标准解读：一起看最新的ISO/IEC 27001: 2022标准详解！逐条理解审核要点、应输出的文档等

产品名称	标准解读：一起看最新的ISO/IEC 27001: 2022标准详解！逐条理解审核要点、应输出的文档等
公司名称	贯标集团
价格	.00/件
规格参数	
公司地址	南京市仙林大道10号三宝科技园1号楼B座6层
联系电话	4009992068 13382035157

产品详情

ISO/IEC 27001: 2022主要变化

（2）4 组织环境/4.1 理解组织及其环境

（3）4 组织环境/4.2 理解相关方的需求和期望

（4）4 组织环境/4.3 确定信息安全管理体系范围

（5）4 组织环境/4.4 信息安全管理体系

（6）5 领导作用/5.1 领导和承诺

（7）5 领导作用/5.2 方针

（8）5 领导作用/5.3 组织的角色、职责和权限

（9）6 策划/6.1 应对风险和机会的措施/6.1.1 总则

（10）6 策划/6.1 应对风险和机会的措施/6.1.2信息安全风险评估

（11）6 策划/6.1 应对风险和机会的措施/6.1.3 信息安全风险处置

（12）6 策划/6.2 信息安全目标及其实现策划

（13）6 策划/6.3 变更的策划

（14）7 支持/7.1 资源

（15）7 支持/7.2 能力

（16）7 支持/7.3 意识

（17）7 支持/7.4 沟通

（18）7 支持/7.5 文件化信息

（19）8 运行

（20）9 绩效评价/9.1 监视、测量、分析和评价

（21）9 绩效评价/9.2 内部审核

（22）9 绩效评价/9.3 管理评审

（23）10 改进/10.1 持续改进

（24）10 改进/10.2 不符合及纠正措施

（25）附录A.5 组织控制/A.5.1 信息安全策略

（26）附录A.5 组织控制/A.5.2 ~ A.5.6

（27）附录A.5 组织控制/A.5.7 威胁情报

（28）附录A.5 组织控制/A.5.8 项目管理中的信息安全

（29）附录A.5 组织控制/A.5.9 ~ A.5.14

（30）附录A.5 组织控制/A.5.15 ~ A.5.18

（31）附录A.5 组织控制/A.5.19 ~ A.5.23

（32）附录A.5 组织控制/A.5.24 ~ A.5.28

（33）附录A.5 组织控制/A.5.29 & A.5.30

（34）附录A.5 组织控制/A.5.31 ~ A.5.37

（35）附录A.6 人员控制

（36）附录A.7 物理控制

（37）附录A.8 技术控制/A.8.1 ~ A.8.5

（38）附录A.8 技术控制/A.8.6 ~ A.8.9

（39）附录A.8 技术控制/A.8.10 ~ A.8.13

（40）附录A.8 技术控制/A.8.14 ~ A.8.19

（41）附录A.8 技术控制/A.8.20 ~ A.8.24

（42）附录A.8 技术控制/A.8.25 ~ A.8.34

ISO/IEC 27001:2022延续了ISO/IEC 27001:2013基本架构和基本思路，因此总体看来，ISO/IEC 27001:2022没有太大变化，虽然附录部分调整比较大，但是基本上是在原来的基础变动的，附录本身属于底层执行的要求，也没有增加太多新东西。

ISO/IEC 27001:2022主要有三方面的变化：

（一）标准的标题稍微有所变化。原先的“ 信息技术-
安全技术 ”变成了“ 信息安全、网络安全、和隐私保护 ”；

（二）标准的正文部分，进行了轻微的调整。主要把其他体系标准如ISO 9001的内容放到ISO/IEC 27001:2022中去了，主要的变化集中在4.2, 6.2, 6.3, 和8.1。详细变化可以参考以下附件ISO/IEC 27001:2022与ISO/IEC 27001:2013对照表：

（三）标准的附录A，整个结构与之前相比变化较大，但内容变化不多。ISO/IEC 27001:2013附录A有14个领域，114项控制要求，ISO/IEC 27001:2022把控制要求减少到93项（有合并、有新增要求），分为4个领域。有35个控制要求和原来保持一样，原来的57个控制要求合并成了24个新的控制要求，还有原来的一个控制要求拆分为两个，新增了11个新的控制要求。详细变化可以参考以下附件ISO/IEC 27001:2022附录A与ISO/IEC 27001:2013附录A对照表：

ISO/IEC 27001:2022标准 正文 4 Context of the organization 组织环境/4.1 Understanding the organization and its context 理解组织及其环境

4.1 Understanding the organization and its context 理解组织及其环境

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

组织应确定与其意图相关的,且影响其实现信息安全管理体系预期结果能力的外部和内部事项。

NOTE Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.4.1 of ISO 31000:2018.

注：对这些事项的确定,参见ISO31000:2018 ,5.4.1中建立外部和内部环境的内容。

ISO/IEC 27001:2013标准 正文 4 组织环境/4.1 理解组织及其环境

4.1 理解组织及其环境

组织应确定与其意图相关的,且影响其实现信息安全管理体系预期结果能力的外部和内部事项。注：确定这些问题涉及到建立组织的外部和内部环境，在ISO 31000:2009的5.3节考虑了这一事项。

标准解析：

1) 本条款与ISO/IEC 27001:2013一样，没有变化，仅更新了备注中的ISO
31000标准版本更新到最新版本。因此，在实施这个条款时，可以比照SO/IEC 27001:2013；

2) 这个条款，目前是各个体系的通用条款，只是各个体系标准要求的侧重点不同，本标准主要关注组

织信息安全方面的内外部因素。所以在实施这个条款时，推荐的做法是，与质量、环境以及职业健康安全等管理体系整合一起实施；

3) 按照条款要求，组织必须建立识别影响信息安全管理体系的相关内外部因素的流程，并形成文件，文件应明确负责部门，识别时机和频率，以及收集内外部因素过程中的输入材料，即从哪些途径获得组织内外部因素。

4) 前面说到，4.1这个条款，是各个体系的通用条款，ISO/IEC 27001:2013与ISO 9001:2015在4.1的文字叙述上其实是大同小异的；

5) 这个条款，有一个重要的注解，提到本条款在实施过程中，可以参考ISO 31000这个标准。前面解析引言部分的时候提到，条款“ 4.1 理解组织及其环境 ”以及“ 6.1.1 总则 ”中，所涉及风险识别的要求，是针对整个组织而言的，这个属于战略层面，而“ 6.1.2 信息安全风险评估、6.1.3 信息安全风险处置、8.2 信息安全风险评估以及8.3 信息安全风险处置 ”所要求的风险评估，偏重于如信息系统的风险评估等属于执行层的，参考的标准是ISO/IEC 27005。

实施本条款应输出的文档：

6) 《环境分析控制程序》；

7) 公司内外部因素清单以及评审记录。

本条款审核要点：

1) 是否按照标准条款要求，建立环境分析控制流程，并形成文件，如《环境分析控制程序》；

2) 《环境分析控制程序》文件中是否明确公司有哪些与信息安全相关的内外部因素，是否有明确内外因素收集途径、收集责任部门/人，收集频率，评审方式和频率等；

3) 是否有按照《环境分析控制程序》文件要求，收集公司信息安全相关的内外部因素（需要提供相关书面清单），是否按照《环境分析控制程序》文件要求的频率定期对内外部因素清单做评审，并提供相关评审记录。

ISO/IEC 27001: 2022标准 正文 4 Context of the organization 组织环境/4.2 Understanding the needs and expectations of interested parties 理解相关方的需求和期望

4.2 Understanding the needs and expectations of interested parties 理解相关方的需求和期望The organization shall determine:组织应确定：a) interested parties that are relevant to the information security management system;a) 信息安全管理体系相关方；b) the relevant requirements of these interested parties;b) 这些相关方的相关要求；c) which of these requirements will be addressed through the information security management system.c) 哪些要求可以通过信息安全管理体系得到解决。NOTE The requirements of interested parties can include legal and regulatory requirements and contractual obligations.注：相关方的要求可包括法律、法规要求和合同义务

ISO/IEC 27001:2013标准 正文 4 组织环境/4.2 理解相关方的需求和期望

4.2 理解相关方的需求和期望组织应确定：a) 与信息安全管理体系有关的相关方；b) 这些相关方与信息安全有关的要求。注：相关方的要求可能包括法律法规要求和合同义务。

标准解析：

1) 本条款ISO/IEC 27001: 2022与ISO/IEC 27001: 2013要求的结果是一样的，都是要求识别出与信息安全管理体系有关的相关方的信息安全要求。但ISO/IEC 27001: 2022与ISO/IEC 27001: 2013要求得到结果的过程不一样。ISO/IEC 27001: 2022将ISO/IEC 27001: 2013的b)条款拆成了b)和c)。ISO/IEC 27001: 2022要求，要先识别出与信息安全管理体系有关的相关方所有要求，可能涵盖质量要求、信息安全要求等，然后再识别哪些要求可以通过信息安全管理体系解决。

2) 这个条款，跟4.1一样，是目前是各个体系的通用条款，只是各个体系标准要求的侧重点不同，本标准主要关注相关方的信息安全方面的需求和期望（见本条款c）。所以在实施这个条款时，同样推荐的做法是，与质量、环境以及职业健康安全等管理体系整合一起实施。

3) 在理解本条款的相关方时，可以参考本条款的备注，重点关注信息安全相关法律法规和客户的合同要求（涉及信息安全的）。但在ISO 9001: 2015等新版体系中，有明确指出相关方包括股东、客户、员工、供应商等。因此，在实施信息安全管理体系考虑相关方的时候，zuihao的做法是参照ISO 9001: 2015中相关方的要求，也需要关注员工的个人信息的保密要求，供应商提供的产品和服务的授权以及保密要求。

4) 在实施ISO/IEC 27001: 2022过程中，要满足4.2的要求，组织必须建立相关方要求分析过程，并形成书面文件。文件必须明确相关方及其要求识别的主导部门，获取途径，获取频率，评审周期等。实施本条款应输出的文档：

1) 《相关方要求管理程序》。

2) 适用法律法规清单及评价记录。

3) 客户信息安全要求清单及评审记录。本条款审核要点：

1) 是否能提供适用法律法规清单及评价记录。

2) 是否有对客户信息安全要求进行收集和评价，并能提供相关记录。

ISO/IEC 27001: 2022标准 正文 4 Context of the organization 组织环境/4.3 Determining the scope of the information security management system 确定信息安全管理体系范围

4.3 Determining the scope of the information security management system 确定信息安全管理体系范围The organization shall determine the boundaries and applicability of the information security management system to establish its scope.组织应确定信息安全管理体系的边界及其适用性，以建立其范围。When determining this scope, the organization shall consider:在确定范围时，组织应考虑：a) the external and internal issues referred to in 4.1;a) 4.1中提到的外部和内部事项；b) the requirements referred to in 4.2;b) 4.2中提到的要求；c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.c) 组织实施的活动之间的及其与其他组织实施的活动之间的接口和依赖关系。The scope shall be available as documented information.该范围应形成文件化信息并可用。

ISO/IEC 27001: 2013标准 正文 4 组织环境/4.3 确定信息安全管理体系范围

4.3 确定信息安全管理体系的范围组织应确定信息安全管理体系的边界和适用性，以建立其范围。当确定该范围时，组织应考虑：a) 在4.1 中提及的外部和内部问题；b) 在4.2 中提及的要求；c) 组织所执行的活动之间以及与其它组织的活动之间的接口和依赖性。范围应文件化并保持可用性。

标准解析：

1) 本条款（ISO/IEC 27001: 2022）条文与ISO/IEC 27001: 2013一样，没有变化。

2) 实施本条款，组织应根据“ 4.1 ”和“ 4.2 ”输出的内容，确定信息安全管理体系的范围。

3) 确定范围除了明确覆盖的业务，还需明确覆盖的组织物理边界（厂区、区域）和相关的逻辑边界（信息系统、网络通信）。

4) 外包项目亦需要纳入信息安全管理范围，ISO/IEC 27001:2022标准正文（条款4-条款10）不能shanchu。

5) 信息安全管理体系的范围，必须形成书面文件。如果有编写信息安全管理手册，可以放在手册之中，如果没有编写手册，可以单独形成文件，当作纲领性文件。

6) 信息安全管理体系范围确定后，必须形成书面的信息安全管理过程之间以及与外部管理过程之间的关系图（参见本条款c）。

实施本条款应输出的文档：

信息安全管理手册，或信息安全管理体系范围和信息安全管理过程关系图。

本条款审核要点：

审核“ 4.1 ”和“ 4.2 ”输出的内容（如法律法规清单和评价记录、客户信息安全要求清单及评审记录等）、组织架构图、营业执照、厂区平面图、网络拓扑图、厂区租赁合约、信息系统清单等资料，确认组织信息安全管理体系范围是否合理，或是否与上述资料存在矛盾的地方。

ISO/IEC 27001: 2022标准 正文 4 Context of the organization 组织环境/4.4 Information security management system 信息安全管理体系

4.4 Information security management system 信息安全管理体系The organization shall establish, implement, maintain and continually improve an information security management system, including the processes needed and their interactions, in accordance with the requirements of this document.组织应按照本文件的要求，建立、实现、维护和持续改进信息安全管理体系，包括信息安全管理体系所需的过程及其相互作用。

ISO/IEC 27001:2013标准 正文 4 组织环境/4.4 信息安全管理体系

4.4 信息安全管理体系组织应该按照本标准的要求，建立、实现、维护和持续改进信息安全管理体系。

标准解析：

1) 本条款（ISO/IEC 27001: 2022）条文与ISO/IEC 27001:2013相比，增加了“ 包括信息安全管理体系所需的过程及其相互作用 ”这句话，更加明确了，在建立信息安全管理体系的过程中，需要信息安全管理体系所需的过程及其相互作用。

2) 本条款规定了建立、实施、维护和持续改进信息安全管理体系的总体要求。ISO/IEC 27001：2022的其他部分描述了信息安全管理体系的要求要素，本条款就是要求组织建立的信息安全管理体系需要符合ISO/IEC 27001：2022其他所有的要求要素。

3) 要实现本条款要求，组织应该根据ISO/IEC 27001：2022的其他全部要求，建立信息安全管理体系一阶文件（信息安全管理纲领性文件、SOA适用性声明、信息安全策略集）、二阶文件（程序文件）、三阶文件（操作指南）以及四阶文件（记录表单）。

4) 其实早在ISO 9001：2015的“ 4.4 ”中，就有明确要求组织必须确定质量管理体系所需过程及相互关系

，也就是必须形成过程乌龟图以及过程关系图。所有可以借鉴ISO 9001：2015的实施，来理解和实施ISO/IEC 27001：2022中新增加的这句话（“ 包括信息安全管理体系所需的过程及其相互作用 ”），同时在ISO/IEC 27001：2022引言中，有特别强调，信息安全管理体系是组织的过程和整体结构的一部分并集成在其中，同时在ISO/IEC 27001：2022的“ 5.1 ”中也有强调，最高管理者应确保将信息安全管理体系要求整合到组织过程中。因此要满足本条款要求，组织必须将ISO/IEC 27001：2022相应的要求整合到组织原来的过程中，如内部审核过程，管理评审过程，人力资源管理过程、环境分析过程、相关方要求分析过程等，同时无法整合过程可以单独形成过程，如信息安全风险评估过程。

实施本条款应输出的文档：

1) 信息安全管理体系文件和记录清单。

2) 信息安全管理体系过程清单。

3) 信息安全管理体系过程关系图。

本条款审核要点：

1) 审核组织是否根据“ 4.3 ”的输出，策划信息安全管理体系的过程、文件和记录。

2) 检查文件清单和记录清单

ISO/IEC 27001: 2022标准 正文 5 Leadership 领导作用/5.1 Leadership and commitment 领导和承诺

5.1 Leadership and commitment 领导和承诺Top management shall demonstrate leadership and commitment with respect to the information security management system by:最高管理层应通过以下活动，证实对信息安全管理体系的领导和承诺：a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;a) 确保建立了信息安全方针和信息安全目标，并与组织战略方向一致；b) ensuring the integration of the information security management system requirements into the organization ’ s processes;b) 确保将信息安全管理体系要求整合到组织过程中；c) ensuring that the resources needed for the information security management system are available;c) 确保信息安全管理体系所需资源可用；d) communicating the importance of effective information security management and of conforming to the information security management system requirements;d) 沟通有效的信息安全管理及符合信息安全管理体系要求的重要性；e) ensuring that the information security management system achieves its intended outcome(s);e) 确保信息安全管理体系达到预期结果；f) directing and supporting persons to contribute to the effectiveness of the information security management system;f) 指导并支持相关人员为信息安全管理体系的有效性做出贡献；g) promoting continual improvement; andg) 促进持续改进；以及h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.h) 支持其他相关管理角色,以证实他们的领导按角色应用于其责任范围。NOTE Reference to “ business ” in this document can be interpreted broadly to mean those activities that are core to the purposes of the organization ’ s existence.注：本文件使用的“ 业务 ”一词可广义地理解为涉及组织存在目的的核心活动。

ISO/IEC 27001:2013标准 正文 5 领导/5.1 领导和承诺

5.1 领导和承诺最高管理者应通过下列方式展示其关于信息安全管理体系的领导力和承诺：a) 确保建立信息安全方针和信息安全目标，并与组织的战略方向保持一致；b) 确保将信息安全管理体系要求整

合到组织的业务过程中；c) 确保信息安全管理体系所需资源可用；d) 传达信息安全管理有效实施、符合信息安全管理体系要求的重要性；e) 确保信息安全管理体系实现其预期结果；f) 指挥并支持人员为信息安全管理体系的有效实施作出贡献；g) 促进持续改进；h) 支持其他相关管理角色在其职责范围内展示他们的领导力。

标准解析：

3) 本条款（ISO/IEC 27001: 2022）条文要素与ISO/IEC 27001:2013一样，仅仅增加了一个注解（注：本文件使用的“ 业务 ”一词可广义地理解为涉及组织存在目的的核心活动）。

4) 领导和承诺对于有效的信息安全管理体系至关重要。在ISO 9001：2015的“ 5.1 ”中有明确指出，最高管理者应对质量管理体系的有效性承担责任，这一要求同样适用于信息安全管理体系。

5) 最高管理者（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，这意味着最高管理者指导ISMS与组织中的其他领域类似，比如分配和监控预算的方式，最高管理者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，最高管理者是指导和控制该业务部门的个人或群体。最高管理者也参与管理评审（见9.3）和促进持续改进（见10.2）。

6) 最高管理者应主导组织的信息安全方针（见5.2）以及信息安全目标（见6.2）的确立，并要确保以上两者必须与组织战略方向一致。曾经就有一个面试官问过我一个这样的问题，制定公司目标的输入材料可以哪些方面去考虑？当时我的回答是三个方面：1）公司的战略规划，2）客户及相关方要求，3）法规法规及其他要求。面试官问之所以这个问题，是他们公司每次制定公司目标时，都无从下手，当时她听了我的答案后，显然很满意，这是因为我的回答完全跟ISO标准要求的是一致的，虽然她可能对ISO体系不是太懂，但还是认为从这几方面去考虑很有道理的。

7) 最高管理者应确保将信息安全管理体系要求整合到组织过程中，这一点至关重要，也是必须的，因为唯有如此，才能避免：1）信息安全管理体系流于形式，无法落地，2）信息安全管理体系成为负担，给正常业务造成严重的fumian作用。信息安全控制措施与业务流程结合的途径有：1）校准，2）整合，3）嵌入。整合的主要目的是降低对主营业务流程干扰，以更节约的方式促进信息安全制度的落地。更多更详细关于整合的介绍可以参考：赵秀堃，谢宗晓. 信息安全与组织业务流程结合探讨[J]. 中国标准导报，2016，07：36-38。另外，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需要最高管理层的支持。

8) 最高管理者宜确保有效的ISMS的资源的可用性（见7.1）。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）人力资源，3）设施，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。管理评审宜提供信息指明资源对组织是否是充足的。

9) 最高管理者宜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。

10) 最高管理者宜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。

11) 最高管理者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fumian影响。最高管理者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。

12) 最高管理者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。

13) 最高管理者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。实施本条款应输出的文档：

1) 信息安全管理层管理会议记录。

2) 信息安全方针和目标制定和评审记录。

3) 信息安全资源需求规划记录。

4) 信息安全管理评审、持续改进记录。

5) 信息安全激励记录。本条款审核要点：

1) 访谈最高管理者，了解组织信息安全规划和实施情况，作为最高管理者参与了哪些信息安全管理事项（如信息安全方针和目标制定和评审、管理评审、资源的提供等）。

2) 检查信息安全管理会议记录，查看最高管理者是否出席。

3) 检查信息安全方针和目标制定和评审记录，查看最高管理者是否签字批准。

4) 查看管理评审记录，检查最高管理者是否参与。

ISO/IEC 27001: 2022标准 正文 5 Leadership 领导作用/5.2 Policy 方针

5.2 Policy 方针Top management shall establish an information security policy that:最高管理层应建立信息安全方针，该方针应：a) is appropriate to the purpose of the organization;a) 与组织意图相适宜；b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives;b) 包括信息安全目标(见6.2)或为设定信息安全目标提供框架；c) includes a commitment to satisfy applicable requirements related to information security;c) 包括对满足适用的信息安全相关要求的承诺；d) includes a commitment to continual improvement of the information security management system.d) 包括对持续改进信息安全管理体系的承诺。The information security policy shall:信息安全方针应：e) be available as documented information;e) 形成文件化信息并可用；f) be communicated within the organization;f) 在组织内得到沟通；g) be available to interested parties, as appropriate.g) 适当时，对相关方可用。

ISO/IEC 27001:2013标准 正文 5 领导/5.2 方针

5.2 方针最高层管理者应建立信息安全方针，以：a) 适于组织的目标；b) 包含信息安全目标（见6.2）或设置信息安全目标提供框架；c) 包含满足适用的信息安全相关要求的承诺；d) 包含信息安全管理体系持续改进的承诺。信息安全方针应：e) 文件化并保持可用性；f) 在组织内部进行传达；g) 适当时，对相关方可用。

标准解析：

1) 本条款（ISO/IEC 27001: 2022）条文要素与ISO/IEC 27001:2013实质上是没有变化的。新版条文仅仅是把条款c)句尾的“ and ”shanchu了，从中文版来看，其实看不出变化的。

2) 本条款是常见体系标准（ISO 9001，ISO 14001以及ISO 45001等）通用条款，因此可以参照这些体系的实施方式进行实施。本条款可以与后面“ 6.2 信息安全目标及其实现规划 ”整合成“ 方针与目标管理过程 ”，此过程推荐与其他常见管理体系（ISO 9001，ISO 14001以及ISO 45001等）整合实施。

3) 最高管理者必须根据组织宗旨，组织战略，组织环境（4.1输出资料），相关方以及法律法规要求等（4.2输出资料）制定相适宜的信息安全方针，并批准。

4) 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。

5) 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。

6) 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。

7) 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。

8) 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（如培训，通告，会议宣导、布告栏、横幅等）。

9) 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。

10) 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)。

11) 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。

12) 信息安全方针应定期进行评审。

实施本条款应输出的文档：

1) 《方针与目标管理程序》（可选）。

2) 书面的信息安全方针，以及信息安全方针评审记录。

3) 信息安全方针培训与宣导证据（如培训记录、宣导资料、看板、会议记录等）。

本条款审核要点：

1) 检查信息安全方针是否有最高管理者批准。

2) 随机抽查员工是否知道信息安全方针。

3) 查看相关信息安全方针宣导和培训资料。