全方针、他们对 ISMS 有效性的贡献、提高信息安全绩效的效益，以及不符合 ISMS 要求的影响。

解释

在组织的控制下工作的人员的意识是指对关于他们对待信息安全方面的预期具有必要的理解和动机。

意识涉及的人员是那些必须知道、理解、接受和：

a) 支持信息安全方针中申明的目标;和
b) 遵守规则，正确执行他们在信息安全方面的日常工作。

的人员。

此外，在组织的控制下工作的人员也需要知道、理解和接受不符合 ISMS 要求的影响。影响可能是对信息安全的负面后果或对个人的不良反响。

这些人员需要意识到信息安全方针的存在以及在哪里可以找到相关的信息。组织中的许多员工不需要知道方针的详细内容。相反，他们宜知道、理解、接受并实现影响其工作角色的派生自方针的信息安全目标和要求。这些要求可能包含在他们预期要遵循其完成他们的工作的标准或规程中。

指南

组织宜：

c) 准备一个聚焦于每个受众（如内部和外部人员）的具体讯息的课程;
d) 将信息安全需求和期望纳入其他主题的意识和培训材料中，以将信息安全需求置入有关的运行环境;
e) 准备一个按计划的时间间隔沟通讯息的计划;
f) 在意识会议结束时和在会议期间随机验证关于讯息的知识和理解;和
g) 验证人们是否根据传达的讯息行动，并使用“好”和“坏”行为的例子来强化讯息。

此活动及其结果的文件化信息仅在形式上或是到了组织确定对其管理体系有效性是必要的程度时是强制性的（见 ISO/IEC 27001：2013,7.5.1 b））

其他信息

关于信息安全领域中的意识的更多信息可以在 ISO/IEC 27002：2013，7.2.2 找到。

7.4.沟通

需要的活动

组织确定与 ISMS 相关的内部和外部通信需求。

解释

沟通是 ISMS 中的一个关键过程。与内部和外部相关方进行充分的沟通是必要的（见 4.2）。

沟通可能是组织内部所有层面的内部相关方之间的或者组织和外部相关方之间的。沟通可能由组织或外部相关方发起。

组织需要确定：

- 需要传达哪些内容，例如，信息安全方针、目标、规程，以及它们的变化，信息安全风险方面的知识，对供应商的要求和信息安全性能反馈;
- 沟通活动的首选或最佳时间点，谁将参与沟通活动，哪些是沟通努力的目标受众；
- 谁发起沟通活动，例如特定的内容可能要求由特定的人或组织发起沟通;和
- 哪些过程推动或启动交流活动，以及哪些过程是沟通活动的对象或受到沟通活动的影响。

沟通可能定期或根据需要进行。它可能是主动的或被动的。

指南

沟通依赖于过程、渠道和协议。宜选择这些来确保沟通的信息被整体接收、正确理解，并在有意义的时候采取适当的行动。

组织宜确定哪些内容需要沟通，比如：

a) 在需要和适当的情况下，在风险识别、分析、评价和处置方面，与相关方沟通风险管理计划和结果;
b) 信息安全目标;
c) 取得的信息安全目标，包括那些能够支持其在市场上的地位的信息安全目标（如：获得 ISO/IEC 27001 证书; 声称符合个人信息保护法）;
d) 事件或危机，透明度往往是在组织管理其信息安全和处理意外情况能力方面保持和增强信任和信心的关键;
e) 角色、责任和权力;
f) ISMS 过程所要求的职能和角色以之间交换的信息;
g) ISMS 的变化;
h) 通过审查 ISMS 范围内的控制和过程所识别的其他事项;
i) 需要与监管机构或其他相关方沟通的事项（例如事件或危机通知）;和

j） 来自客户、潜在客户、服务的用户和当局等外部方的需要或其他交流。

组织宜识别有关问题的沟通要求：

k） 谁被允许在外部和内部进行沟通（例如，像数据泄露一样的特殊情况），分配给特定的角色适当的权限。例如，官方沟通官员可能由适当的权威来明确。他们可能是外部沟通的公共关系官员和内部沟通的安全官员;

l） 沟通的触发或频率（例如，关于事态的沟通，触发条件是事态的识别）;

m） 基于高级别的假设的影响的关键相关方（例如客户、监管人员、普通公众、重要的内部用户）的讯息内容。如果作为沟通计划、事件响应计划或业务连续性计划中的一部分，基于由适当级别的管理者事先准备好的并预先批准的讯息进行沟通，沟通可能会更加有效;

n） 通信的预期接收者;在某些情况下，应该维护一份清单（例如，沟通服务或危机的变化）;

o） 沟通手段和渠道。沟通宜使用专门的手段和渠道，确保信息是正式的，并具有适当的权威。沟通渠道宜满足保护所传递信息的机密性和完整性的任何需求;和

p） 为了确保讯息发送并被正确地接收和理解所设计的过程和方法。

沟通宜依据组织的要求进行分类和处理。

此活动及其结果的文件化信息仅在形式上或是到了组织确定对其管理体系有效性是必要的程度时是强制性的（见 ISO/IEC 27001：2013,7.5.1 b））

其他信息

无其他信息。

7.5.文件化信息

7.5.1. 总则

需要的活动

组织包括 ISO/IEC 27001 直接要求的 ISMS 中的文件化信息，以及组织确定的对 ISMS 的有效性是必要的信息。

解释

需要文件化信息来定义和沟通信息安全目标、策略、指导原则、操作指南、控制、过程、规程，以及人们期望做什么以及他们该如何行事。文件化信息对于 ISMS 的审计和在关键角色中的人员变化时维持稳定的 ISMS 也是必要的。此外，需要文件化信息记录 ISMS 过程和信息安全控制的行动、决策和结果。

文件化信息可以包含：

- 有关信息安全目标、风险、要求和标准的信息;
- 有关过程和规程的信息;和
- 过程输入（例如管理评审）和输出（包括业务活动的计划和结果）的记录。

ISMS 中有许多活动产生文件化信息，多数情况下，这些文件化信息被用作另一个活动的输入。

ISO/IEC 27001 要求有一套强制性的文件化信息，并包含一个通用要求，即如果对 ISMS 的有效性是必要的，则需要额外的文件化信息。

所需的文件化信息量通常与组织的规模有关。

总而言之，强制性和额外的文件化信息包含足够的信息，以允许执行第 9 章中规定的绩效评价要求。

指南

，组织宜确定除了 ISO/IEC 27001 要求的强制性文件化信息之外哪些文件化信息是确保 ISMS 有效性所必要的。

文件化信息宜是适合目的的。如实的和切题的文件化信息是所需要的。

组织可能确定的对确保其 ISMS 的有效性是必要的文件化信息举例如下：

- 背景确立的结果（见条款 4）：
- 角色、责任和权力（见条款 5）：
- 风险管理的不同阶段的报告（见第 6 章）：
- 确定的和提供的资源（见 7.1）：
- 预期的能力（见 7.2）：
- 提高意识活动的计划和结果（见 7.3）；
- 沟通活动的计划和结果（见 7.4）：
- ISMS 所必要的外部来源的文件化信息（见 7.5.3）：
- 控制文件化信息的过程（见 7.5.3）：
- 指导和运营信息安全活动的方针、规则和指令;
- 用于实施、维护和改进 ISMS 和整体信息安全状态的过程和规程（见条款 9）：
- 行动计划;和
- -SMS 过程（例如事件管理、访问控制、信息安全连续性、设备维护等）结果的证据。

文件化信息可能是内部固有的或外部来源的。

其他信息

如果组织想要在文件管理系统中管理其文件化信息，这可能是依据 ISO 30301 中的要求进行构建。

7.5.2. 创建和更新

需要的活动

在创建和更新文件化信息时，组织确保其适当的标识和描述、格式和介质，以及审查和批准。

解释

组织详细识别文件化信息是如何被最好地组织的，并定义一个合适的归档方法。

通过适当的管理进行审查和批准，确保文件化信息是正确的、适合于目的的，并为目标受众提供适当的形式和细节。定期审查确保文件化信息的持续适宜性和充分性。

指南

文件化信息可以以任何形式保留，例如，传统文件（纸质和电子形式）、网页、数据库、计算机日志、计算机生成的报告、音频和视频。此外，文件化信息可以由意图的详述（如信息安全方针）或绩效记录（例如审计结果）或两者的混合组成。以下指导原则直接用于传统文件，并宜在用于其他形式的文件化信息时予以适当解释。

组织宜创建一个结构化的文件化信息库，联系文件化信息的不同部分，通过：

a) 确定文件化信息框架的结构;
b) 确定文件化信息的标准结构;
c) 为不同类型的文件化信息提供模板;
d) 确定准备、批准、发布和管理文件化信息的责任;和
e) 确定并文件化修订和批准过程，以确保持续的适宜性和充分性。

组织宜定义一个文档方法，其中包含每个文档的共同属性，允许清晰和唯一的标识。这些属性通常包括文档类型（例如方针、指令、规则、指南、计划、表格、过程或规程）、目的和范围、标题、发布日期、类别、参考编号、版本号和修订历史。宜包括作者和当前负责文件的人员的身份、其应用和演变，以及批准人或批准机关。

格式要求可能包括合适的文档语言、文件格式、使用的软件版本和图形内容的定义。介质要求定义了信息宜使用哪些物理和电子介质。

陈述和写作风格应该适合受众和文档的范围。

宜避免文件化信息中的信息重复，并使用交叉引用，而不是在不同的文件中复制相同的信息。

文件记录方法应确保及时审查记录在案的信息，所有文件变更须经过批准。合适的评审准则可能是与时间相关的（例如文件评审之间的最大时间周期）或与内容有关的。宜定义审批准则，确保文件化信息是正确的、适合于目的，并为目标受众提供适当的形式和细节。

其他信息

无其他信息

7.5.3. 文件化信息的控制

需要的活动

组织在其整个生命周期中管理文件化信息，并使其在需要的地点和时间可用。

解释

一旦批准，文件化信息将传达给目标受众。文件化信息在需要的地方和时间可用，同时在整个生命周期中保持其完整性、机密性和实用性。

注：考虑到组织的需求和期望，如果能够执行并且有用，那么 ISO/IEC 27001:2013 7.5.3 中描述的“适用（as applicable）”的活动就需要执行。

指南

结构化的文件信息库可能用来来帮助访问文件化信息。

所有文件化信息宜根据组织的分类方案进行分类（见 ISO/IEC 27001:2013，A.8.2.1）。文件化信息且按照其分类级别进行保护和处理（见 ISO/IEC 27001:2013，A.8.2.3）。

文件化信息的变更管理过程宜确保只有获得授权的人员有权通过适当和预先定义的方式根据需要进行变更和分发。文件化信息宜受到保护，以确保其有效性和真实性。

文件化信息宜分发给获得授权的相关方。为此，组织宜针对每个文件化信息（或一组文件化信息）确定谁是有关的相关方，以及用于分发、访问、检索和使用的手段（例如具有适当的访问控制机制的网站）。分发宜遵从关于保护和处理机密信息的任何要求。

组织宜根据其预期有效期和其他有关要求，为文件化信息确立适当的保留期限。组织宜确保信息在整个保留期内是易读的（例如，使用可获得的软件能够读取的格式，或者验证纸张没有损坏）。

组织宜确立文件化信息在其保留期限到期后如何处理。

组织还宜管理外部来源的文件化信息（即来自客户、合作伙伴、供应商、监管机构等）。

此活动及其结果的文件化信息仅在形式上或是到了组织确定对其管理体系有效性是必要的程度时是强制性的（见 ISO/IEC 27001：2013,7.5.1 b））

其他信息

无其它信息。

8. 运行

8.1.运行规划和控制

需要的活动

组织规划、实施和控制过程以满足其信息安全要求并实现其信息安全目标。

组织根据需要保存文件化信息，以确保过程按计划进行。

组织控制计划中的变更，并审查非计划的变更的后果，并确保外包过程得到识别、定义和控制。

解释

规划组织用来满足其信息安全要求的过程，一旦实施，就会受到控制，特别是在需要变更时。

根据 ISMS 的规划（见 6.1 和 6.2），组织执行必要的运行规划和活动来实现满足信息安全要求所需的过程。

满足信息安全要求的过程包括：

a) ISMS 过程（如管理评审、内部审核）;和
b) 实施信息安全风险处置计划所需的过程。

规划结果在运行和受控的过程中实施。

为了实现其信息安全目标，组织最终保留规划和控制任何外包过程的责任。因此，组织需要：

c) 考虑与外包相关的信息安全风险，确定外包过程;和
d) 确保外包过程得到控制（即规划、监视和审查），在一定程度上对他们按预期运行提供保证（也考虑信息安全目标和信息安全风险处置计划）。

实施完成后，对过程进行管理、监视和审查，以确保在理解了相关方的需求和期望（见 4.2）后，继续满足需求。

运行中的 ISMS 的变更可能是计划的或他们的发生是非计划的。无论何时，组织对 ISMS 进行更改（由于计划的结果或非故意的），它会评估变更的潜在后果以控制任何不利影响。

组织可能通过记录活动和使用文件化信息作为第 9 章中规定的绩效评价过程的输入，获得对规划实施的有效性的信心。组织因此建立了所需的文件化信息并保留。

指南

作为第 6 章所描述的规划的结果，已定义的过程宜在整个组织内实现、运行和验证。宜考虑和实现以下内容：

e) 信息安全管理具体的过程（如风险管理、事件管理、连续性管理、内部审计、管理评审）;
f) 信息安全风险处置计划中的信息安全控制所产生的过程;
g) 信息安全领域内的报告结构（内容、频率、格式、责任等），例如事件报告、测量信息安全目标完成情况的报告、所执行活动的报告;和
h) 信息安全领域的会议结构（频率、参与者、目的和授权）。为了信息安全领域的有效的管理，信息安全活动宜由组织的各部门的具有相应的角色和工作职能的代表协调。

对于计划的变更，组织宜：

i) 计划他们的实施并分配任务、责任、期限和资源;
j) 按照计划实施变更;
k) 监视他们的执行，确认他们是按照计划执行的;和
l) 收集并保存变更执行的文件化信息，作为他们已按计划（例如：责任、期限、有效性评价）执行的证据。

对于观察到的非计划的变更，组织宜：

m) 审查其后果;
n) 确定是否已经发生或将来可能发生任何不利影响;
o) 必要时，计划和实施行动以减轻任何不利影响;和

p) 收集和保留有关非计划的变更和为减轻不利影响采取的行动的文件化信息。

如果组织的职能或过程程的一部分外包给供应商，组织宜：

q) 确定所有的外包关系;
r) 建立与供应商的适当的接口;
s) 解决供应商协议中与信息安全相关的问题;
t) 监视和审查供应商服务，确保其按照预期运行，相关的信息安全风险符合组织的风险接受准则;和
u) 根据需要管理供应商服务的变更。

其他信息

无其他信息。

8.2.信息安全风险评估

需要的活动

组织执行信息安全风险评估，并保留有关结果的文件化信息

解释

执行信息安全风险评估时，组织执行 6.1.2 中定义的过程。这些评估要么根据事先定义的时间表执行，要么是为了应对重大变化或信息安全事件。信息安全风险评估的结果作为 6.1.2 中的过程按照定义被执行的证据保留在文件化信息中。

来自信息安全风险评估的文件化信息对于信息安全风险处置是必不可少的，对绩效评价很有价值的（见第 9 章）。

指南

组织宜有计划进行预定的信息安全风险评估。

当 ISMS（或其背景）的重大变化或信息安全事件发生时，组织宜确定：

a) 哪些变更或事件需要额外的信息安全风险评估;和
b) 如何触发这些评估。

在 ISMS 持续改进的背景下，风险识别的详细程度宜在信息安全风险评估的进一步迭代中逐步提高。广泛的信息安全风险评估宜每年至少进行一次。

其他信息

ISO/IEC 27005 为执行信息安全风险评估提供指导。

8.3.信息安全风险处置

需要的活动

组织实施信息安全风险处置计划，并保留有关信息安全处置结果的文件化信息。

解释

为了处理信息安全风险，组织需要完成 6.1.3 中定义的信息安全风险处置过程。在 ISMS 运行期间，每当风险评估根据 8.2 更新时，组织则根据 6.1.3 进行风险处置并更新风险处置计划。更新的风险处置计划再次实施。

信息安全风险处置的结果保存在文件化信息中，作为 6.1.3 中的过程按照定义执行的证据。

指南

信息安全风险处置过程宜在 8.2 中信息安全评估过程的每次迭代后或者在风险处置计划或其一部分执行失败时执行。

信息安全风险处置计划的实施进度宜由这个活动来推动和监视。

其他信息

无其他信息。

9. 绩效评价

9.1.监视、测量、分析和评价

需要的活动

组织评估信息安全绩效和 ISMS 的有效性。

解释

监视和测量的目的是帮助组织评判包括风险评估和处置在内的信息安全活动的预期成果是否按计划实现。

监视确定一个系统、一个过程或一个活动的状态，同时，测量是确定一个值的过程。因此，监视可能是通过一段时间内的一系列相似的测量来实现。

为了监视和测量，组织建立：

a) 要监视和测量什么;
b) 谁，什么时候监视和测量;和
c) 为了产生有效的结果所使用的方法（即可比较的和可重现的）。

为了分析和评价，组织建立：

d) 谁、什么进候分析和评价监视和测量的结果;和
e) 为了产生有效的结果所使用的方法。

评价有两个方面：

f) 评价信息安全绩效，以确定组织是否按预期行事，其中包括确定 ISMS 内的过程如何符合其规范;和

g) 评价 ISMS 的有效性，以确定组织是否做正确的事情，其中包括确定信息安全目标的实现程度。

注：“如果适用（as applicable）”（ISO/IEC 27001:2013，9.1，b））意味着如果能够确定监视、测量、分析和评价的方法，则它们需要被确定。

指南

一个好的实践是，在规划监视、测量、分析和评价时定义“信息需求”。信息需求通常表达为一个高层次的信息安全问题或陈述，可以帮助组织评价信息安全绩效和 ISMS 的有效性。换句话说，监视和测量宜被保证，以获得已定义的信息需求。

确定要测量的属性时宜小心。测量太多或错误的属性是不切实际的、昂贵的和适得其反的。除了测量、分析和评价众多属性的成本之外，关键问题可能会被掩盖或完全忽略。

有两种通用的测量类型：

h) 绩效测量，根据计划活动的特点（如人数、里程碑成就或信息安全控制的实施程度）来表达计划的结果;和

i) 有效性测量，表达计划的活动的实现对组织信息安全目标的效果。

为那些参与监视、测量、分析和评价的人员确定和分配不同的角色可能是合适的。这些角色可能是评价的输入或输出的测量客户、测量计划者、测量审查者、信息所有者、信息收集者、信息分析者和信息沟通者[见 ISO/IEC 27004:2016,6.5)。

监视和测量以及分析和评价的责任往往分配给需要不同能力的独立人员。

其他信息

监视、测量、分析和评价对于有效的 ISMS 的成功至关重要。ISO/IEC 27001 中有许多条款明确要求确定一些活动的有效性。例如，ISO/IEC 27001:2013,6.1.1e)、7.2c）或 10.1d)。

更多的信息可以在 ISO/IEC 27004 中找到，它提供了满足 ISO/IEC 27001:2013 9.1 的要求的指导。特别是它扩展了上面提到的所有概念，如角色和责任、形式，并给出了很多例子。

9.2.内部审核

需要的活动

组织进行内部审核，以提供有关 ISMS 符合要求的信息。

解释

通过内部审核的手段按计划的时间间隔对 ISMS 进行评价，提供对最高管理层的 ISMS 状态的保证。审计的特点是一些原则：正直的、公允表达、应有的职业审慎性、机密性、独立性和以证据为基础（见 ISO 19011)。

内部审核提供 ISMS 是否符合组织自身对 ISMS 的要求以及 ISO/IEC 27001 的要求的信息。组织自身的要求包括：

a) 信息安全方针和规程中规定的要求;
b) 设定信息安全目标的框架所产生的要求，包括风险处置过程的结果;
c) 法律和合同的要求;和
d) 文件化信息的要求。

审计师还评价 ISMS 是否得到有效实施和维护。

审计程序描述了一套审核的总体框架，在具体的时间框架内的计划，并针对特定的目的。这与描述具体审计的活动和安排的审核计划不同。审计准则是用作比较审计证据的参考的一组策略、规程或要求，即审计准则描述了审计师的期望。

内部审核可能识别不合格、风险和机会。不合格按照 10.1 的要求进行管理。风险和机会根据 4.1 和 6.1 的要求进行管理。

要求组织保留有关审计程序和审计结果的文件化信息。

指南

管理审计程序

审核程序定义了个体审核活动的计划、执行、报告和跟进的结构和责任。因此，宜确保所进行的审计是合适的，有正确的范围，最少化对组织运行的影响，并保持必要的审核质量。审核程序还宜确保审核小组的能力、审核记录的适当维护，以及对审计的运行、风险和效用的监视和审查。此外，审核程序宜确保 ISMS（即所有相关过程、功能和控制）在规定的时间框架内被审计。最后，审核程序宜包括有关审计的类型、持续时间、地点和进度表的文件化信息。

内部审核的范围和频率应基于组织的规模和性质以及 ISMS 的性质、设计目的、复杂性和成熟度水平（基于风险的审计）。

宜在内部审核的范围内检查实施的控制的有效性。审核程序宜被设计为确保涵盖所有必要的控制，并宜包括随着时间推移所选择的控制的有效性的评价。关键控制（依据审核程序）宜被包括在每次审核中，而为了管理较低风险而实施的控制可以以较少的频率审核。

审核程序还宜考虑，过程和控制应该已经运行了一段时间，以便能够评价合适的证据。

关于 ISMS 的内部审核可能作为组织其他内部审核的一部分或与其合作进行有效执行。审核程序可能包括与一个或多个管理体系标准相关的审核，分别或组合进行。

审核程序宜包括有关审核准则、审核方法、审核小组的选择、处理机密性的过程、信息安全、审核员的健康和安全准备，以及其他类似事宜。

审核员的能力和评价

关于审核员的能力和评价，组织宜：

e) 识别其审核员的能力要求;
f) 选择具有适当能力的内部或外部审核员;
g) 有适当的程序来监视审核员和审核小组的绩效;和
h) 包括内部审核小组的人员，这些人员具有适当的领域特定的和信息安全知识。

审核员宜进行选择，考虑到他们应是能胜任的、独立的、受过充分培训的。

选择内部审核员对于小公司来说可能是困难的。如果内部没有必要的资源和能力，外部审核员宜被委任。当组织使用外部审核员时，他们宜确保他们已经获得了有关组织背景的足够知识。这些信息宜由内部员工提供。

组织宜考虑作为内部审核员的内部员工能够鉴于组织的背景执行具体的审核，但是可能没有足够的关于执行审核的知识。

组织宜承认内部审核员相对外部审核员的特点和潜在的不足，并建立适当的具有必要的知识和能力的审核团队。

执行审核

在执行审核时，审核团队领导宜预备一份审核计划，考虑之前的审核结果，以及跟进之前报告的不合格项和不可接受的风险。审核计划宜保留为文件化的信息，并宜包括审核的准则、范围和方法。

审计团队宜审查:

- 过程和确定的控制的充分性和有效性;
- 信息安全目标的完成情况;
- ISO/IEC 27001:2013 第 4 至 10 条定义的要求的遵从情况;
- 组织自己的的信息安全要求的遵从情况;

- 适用性声明针对信息安全风险处置过程的结果的一致性;
- 实际的信息安全风险处置计划与已识别评定的风险及风险接受准则的一致性;
- 管理评审的输入和输出的相关性(考虑组织的规模和复杂性);和
- 管理评审输出(包括改进需求)对组织的影响。

对 ISMS 产生的控制的有效性的可获得的监视的程度和可信赖性(见 9.1)可以允许审核员减少他们自己的评价尝试,前提是他们已经确认了测量方法的有效性。

如果审核结果包括不合格，则被审核方宜为每个不合格准备一个行动计划，以便与审核团队领导达成一致。后续行动计划通常包括:

i) 检测到的不合格的描述;
j) 不合格原因的描述;
k) 短期纠正和长期纠正活动的描述，以在限定的时间表内消除检测到的不合格;和
l) 负责实施该计划的人员。

审核报告，与审计结果，宜分发给最高管理层。

宜审查以前的审计结果，并调整审计程序，以更好地管理由于不合格而面临较高风险的领域。

其他信息

可以在 ISO 19011 中找到进一步的信息,它提供了审核管理体系的通用指南,包括审计原则、管理审计程序和进行管理体系审计。它还提供了对参与审核的人员或群体的能力的评价的指导，包括管理审计程序的人员、审核员和审计团队的人员。

另外，除了包含 ISO 19011 中的指导外，更多的信息可以在以下地方找到:

a）ISO / IEC 27007[1)]，其中提供了关于管理 ISMS 审核程序、进行审计以及 ISMS 审核员的能力的具体指导;和

b）ISO / IEC 270080[1)]，其中提供了评估信息安全控制的指导。

9.3.管理评审

需要的活动

最高管理层按照计划的时间间隔审查 ISMS。

解释

管理评审的目的是确保 ISMS 的持续的适宜性、充分性和有效性。适宜性是指持续与组织目标保持一致。充分性和有效性是指 ISMS 的适当设计和组织嵌入，以及由 ISMS 驱动的过程和控制的有效实施。

总的来说，管理评审是在组织内各个层级进行的一个过程。这些活动可以从每天、每周或每月的组织单元会议到简单的报告讨论。最高管理层最终负责管理评审，并从组织的各个层级获得输入。

指南

最高管理层应要求并定期审查 ISMS 绩效报告。

1）正在编写第二版。

管理层可能通过多种方式审查 ISMS，例如接收和审查测量和报告、电子通信、口头补充资料。主要输入是 9.1 中描述的信息安全测量的结果和 9.2 中描述的内部审核的结果，以及风险评估结果和风险处置计划的状态。在审查信息安全风险评估的结果和信息安全风险处置计划的状态时，管理层应确认残余风险符合风险接受准则，以及风险处置方案处理了所有相关风险及其风险处置选项。

ISMS 的所有方面都宜通过在管理会议上设置适当的时间表和议程项目，由管理层按计划的时间间隔进行审查，至少每年一次。新的或不太成熟的 ISMS 宜由管理层更频繁地审查，以推动其增强有效性。

管理评审的议程应处理以下题目：

a) 以前的管理评审的行动的状态;
b) 与 ISMS 相关的外部和内部问题的变化（见 4.1);
c) 对信息安全绩效（包括趋势）的反馈：

1) 不合格和纠正行动;
2) 监视和测量结果;
3) 审核结果;和
4) 信息安全目标的完成情况。

d) 相关方的反馈，包括改进建议、变更请求和投诉;
e) 信息安全风险评估的结果和信息安全风险处置计划的状态;和
f) 持续改进的机会，包括 ISMS 和信息安全控制的效能改进。

管理评审的输入宜根据参与评审的管理层确定的目标进行适当的细化。例如，最高管理层宜根据信息安全目标或高层次目标，仅评价所有条目的摘要。

管理评审过程的输出宜包括有关持续改进机会的决策和对 ISMS 进行变更的任何需求。他们可能还包括下列决策的证据：

g) 信息安全方针和目标的变化，例如受外部和内部问题的变化以及相关方的要求所驱动;
h) 风险接受准则和进行信息安全风险评估的准则的改变（见 6.1.2)：
i) 在评估信息安全绩效之后，如果需要，采取的行动;
j) ISMS 资源或预算的变化;
k) 更新的信息安全风险处置计划或适用性声明;和
l) 监视和测量活动的必要改进。

来自管理评审的文件化信息是必要的。它宜被保留，以证明对 ISO/IEC 27001 中列出的所有领域（至少）给予了考虑，即使它被决策为没有采取措施的必要。

当在组织的不同层次上进行多次管理评审时，那么，他们宜以适当的方式相互联系。

其他信息

无其他信息。

10. 改进

10.1. 不合格和纠正措施

需要的活动

组织对不合格做出反应，评估他们，并在需要时采取纠正以及纠正措施。

解释

不合格是未满足 ISMS 的要求。要求是申明的、暗指的或强制性的需要或期望。有几种类型的不合格，比如：

a) 未能在 ISMS 中满足（完全或部分）ISO/IEC 27001 的要求;
b) 未能正确地执行或符合 ISMS 规定的要求、规则或控制;和
c) 部分或全部未能遵守法律、合同或商定的客户要求。

不合格可能是例如：

d) 人员未按照规程和政策的预期工作;
e) 未提供商定的产品或服务的供应商;
f) 未交付预期结果的项目;和
g) 未按设计运行的控制。

不符合可能通过以下方式来辨认：

h) 在管理体系范围内执行的活动的缺陷;

i) 没有适当补救的无效控制;

j) 信息安全事件分析，显示不符合 ISMS 的要求;

k) 客户的投诉;

l) 来自用户或供应商的警报;

m) 不符合接受准则的监视和测量结果;和

n) 未实现的目标。

纠正旨在立即解决不合格问题并处理其后果(ISO/IEC 27001:2013,10.1 a))。

纠正措施旨在消除不合格的原因并防止再发生（ISO/IEC 27001：2013,10.1 b）至 g))。

注：如果“适用时(as applicable）”（ISO/IEC 27001：2013,10.1 a))意味着如果控制和纠正不合格的行动可以被采取，则它需要被采取。

指南

信息安全事件并不一定意味着存在不合格，但它们可能不合格的迹象。内部和外部审核和客户投诉是帮助辨认不合格的其他重要来源。

对不合格的反应宜基于明确的处理过程。这个过程宜包括：

- 识别不合格的程度和影响;
- 纠正的决定以限制不合格的影响。纠正可能包括切换到之前的、故障保护的或其他适当的状态。宜小心，使纠正不会使情况变得更糟;
- 与有关人员沟通，确保纠正得到执行;
- 按照决策执行纠正;
- 监视情况，确保纠正有预期的效果，并且没有产生意外的副作用;
- 如果仍未得到补救，进一步行动以纠正不合格;和
- 酌情与其他有关的相关方进行沟通。

作为总体结果，处理过程宜把不合格及其连带的后果带到一个受监管的状态。然而，更正本身不一定能防止不合格的再次发生。

纠正措施可以在纠正发生之后或与纠正并行。宜采取以下处理步骤：

1. 根据既定准则（如不合格的影响、重复性）决定是否需要执行纠正措施;
2. 不合格的审查，考虑到：

   - 如果相似的不符合记录在案;
   - 不合格引起的所有后果和副作用;和
   - 所采取的纠正。

3. 对不合格进行深入的原因分析，考虑到：

   - 什么出错了，导致不合格的具体触发或情况（例如，由人员、方法、过程或规程、硬件或软件工具、错误的测量、环境决定的错误）;和
   - 可能有助于识别未来的类似情况的模式和准则。

4. 对 ISMS 的潜在后果进行分析，考虑到：

   - 其他领域是否存在类似的不合格，例如通过使用原因分析中发现的模式和标准;和
   - 其他领域是否与已确认的模式或准则匹配，以致，在类似的不合格发生之前这只是一个时间问题。

5. 确定纠正原因所需的措施，评价它们是否与不合格的后果和影响相称，并检查它们是否有可能导致其他不合格或重大的新的信息安全风险的副作用;
6. 计划纠正措施，如果可能的话，优先考虑不合格重复出现的可能性较大和更重大的后果的领域。规划宜包括纠正措施的责任人和实施的最后期限;
7. 按照计划执行纠正措施;和

8. 评定纠正措施，确定他们是否确实处理了不合格的原因，以及是否防止了相关不合格的发生。这种评估宜是公正的、以证据为基础的，并形成文件。它也宜被传达给适当的角色和相关方。

作为纠正和纠正措施的结果，新的改进机会被识别是有可能的。这些宜被相应地处理（见 10.2）。

需要保留足够的文件化信息来证明组织已经采取适当的行动来处理不合格并处理了其连带的后果。所有不合格管理的重要步骤（从发现和纠正开始），如果启动，纠正措施的管理（原因分析、审查、关于措施实施的决策、为 ISMS 本身做出的审查和变更决定）宜予以记录。文件化信息也需要包括所采取的行动是否达到了预期的效果的证据。

一些组织维护登记表以跟踪不合格和纠正措施。可能有多个登记表（例如每个功能区域或过程一个登记表）和不同的介质（纸张、文件、应用程序等）。如果是这样的话，那么它们宜作为文件化信息被建立和控制，并且宜对所有不合格和纠正措施进行全面审查，以确保正确评价措施的必要性。

其他信息

ISO/IEC 27001 没有为“预防措施”明确规定任何要求。这是因为一个正式的管理体系的关键目的之一就是作为预防工具。因此，ISO 管理体系标准使用的通用文本要求对组织的“与其目的相关的，影响其实现预期结果的能力的外部和内部问题”(在 4.1 中)进行评估，以及“确定需要解决的风险和机遇：确保 ISMS 能够达到预期的结果;预防或减少意外的影响;实现持续改进”（在 6.1 中）。这两组要求是经过深思熟虑的以涵盖“预防措施”的概念，并且从更广阔的视野看待风险和机会。

10.2. 持续改进

需要的活动

组织不断提高其 ISMS 的适宜性、充分性和有效性。

解释

组织及其背景永远不会是静态的。此外，信息系统面临的风险及其可能受到损害的方式正在急速演变。最后，没有 ISMS 是完美的;即使组织及其背景没有改变，总有一种可以改进它的方法。

作为一个与不合格或风险无关的改进的例子，ISMS 中要素（在适宜性、充分性和有效性方面）的评估可能表明其超出了 ISMS 要求的界限或缺乏效率。如果确实如此，则通过改变评估的要素来改进 ISMS 可能是一个机会。

采用持续改进的系统方法将引领更有效的 ISMS，从而改善组织的信息安全。信息安全管理引导组织的运营活动，以避免过度反应，即大部分资源用于发现问题和解决这些问题。ISMS 通过持续改进有条不紊的工作，使组织能够采取更积极主动的方法。最高管理层可能设定持续改进的目标，例如通过有效性测量、成本或过程成熟度。

因此，组织将其 ISMS 视为业务运营中不断发展、学习、生机勃勃的一部分。为了使 ISMS 跟上变化，其适宜性、有效性，以及与组织目标的一致性是经常被评价的。没有什么是理所当然的，没有什么仅仅因为它在实施时是足够好的就被认为是“禁区”。

指南

ISMS 的持续改进宜包括 ISMS 本身以及考虑内部和外部问题（4.1）所评估的所有要素，相关方的要求（4.2）和绩效评价的结果（第 9 条)。评估宜包括以下分析：

a) ISMS 的适宜性，考虑外部和内部问题、相关方的要求、已建立的信息安全目标和已识别的信息安全风险，是否通过信息安全管理体系和信息安全控制的规划和实施，得到了适当的处理;

b) ISMS 的充分性，考虑 ISMS 过程和信息安全控制是否与组织的总体目标、活动和过程兼容，是否足够；和

c) ISMS 的有效性，考虑是否 ISMS 的预期结果得到实现，相关方的要求得到满足，信息安全风险被管理至满足信息安全目标，不合格被管理，ISMS 的建立、实施、维护和持续改进所需的资源与这些结果是相称的。

评估还可能包括对 ISMS 及其要素的效率的分析，考虑它们的资源使用是否适当，是否存在效率低下可能导致效率损失的风险或是否有提高效率的机会。

管理不合格和纠正措施时，也可能识别改进机会。

一旦改进的机会被识别，组织宜根据 6.1.1：

d) 评价他们是否值得追求；

e) 确定 ISMS 及其要素的变化以实现改进；

f) 计划和实施措施处理机会，确保收益实现，和不合格不会发生；和

g) 评价行动的有效性。

这些措施宜被视为 6.1.1 中描述的处理风险和机会的措施的一个子集。

其他信息

无其他信息。

附录 A

（资料）

方针框架

附录 A 提供了包含信息安全方针的文档结构的指导。

总的来说，方针是由组织的最高管理层正式表达的组织的意图和方向的声明（见 ISO/IEC 27000：2016,2.84）。

方针的内容指导关于方针中主题的活动和决策。

一个组织可以有多个方针；每个活动领域对组织都是重要的。有些方针是相互独立的，其他的方针是有层次关系的。

通常，组织有一个总的方针，例如行为准则，在方针层次的最高层。总体方针由处理不同主题并可适用于组织的特定领域或职能的其他方针支持。信息安全方针是这些具体方针之一。

信息安全方针由一系列与信息安全方面相关的专题方针支持。ISO/IEC 27002 中讨论了其中的一些内容，例如信息安全方针可能由关于访问控制、信息分类（和处理）、物理和环境安全以及最终用户导向的主题、其它特有的方针来支持。可以增加额外的方针层。这种安排如图 A.1 所示。请注意，有些组织为专题方针文件使用其他术语，例如“标准”、“指令”或“规则”。

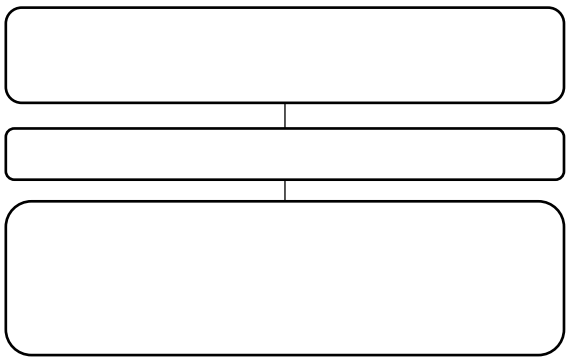


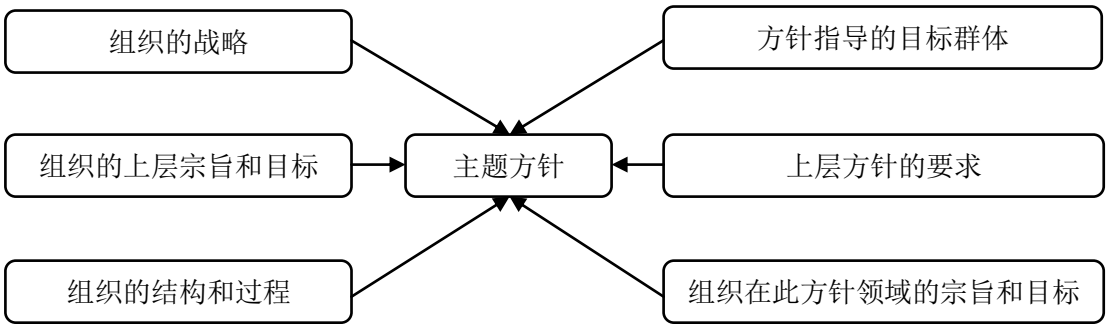
图 A.1 方针层次

ISO/IEC 27001 要求组织制定信息安全方针。但是，它没有说明该方针和本组织的其他方针之间的任何特殊关系。

方针的内容是基于组织的运营背景的。具体而言，在制定方针框架内的任何方针时宜考虑以下几点:

1. 组织的宗旨和目标;
2. 为实现组织目标所采用的战略;
3. 组织采用的结构和过程;
4. 与方针主题相关的目的和目标;
5. 相关的上层方针的要求;和
6. 由方针指导的目标群体。

如图 A.2 所示。



A.2 制定方针的输入

方针可能具有以下结构：

a) 行政 - 方针标题、版本、公布/有效日期、变更历史、所有者和审批人、分类、目标受众等。
b) 方针概要 - 一两句话概述。 （这有时可能与引言合并）。
c) 简介 - 对方针主题的简要解释;
d) 范围 - 描述组织内受方针影响的部分或活动。如果相关，范围条款列出了本方针支持的其他方针;
e) 目标 - 描述方针的意图;

f) 原则 – 描述关于实现目标的行动和决定的准则。在某些情况下，它对于识别与方针主题相关的关键流程以及操作流程的规则可能是有用的;

g) 职责– 描述谁来负责行动以满足方针的要求。在某些情况下，这可能包括对组织安排的描述以及具有指定角色的人的责任和权力;

h) 主要成果 – 如果目标得到满足，则描述业务成果。 在某些情况下，这可以与目标相结合;

i) 相关政策 – 描述与实现目标相关的其他政策，通常通过提供有关具体主题的更多细节; 和

j) 方针要求 – 描述方针的详细要求。

方针内容可以以各种方式进行组织。 例如，强调角色和责任的组织可以简化目标的描述，并将原则专门用于描述职责。

参考书目

[1] ISO 19011, *Guidelines for auditing management systems*

[2] ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

[3] ISO/IEC 27003:2010, *Information technology — Security techniques — Information security management system implementation guidance*

[4] ISO/IEC 27004:2016, *Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*

[5] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

[6] ISO/IEC 27007[2)], *Information technology — Security techniques — Guidelines for information security management systems auditing*

[7] ISO/IEC/TS 27008[2)], *Information technology — Security techniques — Guidelines for the assessment of information security controls*

[8] ISO 30301, *Information and documentation — Management systems for records — Requirements*

[9] ISO 31000, *Risk management — Principles and guidelines*