认 证 规 则

隐私信息管理体系认证规则

编 号：ZXB-PIMS-01-2025
受 控 状 态：受 控

版本	编修	审核	批准	编写/修订日期	发布日期
A/0	崔海军	张京梅	郑宇兵	20250418	20250530
A/0	崔海军	张京梅	郑宇兵	20250825	20250825

管理体系手册编制/修订履历

版本	修订内容	编写日期/修订日期	发布日期
A0	新编	20250418	20250530
A0	增加认证标志的要求内容	20250825	20250825

目 录

一、前言

大数据时代的到来，为我们带来了空前的便利，随着大数据在各个领域的渗透逐渐加深，个人隐私泄露的风险也愈加严重，人们对信息安全的关注日益提升，全球多个国家和地区相继出台了一系列隐私保护的法律法规，当前几乎所有的组织都有处理个人信息 (PII) 的情况，保护 PII 不仅是法律要求，也是社会需要。

因此，新标准 ISO/IEC 27701 隐私信息管理体系应势而生。助力组织为 GDPR 合规展现、保护用户隐私和个人信息合规管理提供了更多相关指南。2019 年 8 月 6 日，国际标准化组织 ISO 和国际电工委员会 IEC 正式对外发布 ISO/IEC 27701 隐私信息管理体系标准。这标志着信息安全、隐私与个人信息保护，在国际间法律与法规的合规展现有了一致性的标准。

该标准填补了目前隐私信息管理体系的空白，将隐私保护的原则、理念和方法，融入到信息安全保护体系中，并且对 PII 控制者和 PII 处理者进行了较为详细且落地性强的规定，细化了隐私信息管理的要求，给组织在隐私保护和信息安全方面给出了指导建议。作为一个国际通用的隐私信息管理工具，能够有效的协助组织对隐私风险进行识别、分析，采取措施将风险降到可接受水平并维持该水平，并建立隐私保护体系，从管理与技术等多方面满足国内外的监管合规要求。

二、适用范围

2.1 本规则用于规范众信标（北京）认证有限公司（以下简称：ZXB）对申请认证和获证的各类组织按照信息管理的扩展要求和指南 ISO /IEC 27701:2019《安全技术针对 ISO/IEC 27001 和 ISO/IEC 27002 在隐私信息管理的扩展要求和指南》标准建立适用于 PIMS 文件审核、编制审核计划及现场前的准备、审核组内部会议、第一阶段/第二阶段现场审核、不符合、对受审核方体系评价、监督审核、再认证等审核相关活动。

2.2 本规则适用于各类组织，包括但不限于企业、政府机构、事业单位、社会团体等。这些组织在其运营过程中，涉及对个人可识别信息（PII）进行收集、保存、传输、处置、使用、共享、转让、披露和委托处理等活动，均可依据本规则申请隐私信息管理体系认证。无论是大型跨国企业，还是小型初创公司；无论是传统行业，如制造业、金融业，还是新兴的互联网、大数据行业，只要存在处理 PII 的行为，都能适用本认证规则，以提升自身在隐私信息

管理方面的能力和水平，增强社会公信力和市场竞争力。

三、认证依据用技术规范、技术规范强制性要求或者标准

3.1 ISO/IEC 27701:2019《安全技术 - ISO/IEC 27001 和 ISO/IEC 27002 在隐私信息管理方面的扩展 - 要求与指南》：该标准详细规定了作为 PII 控制者和 PII 处理者的组织在隐私信息管理方面的特定目标和控制措施，从管理体系层面为组织提供全面指导，确保组织对隐私风险进行有效识别、分析，并采取相应措施，以符合高级别的隐私保护合规要求。

3.2 GB/T 22080/ISO/IEC 27001《信息技术 安全技术 信息安全管理体系要求》：作为信息安全管理体系的基础标准，其为隐私信息管理体系提供了必要的信息安全管理框架和基础要求。组织在构建隐私信息管理体系时，需遵循该标准中关于信息安全管理的通用要求，如信息安全策略制定、风险评估与处置、人力资源安全、物理和环境安全、通信和操作管理等方面的要求，以保障 PII 在整个生命周期中的安全性。

四、对认证人员的要求

4.1 认证人员基本要求

认证人员应当遵守与从业相关的法律法规，对认证活动及作出的认证审核报告和认证结论的真实性承担相应的法律责任。

4.2 隐私信息管理体系审核员资质要求

4.2.1 隐私信息管理体系审核员，应至少具备信息安全管理体系审核员资格；

4.2.2 需通过 ISO/IEC 27701 标准基础知识及相关从业法律法规的培训，并经过考试合格；

4.2.3 掌握相应隐私信息管理体系的知识和技能，经 ZXB 人员能力评价，确认符合要求，方可获得隐私信息管理体系审核员资格。

4.3 隐私信息管理体系认证人员专业能力评价准则，参考 ZXB-CX-11 认证人员管理程序。

五、认证实施程序

5.1 申请

5.1.1 组织要求：

申请认证的组织应具有明确的法律地位，如企业法人需提供营业执照等合法注册证明；非法人

组织需提供相应的登记注册文件或批准成立文件。组织应已按照认证依据标准建立了隐私信息管理体系，且体系文件涵盖了认证范围内的所有活动和流程，包括但不限于隐私政策、PII 处理流程说明、风险评估报告、内部审核程序等。

5.1.2 申请材料：

(1) 正式的认证申请书，应详细填写组织名称、地址、联系方式、申请认证范围、组织简介、业务范围等基本信息。

(2) 组织的法律地位证明文件复印件，如营业执照副本、事业单位法人证书等。若管理体系覆盖多场所活动，应附每个场所的法律地位证明文件的复印件（适用时）；

(3) 有关法律法规规定的行政许可证明、资质证书、强制性认证证书、备案证明等的复印件（适用时）；诚信守法记录或认证人员身份背景的要求，以及适用的与保守国家秘密或维护国家安全有关的法律法规要求。并在有需要情况下即时更新该说明，以便 ZXB 判断其是否具备对该客户实施认证活动的资格或条件。

(4) 隐私信息管理体系文件，包括手册、程序文件、作业指导书等，需清晰展示体系如何满足认证依据标准的各项要求。

(5) 体系运行的相关记录，如内部审核报告、管理评审报告、PII 处理活动记录、风险评估与处置记录等，以证明体系已有效运行至少 3 个月。

(6) 适用的法律法规清单，以及组织对这些法律法规合规性的说明，表明组织了解并遵循与隐私信息管理相关的国家和地方法规。

(7) 适用时，可要求客户指明其在申请认证的 PIMS 范围内与其他方共同提供服务的情况。

(8) 对 PIMS 认证范围涉及的业务活动的描述，包括利用信息技术为内部或外部顾客的业务过程提供支持的说明。

(9) 其他与认证审核有关的必要文件。

5.2 申请评审及方案策划

5.2.1 申请评审

认证机构收到申请材料后，将组织专业人员对申请材料进行全面评审。评审内容包括：

(1) 申请完整性审查：确认申请材料是否齐全，各项信息填写是否完整、准确，如申请书上的组织信息与法律地位证明文件是否一致，体系文件是否涵盖了标准要求的所有要素等。

(2) 认证范围合理性评估：审核申请的认证范围是否明确、合理，与组织的实际业务活动和 PII 处理活动是否相符。例如，若组织申请的认证范围包含某一业务线，但该业务线实际并不

涉及 PII 处理活动，则认证范围需进行调整。

(3) 体系文件符合性审查：初步审查组织提交的隐私信息管理体系文件是否符合认证依据标准的要求，文件之间的逻辑关系是否清晰，是否具有可操作性。如隐私政策是否明确告知 PII 主体关于 PII 的收集目的、方式、使用范围、存储期限、共享对象等关键信息；内部审核程序是否规定了审核的频率、方法、人员职责等。

(4) 体系运行有效性初步判断：通过对体系运行记录的审查，初步判断组织的隐私信息管理体系是否已按照文件要求有效运行。例如，内部审核报告是否显示按照计划进行了审核，且对发现的不符合项采取了相应的纠正措施。

若申请材料存在不完整、不准确或不符合要求的情况，认证机构将通知组织进行补充或修改。只有在申请材料通过评审后，认证机构才会受理组织的认证申请，并与组织沟通确定后续的认证安排。

5.2.2 方案策划

ZXB 应对整个认证周期制定审核方案，以清晰地识别所需的审核活动，这些审核活动用以证实认证客户的管理体系持续符合认证所依据的标准或其他规范性文件的要求。认证周期的审核方案应覆盖全部的管理体系要求。

通用审核方案（包括程序、通用要求等）由技术部负责组织制定，针对特定认证项目的项目审核方案由运营部负责策划。

初次认证审核方案包括两阶段初次审核、认证决定之后的第一年与第二年的监督审核和第三年在认证到期前进行的再认证审核。一个认证周期一般为三年，第一个三年的认证周期从初次认证决定算起，以后的周期从再认证决定算起。如果特定的行业认证方案有规定，认证周期可以不为 3 年。

对每个认证项目，应策划项目审核方案。在策划项目审核方案以及后续的调整时，应考虑申请客户的规模，其管理体系、产品和过程的范围与复杂程度，其生产过程和产品的安全风险程度，以及经过证实的管理体系有效性水平和以前审核的结果。

如果运营部鉴于申请客户已获的认证或由另一认证机构实施的审核，则应获取并保留充足的证据，例如报告和对不符合采取的纠正措施的文件。所获取的文件应为满足要求提供支持。运营部应根据获取的信息证明对审核方案的任何调整的合理性，并予以记录，并对以前不符合的纠正措施的实施进行跟踪。如果申请客户采用轮班作业，应在建立审核方案和编制审核计划

时考虑在轮班工作中发生的活动。

ZXB 在建立或修改审核方案时可能需要考虑的其他事项，如：收到的对申请客户的投诉；结合、一体化或联合审核；认证要求的变化；法律要求的变化；组织的绩效数据（例如缺陷水平、关键绩效指标（KPI）数据等）；利益相关方的关注。在确定审核范围和编制审核计划时可能也需要考虑这些事项。

a）PIMS 审核的审核方案应考虑所确定的信息安全控制。

b）对于审核方法不应预先假定 PIMS 实施的特殊方式或文件和记录的特殊格式，而应将重点放在确定客户满足 ISO/IEC 27001 和 ISO /IEC 27701 的要求和客户的策略与目标。

c）在初次审核的总体准备时，应要求客户为调阅内部审核报告和信息安全独立评审报告做出所有必要的安排。在认证审核的一阶段，客户应至少提供以下信息：PIMS 和其所覆盖活动的一般信息；ISO/IEC 27001 所规定的、必要的 PIMS 文件的副本，及必要的相关文件。

d）评审周期：如果一个 PIMS 没有至少实施过一次覆盖认证范围的管理评审和内部审核，运营部不予安排对该 PIMS 实施认证。

e）认证范围：审核组应根据所有适用的认证要求，对包含在确定范围内的客户 PIMS 进行审核。审核组应确认客户在其 PIMS 范围内满足了 ISO/IEC 27001 和 ISO /IEC 27701 要求。如不能满足要求时，需及时向运营部反馈。

运营部和审核组应确保：客户的信息安全风险评估和风险处置准确地体现了认证范围所界定的活动并扩展到活动的边界。运营部应确认这在客户的 PIMS 范围和适用性声明中得到了体现。运营部和审核组应验证每个认证范围至少有一个适用性声明。

运营部和审核组应确保：与不完全包含在 PIMS 范围内的服务或活动的接口，已在寻求认证的 PIMS 中得到说明，并已包括在客户的信息安全风险评估中。与其他机构共享设施（如：IT 系统、数据库和通讯系统或外包一项业务职能），是这类情形的一个示例。

f）认证审核准则：客户 PIMS 接受审核的准则应是 PIMS 标准 ISO/IEC 27001 和 ISO /IEC 27701。与所实施的业务相关的其他文件，也可以作为认证要求。

审核方案的策划，按《管理体系认证审核实施程序》的规定执行。

5.3 文件审核：

5.3.1 文件评审的目的是：了解受审核方的 PIMS 文件是否满足标准及相关法律法规的要求，从而确定能否进行现场审核；了解受审核方的 PIMS 概况，以便进行相关的审核准备工作。

5.3.2 文件评审的时机是：初次申请认证审核之前：填写《文件评审报告》，若无重大问题，

可进入第一阶段现场审核，并将文审发现问题结合第一阶段审核发现填入《第一阶段审核问题汇总表》中，无论如何，文件评审应结合第一阶段审核进行，并确保在第二阶段现场审核前完成；体系文件发生变化时现场审核之前：针对变化的部分进行评审，组长应在接到文件后尽快出具文件纠正通知（存在时）及文审报告，组长应确保文件评审应在现场审核前完成。

5.3.3 PIMS 文件审核的重点：

(1) 标准中所要求的建立文件化的 PIMS 是否完整；

(2) PIMS 文件层次、结构及相互关系是否清晰；

(3) 是否明确 PIMS 各个职能与层次的组织机构与职责；

(4) 风险评估的方法是否合理？如何进行风险评估与风险管理？及其有效性及充分性；

(5) 适用性声明中控制措施的选择及删减理由描述是否充分合理；

(6) 方针和目标、风险处置计划、运行、监测、纠正与预防措施等有逻辑关系的要素之间的接口关系是否描述清楚；

(7) 程序文件是否明确阐述该程序的目的和范围；职责是否清楚；程序及方法描述是否清晰并具可操作性；

5.3.4 文件审核的范围：

文件评审应覆盖 PIMS 标准 ISO/IEC 27001、 ISO/IEC 27701:2019 中要求，主要包含：

(1) PIMS 方针和控制目标；

(2) 审核 PIMS 的管理架构，各个职能层次上的机构与职责；

(3) 支持 PIMS 的规程和控制措施；

(4) 范围；

(5) 适用性声明（SOA）；

(6) 风险评估方法的描述；

(7) 风险评估报告；

(8) 风险处置计划；

(9) 组织为确保其信息安全过程有效策划、运行和控制以及描述如何测量控制措施的有效性所需的形成文件的规程；

(10) 组织应遵守的的法律法规清单或合同中的相关要求（含经营许可的要求）；

(11) 标准要求的形成文件的规程，如文件控制规程等；

(12) 标准所要求的记录。

5.3.5 文件审核其它关注点：

(1) 文件的格式：有效版本、审批、编号、受控、变更、标识、发布时间等信息。

(2) 文件审核的要求：符合性（与标准、法规）；系统性（包括组织全部信息安全管理活动的控制要求、标准规定的应形成程序的文件）；协调性（文件之间、有逻辑关系的要素之间）；有效性（现行有效、符合文件控制要求）；名词术语；

(3) 现场审核时仍需对体系文件进行审核，同时审核文件的合理性和可操作性。若发现的文件不符合情况，也应构成不符合项或审核发现问题清单（第一阶段审核）。

(4) 文件审核一般针对 4.3 中要求的文件。若认为不充分应要求受审核方提供补充文件。

(5) 办公室文件审核结论：a. 文审通过；b.对不符合要求处整改后验证；c.文审不通过。

(6) 在审核报告中应对办公室文件审核以及现场文件审核两方面的内容进行描述。

(7) 组长接到 PIMS 文件后应在现场审核前出具文件报告单。对于文件整改时间应结合问题的多少、解决难易、合同要求及与顾客协商作出。

(8) 在进行初次认证审核时文件审核应结合第一阶段审核进行，在审核发现问题清单中应体现文件审核中发现的问题，初次认证审核可不出具文件报告单，第一阶段审核报告中应包含文审的内容和结果。文件审查原则上由组长进行，必要时可由组内专业小类人员参与。

5.4 审核计划

5.4.1 审核计划的编制及现场审核前的准备要求

(1) 审核范围与合同评审单及审核工作通知一致；

(2) 按运营部安排进行审核时间、审核人员、审核人日数的安排；

(3) PIMS:按照专业类别及技术能力实施控制；

(4) 每天日程安排 8 小时，审核人员注明级别，按照要求实施评审、批准；

(5) 审核组长原则上应实施对最高管理层的审核；

(6) 审核组长应合理安排审核分工及审核时间。

除上述之外，在制定审核计划时，还应关注初次审核、监督审核、再注册及特殊项目审核时的要求。

5.4.2 计划评审/确认时组长应将《审核计划》及相关资料一齐交与审核计划评审人员进行评审确认。

5.4.3 组长做好审核前的布置工作，专业人员做好组内的专业培训工作，并按审核组内部会议的要求做好记录。

5.4.4 组长对组员编制的检查单把关，重点：a.覆盖计划中的条款；b.反映公司文件/产品/信息安全管理特点；c.满足标准要求（检查单左边的检查内容应尽可能详细书写）；d 带有验证审核任务的审核，验证审核员应对被验证审核人员的检查单进行把关。

5.4.5 审核计划应提前 5 个工作日传至受审核方，并沟通确认。审核组长应将受审核方确认的审核计划及时通知审核组组员，并着手进行审核安排。计划最终应由受审核方签字盖章带回。

5.4.6 审核计划如果在审核过程中发生变化，审核组长应在审核组内部会议记录中进行说明，并在交回审核资料时告知运营部资料接受人员，但变化不应影响到专业审核员对重要部门及场所的审核。

5.4.7 审核组内部会议要求

从审核组进入驻地直至审核结束，组长应充分利用审核组内部会议做好审核安排、沟通及控制，审核组内部会议应在现场审核开始前、每天审核结束后、末次会议开始前进行，并应在每次会议结束后进行记录。下述方面应至少涉及：

(1) 审核前的必要专业培训；

(2) 相关文件的熟悉；

(3) 审核分工及安排；

(4) 审核进度掌握及审核信息沟通；

(5) 审核组的内部审核评价；

(6) 审核结果的确定（包括不符合项及审核结论）。

审核过程中与审核策划不一致的内容及处理情况应重点进行记录；

5.5 多现场审核

公司 PIMS 多现场审核请依据《多现场审核管理规定》的要求进行。

当客户拥有满足以下 a)至 c)的多个场所时，审核员可以考虑使用基于抽样的方法进行多场所认证审核：

a） 所有的场所在同一 PIMS 下运行，并接受统一的管理、内部审核和管理评审；

b） 所有的场所都包含在客户组织的 PIMS 内部审核方案中；

c） 所有的场所都包含在客户组织的 PIMS 管理评审方案中。

无论如何，请审核员关注以下几点：

a） 审核员应审核 PIMS 中每个有重大信息安全风险的场所；

b） 无论在其总部或中心办公室或其他任一单一场所发现不符合，纠正措施的实施适用于该组

织的所有场所；

c） 在审核周期内（3 年获证期间），监督审核方案应覆盖其组织的所有场所。

5.6 认证范围的确定要求

审核组长在审核准备过程中，应在合同评审的基础上充分与受审核方进行沟通，充分了解与受审核方申请认证范围相关的企业特点、相关物理区域、组织状况、以及目前信息安全管理状况。如发现审核过程中企业实际状况与申请认证范围不一致，应充分与受审核方沟审核组应针对所有适用的认证要求，对包含在确定范围内的受审核方的 PIMS 进行审核。审核组应确保根据客户组织的业务、组织、位置、资产和技术的特点清晰地确定其 PIMS 的范围和边界。并确认受审核方在其 PIMS 范围内满足了 GB/T 22080-2016 中 1.2 的要求。

审核组保证按照 PIMS 标准 GB/T 22080-2016 的要求，受审核方的信息安全风险评估和风险处置与客户组织的活动及活动的边界相一致，并应确认这些都在受审核方的 PIMS 范围和适用性声明中得到体现。

审核组应确保，与不完全属于 PIMS 范围内的服务或活动的接口已在接受认证的 PIMS 中得到说明，并已包括在受审核方的信息安全风险评估中，例如，与其他机构共享设施的情况（信息技术系统、数据库和通讯系统等）。

认证范围的确定宜考虑下列因素：

a）文件化的适用性声明；

b）申请认证所涉及的活动、产品或服务的类别和性质；

c）与活动、产品或服务有关的场所及场所的分布状况和地理位置；

d）受审核方的特殊要求或现场审核观察，是否有需排除在审核范围之外的场所和地点。

e）受审核方的组织机构的设置及其管理权限所覆盖的范围。

此外，还应关注一下几个因素：

a）信息系统边界、平台、应用；

b）与不完全在 PIMS 范围内的服务或活动的接口（如与其它人共享的设施）；

c）组织所遵循的法规要求、标准和其他引用文件（注册要求、公告要求、经营者的证书、许可证等）；

认证范围举例说明：

与安全防范系统、计算机信息系统所涉及的隐私信息管理活动。

适用性声明：xxxxx x.x

5.7 不符合项纠正和纠正措施及验证要求

5.7.1 不符合的性质可分为两类：严重不符合和一般不符合。

严重不符合

失败的实施或遵守一个或多个标准适用的控制措施条款要求，因此产生关于对保护敏感信息的保密性、完整性和可用性测量的适当性的严重质疑，和/或一个无法接受的风险，可能未被组织的利害关系人觉察到。整个体系控制措施或程序的实效。

严重不符合项的部分范例如下：

a) 没有安全方针；

b) 没有安全事件管理系统；

c) 缺乏业务持续性计划；

d) 没有正式的系统来管理和更新 PIMS 文件；

e) 体系、控制措施，或程序的完全失效；

f) 极高数量的不符合项集中在标准中某一要素或是部门；

g) 未经批准的实行 PIMS 的变更；

h) 严重违背法律法规要求，后果较严重；

i) 相关方的严重投诉；

j) 上次发现的一般不符合重复发生等。

一般不符合

在一个隔离的环境中有一些适用控制措施的要求没有被满足，因此产生一些关于对敏感信息的保密性、完整性和可用性测量的适当的质疑。和/或表示一个轻微的风险，可能将被组织的利害关系人觉察到。被观察到的一个单独失误，或隔离的意外事件。

一般不符合项的部分范例如下：

a) 观察到的未遵守清空桌面和屏幕策略；

b) 在某种场合中访客离开场所时未登记；

c) 现场发现某天未按照备份策略进行备份等。

5.7.2 当审核发现体系运行中存在明显的不符合时，应在检查单中详细记录该不符合事实。

5.7.3 根据不符合事实记录开出不符合项报告。不符合项报告的事实应经受审核方陪同人员的见证，并由受审核方代表确认。

5.7.4 不符合项跟踪方式有三种：

1. 书面验证；2.现场验证；3.下次监督时验证。

具体详见 ZXB-CX-07 不符合及纠正措施、预防措施控制程序

5.8 综合评价及审核报告

审核组在离开客户审核现场前，审核组应在和组织管理层沟通会议和末次会议上和受审核方就以下两方面进行充分的沟通：

a) 受审核方 PIMS 与标准要求的符合性方面的书面或口头说明；

b) 受审核方就审核发现及其根据提出问题。

审核组向认证机构提供关于审核发现的审核报告，这些审核发现是针对客户组织的 PIMS 与所有认证要求的符合性，审核报告及体系评价从以下方面进行考虑。

a) 安全方针和目标的制定、实现；相应风险处理计划的有效性；

b) 风险评估、风险管理的适宜性和有效性；业务可持续性计划的有效性；

c) 是否形成了一套自我完善的机制；

d) 纠正和预防措施的有效性；

e) 员工的安全意识，有章必循的自觉性；

f) 法律法规的识别、获取、遵守情况；

g) 最高管理者的承诺；

h) 资源；

i) 职责；

j) 文件化 PIMS 建立及符合性；

k) 监视测量的实施及有效性；

审核结束后，组长应将文审相关证据（若有）、审核计划、审核检查单、不符合项及跟踪验证记录及审核报告等，按公司的文件资料清单要求整理成套，报公司技术部。

六、初次认证审核：

6.1 第一阶段审核

6.1.1. 审核第一阶段的目的的核心在于通过对组织的安全方针和目标的理解、以及对组织的审核准备状态的理解，为第二阶段的策划作准备。审核第一阶段应包括文件评审。审核组应和受审核方应就文件评审的时机和地点达成共识。无论如何，文件评审应在第二阶段阶段审核之

前完成。

6.1.2. 第一阶段审核主要侧重于组织的策划过程，在制定审核计划是应按照下面要求进行策划，主要内容为：

a) 通过现场观察，了解组织的基本概况，包括受审核方的范围，组织机构及职能，生产（或服务）的流程和特点，生产（或服务）活动的现场分布情况，生产（或服务）提供过程中对资产的保密性、完整性及可用性要求，资产清单中所列资产的物理位置等。

d) 通过收集有关安全方针方针、目标指标、风险评估及风险管理、以及为实现安全方针、目标指标、满足 PIMS 相关法律、法规要求所制定的风险处置计划和运行控制程序等信息，了解受审核方 PIMS 的整体情况；

c）通过收集组织识别风险、分析和评价风险、识别和评价风险处理的可选措施及为处理风险选择控制目标和控制措施，对受审核方风险评估的合理性、适用性以及可选控制措施的有效性作出初步评价；

d）评价受审核方识别 PIMS 相关法律、法规程序的有效性，以及组织遵守环境法律、法规及标准的状况；

e）审核组织的 PIMS 内审程序、内审计划和各项内审记录，对受审核方的内审程序和内审实施的有效性进行评价；评价管理评审的实施情况及有效性；评价组织自我完善和持续改进机制；

f）全员的信息安全意识是否具备；

g）体系文件的建立是否完备；在办公室文件审查的基础上，在现场进一步信息安全管理体系文件进行审查，考察其完整性、协调性、可操作性及合理性；

h）评价组织对相关方合同或协议中安全要求的识别情况，沟通程序的建立及执行情况；

i）现场调查过程中，应关注在生产、服务和活动过程中和 PIMS 直接相关的场所：

信息安全管理管理体系推进部门；

核心信息处理设施的放置场所；

IT 部门，设计、开发及维护部门；

与信息资产有关的现场；

6.1.3. 第一阶段审核完成后，审核组长应将审核资料及时提交技术部；如果第二阶段审核组长不是第一阶段审核组长，第一阶段审核组长应做好交接工作，将审核情况通报二阶段审核组长。

6.1.4. 第一阶段审核报告中评价的主要方面：

a）文件符合性结论；

b）体系建立和运行的基本情况；

c）组织机构和安全职责的合理性；

d）风险评估、风险管理方法策划的合理性及充分性；

e）适用于组织的 PIMS 法律、法规及合同要求的识别、获取和遵守情况；

f）目标、指标策划的合理性；

g）组织内审与管理评审的实施状况。

6.2 第二阶段审核

6.2.1. 第二阶段审核通常在组织的现场实施。审核组长根据第一阶段审核报告中报告的审核发现拟定第二阶段审核计划。第二阶段审核的目的如下：

a） 确认组织遵循了其方针、目标和程序；

b）确认组织的 PIMS 符合 PIMS 标准或规范性文件的所有要求并正在实现组织的方针目标；

6.2.2. 第二阶段审核应关注组织的以下内容：

c） 对信息安全相关的风险的评估和据此设计的 PIMS；

d） “适用性声明”；

e） 由此过程产生的目标和指标；

f） 根据目标和指标对绩效进行的监视、测量、报告和评审；

g） 安全和管理评审；

h） 信息安全方针的管理职责；

i） 方针、信息安全风险评估、目标和指标、职责、计划、程序、绩效数据及安全评审之间的联系。

6.2.3. 审核组应按公司程序文件《管理体系认证审核实施程序》实施现场审核。

6.2.4. 审核员现场实施审核时，应注意收集受审核方 PIMS 运行中的客观证据：

a）安全方针是否已得到贯彻实施；

b）安全目标、指标是否正在按规定的管理方案和计划进行；

c）重要的管理程序和运行控制程序是否已被严格遵守或执行；

d）体系中规定的日常监控和监测内容是否已执行；

e）内审和管理评审等是否已按规定实施。

6.2.5. 第二阶段审核报告评价内容：

体系的实施情况，是否正确的实施和保持：包括方针、目标指标和风险处理计划的实施完成情况，各种程序文件和作业指导书的执行情况；

内审和管理评审是否按程序规定执行。能否实现自我发现、自我纠正、自我完善的运行机制；受审核方 PIMS 实施的持续适宜性和有效性；审核发现的不符合项概述，以及实施完成纠正措施的要求；

不符合项纠正措施有效性验证情况。

受审核方的 PIMS 符合标准的情况。

七、复核、认证决定

7.1 复核

审核组完成现场审核后，将审核资料提交给认证机构的技术委员会或相关专业人员进行复核。复核的主要内容包括：

审核过程合规性审查：检查审核组的审核活动是否按照认证机构的审核程序和相关标准要求进行，审核计划的执行是否严格，审核方法是否得当，审核证据的收集是否充分、有效。例如，复核审核员在现场检查时是否对标准要求的所有条款都进行了合理的抽样检查，审核记录是否清晰、准确地反映了审核过程和发现的问题。

不符合项判定准确性评估：对审核组判定的不符合项进行重新评估，确认不符合项的描述是否准确、清晰，判定依据是否充分，不符合项的性质划分是否合理。例如，复核严重不符合项的判定是否确实符合严重不符合项的定义，是否有足够的证据支持该判定。

审核结论合理性审查：审查审核组给出的审核结论是否客观、公正，是否基于充分的审核证据。审核结论通常包括推荐通过认证、有条件通过认证（需在规定时间内完成不符合项整改并经审核组验证）、不通过认证三种情况。复核人员将综合考虑审核过程中的各项因素，判断审核结论是否恰当。

若复核过程中发现问题，认证机构将与审核组沟通，要求审核组进行补充说明或采取相应的纠正措施。只有在复核通过后，认证机构才能根据审核结果做出认证决定。

7.2 认证决定

7.2.1 ZXB 在对审核报告、不符合项的纠正和纠正措施及其结果进行综合评价基础上，作出认证决定。

7.2.2 审核组成员不得参与对审核项目的认证决定。

7.2.3 认证决定人员在作出认证决定前应确认如下情形：

（1）审核报告符合本规则第 5.4 条要求，能够满足作出认证决定所需要的信息；

（2）反映以下问题的不符合项，ZXB 已评审、接受并验证了纠正和纠正措施及其结果的有效性：

① 未能满足社会责任及管理体系标准的要求；

② 制定的目标不可测量、或测量方法不明确；

③ 对实现目标具有重要影响的关键点的监视和测量未有效运行，或者对这些关键点的报告或评审记录不完整或无效；

④ 在持续改进隐私信息管理体系及管理体系的有效性方面存在缺陷，实现业务连续性目标有重大疑问。

（3）ZXB 对其他不符合项已评审，并接受了申请组织计划采取的纠正和纠正措施。

7.2.4 在满足 5.6.3 条要求的基础上，对有充分的客观证据证明申请组织满足下列要求的，ZXB 将评定该申请组织符合认证要求，向其颁发认证证书：

（1）申请组织的隐私信息管理体系符合标准要求且运行有效；

（2）认证范围覆盖的产品或服务符合相关法律法规要求；

（3）申请组织按照认证合同规定履行了相关义务。

7.2.5 申请组织不能满足上述要求的，评定该申请组织不符合认证要求，以书面形式告知申请组织并说明其未通过认证的原因。

7.2.6 ZXB 在颁发认证证书后 30 个工作日内按照规定的要求将相关信息报送国家认监委。证书信息可在：国家认证认可监督管理委员会官方网站（www.cnca.gov.cn）或众信标（北京）认证有限公司官方网站（www.zhongxinbiao.com/）上查询。

7.2.7 ZXB 不得将申请组织是否获得认证与参与认证审核的审核员及其他人员的薪酬挂钩。

八、监督

8.1 监督审核的目的：验证获证组织的PIMS是否持续满足认证标准的要求，或考察组织运行引起的PIMS的变化是否符合认证要求。

8.2 监督审核的要求：

8.2.1 监督审核可采用抽样的方式进行。对各部门、相同的现场的抽样须三年内全部覆盖。PIMS的推进部门及重要部门每次都应进行审核。如果获证组织上的分布于几个不同的场所，每监督审核可针对不同的现场进行抽样，但应确保在三年中覆盖全部现场，其中每年对其总部的审核应至少一次。

8.2.2 每次监督审核应涉及全部PIMS要素，三年内的不同次监督审核对各个要素审查的深度和广度可各有侧重，告别应注意对上次现场审核遗留问题的验证。

8.2.3 较之初次审核，监督审核的要求不仅不应放松，反而应适度从严，如发现与上次审核相同的问题，应考虑不符合项性质的升级。

8.2.4 监督审核的主要内容：

每次监督审核均应特别关注以下内容：

a）PIMS在实现组织的安全方针、目标方面的持续有效性；

b）PIMS因素的变化及控制；

c）文件化的PIMS的变更；

d）体系的保持，即内审、管理评审、预防和纠正措施；

e）组织高层及全员的安全意识；

f）组织有关PIMS法律法规的变化及符合性的定期评价工作是否有效；

g）为实现整体安全绩效的改进，依据组织的安全方针对PIMS加以不断改进并采取的方案措施、计划等的进展情况；

h）与相关方的信息交流，包括有关安全要求识别、记录及反应程序以及执行情况；

i）上次审核中发现的不符合所采取的现场验证；

j）体系范围的变更；

k）认证证书、标志和报告的使用和宣传情况；

l）内部运行及监测情况；

m）选定的其它审核内容。

监督审核每次必查条款： A.5，A.6.1，A.7.1，A.9.1，（A10、A11、A12每次要抽查，三年全覆盖。每次监督审核必查项A.10中A.10.4；A.10.6；A.10.10；A.11中的A.11.1，A.11.2，A.11.6 ；A.12中的A.12.1和A.12.4)，A.13，A.14，A.15.1

主业务部门、主实施部门、体系推进部门均要涉及。

其他条款三年覆盖一遍。

8.3 监督审核时间间隔每两次不应超过12个月，若企业由于季节性生产或其他原因不能按原计划进行复查，需调整时间安排时，应由受审核方提出书面文件（传真件也可）说明推迟理由，由运营部相应人员将书面文件提交公司领导批准。相关资料应保存至运营部，最多可以延长1个月，涉及如认证合格证书上覆盖产品范围扩大类别等重大事由，应通知运营部办理相关补充合同。若企业变更地址、名称时，由审核组长在现场审核时确认并带回证据。

8.4 监督审核的现场审核与初审程序一致，审核组长在监督审核现场审核时，将监督审核收费通知单交与受审核方。

8.5 监督审核结论为：a）证书继续有效；b）证书暂停；c）证书撤销。

8.6 在监督审核现场审核末次会议上，监督审核组长应向获证单位清楚说明对不合格项的纠正期限及以下相关内容：

证书继续有效：

a）一般不符合项：一般一个月内完成纠正措施且有效；

b）严重不符合项：一般半个月内完成纠正措施且有效。

证书暂停：

a）获证组织私自对证书进行了更改；

b）获证组织体系运行达不到规定的要求，但严重程度并不构成撤销认证资格。

证书撤消：

a）证书暂停后，在规定时间内按规定要求采取适当纠正措施；

b）存在严重不符合规定要求的情况。

8.7 监督审核报告至少覆盖下述内容：

(1) PIMS是否得到正确的实施和保持。

(2) PIMS是否确保持续适用性和有效性。

(3) 组织是否持续遵守PIMS相关法律法规及其它要求，有无违法现象。

(4) 不符合项是否破坏体系的完整性、有效性，是否得到纠正。

(5) 是否推荐保持认证证书或暂停，撤销认证证书。

(6) 对下一次监督审核应关注的要点及需要重点抽查的要素提出线索和建议。

8.8 监督审核后做好资料整理上报工作，提交审核案卷的时限要求是现场审核结束后45天内。

8.9 审核组长负责编写监督审核报告，并交技术部审查。技术部资料审查内容按照《管理体系

认证决定审批意见》进行。

8.10 监督审核资料经授权评定人员审查后，技术部将监督审核的全部资料进行归档。

九、再认证

9.1 运营部根据签订合同后的复评企业汇总情况，结合实际情况制定具体的再认证工作实施计划。

9.2 运营部根据审核任务及计划下发审核通知单，指定复评组长。获证单位的任何变更信息，应根据合同评审单中的内容，在复评工作通知单中写明,并要求做文件审查。

9.3 复评工作所需人日数在认证基础无更改的情况下，按相当于初次审核的 2/3 人日数进行。若有变动应根据实际情况加大复评力度。

9.4 复评工作程序与正式审核程序相同。

9.5 文件审核，按《管理体系认证审核实施程序》进行。

9.6 审核准备，按《管理体系认证审核实施程序》进行。

9.7 现场审核，按《管理体系认证审核实施程序》进行。

9.8 审核报告的编写、发放与批准，按《管理体系认证审核实施程序》进行。

9.9 再认证的审核内容应结合初次认证注册审核第一阶段和第二阶段的审核内容，应考虑上次审核的结果并至少包括 PIMS 文件的审核和所有认证范围的现场审核；还应检查组织投诉、申诉及其所采取的纠正措施记录，至少应确保组织：

a）PIMS 的所有要素之间统一协调；

b）发生变更后，PIMS 运行良好；

c）PIMS 得到有效的保持；

9.10 审核资料的上报、审查、评定、归档与上相同

9.11 再认证换证后对获证单位每年进行一资监督审核。监督审核工作程序按《管理体系认证审核实施程序》进行。

十、认证证书状态管理规定、要求

认证的批准、拒绝、保持、扩大、缩小、暂停、恢复或撤销认证证书

10.1 批准认证资格

10.1.1 批准认证资格条件：

（1）认证申请材料真实、准确、有效；

（2）受审核方建立和实施的隐私信息管理体系符合认证标准/规范性文件要求，审核组提出推荐认证的结论意见；

（3）受审核方审核的认证范围在法律地位文件和资质规定的范围内；

（4）国家或地方或行业有要求时，受审核方申请的认证范围内的组织单元、产品、服务及其过程和多动以满足使用额法律法规要求；

（5）审核证据表明管理评审和内部审核的安排已实施、有效且得到保持，并已进行了一次覆盖隐私信息管理体系所有要求的完整内部审核和管理评审；

（6）审核中发现的不符合在规定期限内已采取纠正/纠正措施，经认证机构验证有效；

（7）认证申请方已与 ZXB 签订认证合同，承诺始终遵守认证有关规定，并按认证合同规定缴纳认证费用。

10.1.2 批准认证

（1）满足批准认证资格的条件，经 ZXB 评定，认为认证客户在认证范围内已满足批准认证资格的条件，同意批准认证注册；

（2）ZXB 向认证客户颁发认证证书，要求获证客户按规定使用认证标志。

10.2 拒绝认证

（1）经 ZXB 技术部评定，被认证客户的隐私信息管理体系不满足批准认证注册的条件，不予批准认证注册。运营部制作《不予认证注册通知》；

（2）ZXB 法定代表人或授权人签发《不予认证注册通知》；

（3）运营部向被认证客户发出《不予认证注册通知》；

（4）经评审不予受理的认证申请，有运营部通知认证申请组织；

（5）现场审核为“不推荐注册”结论的，有 ZXB 法定代表人或授权人签发《不予认证注册通知》。

10.3 保持资格

10.3.1 保持认证资格的条件：

（1）获证组织的法律地位、资质持续符合国家的最新要求，并且认证范围在法律地位文件和资质规定的范围内；

(2)获证组织的隐私信息管理体系持续符合认证标准/规范性文件要求；

(3)获证组织持续避守认证有关的规定，包括变更的规定；

(4)获证组织在认证范内的组织单元、产品、服务及其过程和活动持续满足适用的最新法律法规的要求，如发生不满足时及时采取有效的措施；

(5)获证组织于获证期间在认证范围内未发生重大事故和国家检查不合格；

(6)获证组织在获证期间未发生误用认证证书和认证标志，如有发生能及时有效地采取纠正和纠正措施，并将误用产生的影响降至最少程度；

(7)获证组织对顾客或相关方的重大投诉和关切能及时有效地处理；

(8)管理评审、内审每年至少进行一次，原则上两次内审时间不超过 12 个月；

(9)按时接受监督审核的；

(10)获证组织能按照 ZXB 要求向 ZXB 通报隐私信息管理体系和重要过程变更等信息；

(11)获证组织履行与 ZXB 签订认证合同中规定的责任和义务，并按照认证合同规定缴纳认证费用。

10.3.2 保持认证资格：

(1)满足保持认证资格的条件，监督审核后经 ZXB 的审核组长确认后，认为获证组织在认证范围内能持续满足保持认证资格的条件，同意保持认证资格，由 ZXB 签发确证书并向获证组织发放；

(2)在认证证书有效期内如有认证要求变，获证组织接受变更的认证要求，并经 ZXB 验证在认证范围内管理体系满足变更的要求，可保持认证资格。

10.4 扩大认证范围

10.4.1 扩大认证范围的条件：

获证组织保持认证资格有效；

国家、地方或行业有要求时，获证组织在扩大认证范围内具有规定的资质

(3)获证组织申请扩大认证范围在法律地位文件和资质规定的范围内；

(4)获证组织的管理体系覆盖申请扩大的认证范围，并符合认证标准/规范性文件要求 ；

(5)国家或地方或行业有要求时，获证组织在申请扩大认证范围内的组织单元、产品、服务及

其过程和活动已满足适用的法律法规的要求；

（6)获证组织按照认证规定缴纳补充认证费用。

10.4.2 扩大认证范围：

（1）获证组织向 ZXB 正式提交扩大认证范围的申请和相关附件；

（2）满足扩大认证范围的条件，经 ZXB 审核、评定，认为获证组织在申请扩大认证范围内已满足批准认证资格的条件，同意批准扩大认证范围，认证证书的注册号和有效期保持不变。

10.5 缩小认证范围

10.5.1 缩小认证范的条件：

（1）组织的认证范围内部分产品服务范围、区域等不再符合认证标准/规范性文件和其他附加要求；

（2）获证组织不愿再继续保持认证范围内的部分产品服务范围、区域等认证资格；

（3）获证组织缩小认证范围应不包括为缩小认证风险的情况。

10.5.2 缩小认证范围

（1）获证组织向 ZXB 正式提交缩小认证范围的申请，或 ZXB 提出缩小获证组织认证范围的建议，并提供理由和证据 ZXB 的评定意见和日常监督结果也可作为认证范围缩小的信息来源和理由。经认证双方沟通后达成一致意见；

(2)经 ZXB 评定，认为获证组织在申请缩小认证范围不会对仍保持的认证范围产生影响，同意批准缩小认证范围，收回原认证证书，换发认证证书或附件，认证证书的注册号和有效期保持不变；

（3）需要时，获证组织与 ZXB 补充签订认证合同。

10.6 暂停证书

10.6.1 获证组织有以下情形之一的，ZXB 应在调查核实后的 5 个工作日内暂停其认证证书：

（1）隐私信息管理体系及管理体系持续或严重不满足认证要求，包括对隐私信息管理体系及管理体系运行有效性要求的；

（2）不承担、履行认证合同约定的责任和义务的；

（3）被有关执法监管部门责令停业整顿的；

（4）被地方认证监管部门发现体系运行存在问题，需要暂停证书的；

（5）持有的与行政许可证明、资质证书、强制性认证证书等过期失效，重新提交的申请已被受理但尚未换证的；

（6）主动请求暂停的；

（7）其他应当暂停认证证书的。

10.6.2 认证证书暂停期不得超过 6 个月。但属于 8.2.1 第（5）项情形的暂停期可至相关单位作出许可决定之日。

10.6.3 ZXB 暂停认证证书的信息，应明确暂停的起始日期和暂停期限，并声明在暂停期间获证组织不得以任何方式使用认证证书、认证标识或引用认证信息。

10.7 恢复认证资格

10.7.1 恢复认证资格的条件：

恢复认证资格的条件获证组织已针对暂停认证资格的原因采取了有效的纠正措施，产生原因已经消除，恢复符合相关的认证要求，同时已证实在暂停期内没有使用引用认证资格，广告宣传和使用标志。

10.7.2 恢复认证资格

在确定的认证资格暂停限期结束前，根据暂停原因，组织在规定期限内向 ZXB 运营部提出恢复认证资格的申请，并附相关纠正措施和有效性验证材料 ；

经 ZXB 评定，确认组织在暂停认证资格的认证范围内已恢复符合相关的认证要求，作出同意恢复认证资格的评定结论，颁发《恢复使用认证证书和标志的通知》并公告。

10.8 撤销证书

10.8.1 获证组织有以下情形之一的，ZXB 应在获得相关信息并调查核实后 5 个工作日内撤销其认证证书：

（1）被注销或撤销法律地位证明文件的；

（2）拒绝配合认证监管部门实施的监督检查，或者对有关事项的询问和调查提供了虚假材料或信息的；

（3）出现重大的与隐私信息管理体系相关的事故，经执法监管部门或经 ZXB 确认是获证组织违规造成的；

（4）有其他严重违反法律法规行为的；

（5）暂停认证证书的期限已满但导致暂停的问题未得到解决或纠正的（包括持有的行政许可证明、资质证书、强制性认证证书等已经过期失效但申请未获批准）；

（6）没有运行隐私信息管理体系及管理体系或者已不具备运行条件的；

（7）不按相关规定正确引用和宣传获得的认证信息，造成严重影响或后果，或者 ZXB 已要求

其纠正但超过6个月仍未纠正的；

（8）其他应当撤销认证证书的。

10.8.2 撤销认证证书后，ZXB应及时收回撤销的认证证书。若无法收回，ZXB应及时在相关媒体和网站上公布或声明撤销决定。

10.9 ZXB暂停或撤销认证证书应当在其网站上公布相关信息，同时按规定程序和要求报国家认监委。

10.10 ZXB有义务和责任采取有效措施避免各类无效的认证证书和认证标志被继续使用。

10.11 ZXB应制定批准、拒绝、保持、扩大、缩小、暂停、恢复或撤销认证证书或缩小认证范围的规定，并形成文件化的管理制度.

十一、影响认证的变更

11.1 变更地址：按照《管理体系认证审核实施程序》执行

11.2 变更名称：提供新法人执照、变更申请、体系变更申请表、更名后的方针文件、适用性声明、证书制作单、注册审定批准表。技术部将资料审核后报总经理批准。

11.3 扩大、缩小范围：

11.3.1. 单独扩项按照初审资料提供、填写和审查。

11.3.2. 结合监督按照监督资料提供、填写和审查，但须将扩项内容填在审核计划、审核报告中。

11.4 暂停、撤销后的审核要求：应根据暂停时间长短，由运营部适当增加人日数，并在审核通知单中明示告知组长。

十二、认证证书及认证标志的要求

12.1 认证证书应至少包含以下信息：

（1）获证组织名称、地址和组织机构代码。该信息应与其法律地位证明文件的信息一致；

（2）隐私信息管理体系及管理体系覆盖的生产经营或服务的地址和业务范围。若认证的隐私信息管理体系及管理体系覆盖多场所，表述覆盖的相关场所的名称和地址信息，该信息应与相

应的法律地位证明文件信息一致；

（3）隐私信息管理体系及管理体系符合隐私信息管理体系标准的表述；

（4）证书编号；

（5）ZXB 名称；

（6）证书签发日期及有效期的起止年月日。

对初次认证以来未中断过的再认证证书，可表述该获证组织初次获得认证证书的年月日。

（7）相关的认可标识及认可注册号（适用时）；

（8）证书查询方式。ZXB 除公布认证证书在 ZXB 网站上的查询方式外，还应当在证书上注明：“本证书信息可在国家认证认可监督管理委员会官方网站（www.cnca.gov.cn）上查询”，以便于社会监督。

12.2 认证证书有效期最长为 3 年。

12.3 ZXB 建立证书信息披露制度。除向申请组织、认证监管部门等执法监管部门提供认证证书信息外，还应当根据社会相关方的请求向其提供证书信息，接受社会监督。

12.4 认证要求变更

认证要求变更时，ZXB 及时将认证要求变更的文件发给所有相关的获证组织，同时将认证要求的变更信息通过网络向社会公告。ZXB 根据认证要求变更的性质和内容，采取适当方式对获证组织实施变更后的认证要求有效性的验证，如文件审查、现场补充审核。ZXB 最终根据以上步骤确认认证要求变更后获证组织的证书有效性.

12.5 认证标志要求

a)获证客户在传播媒介(如互联网、宣传册或广告)或其他文件中引用认证状态时，应符合 ZXB 的要求。

b）使用 ZXB 的认证标志，需向 ZXB 提出申请。在使用时，其图案必须按照 ZXB 提供的 图案的比例放大或缩小，并且做到颜色一致。未经 ZXB 许可不得使用认证标志；

c）不得在任何资料中有关于其认证资格的误导性说明； d）不得以误导性方式使用认证文件或其任何部分；

e）不得利用管理体系认证证书和相关文字、符号，暗示或误导公众认为认证证书覆盖 范围外的管理体系、产品或服务、过程、活动和场所获得 ZXB 的认证；

f）宣传认证结果时不得损害 ZXB 的声誉和（或）使认证制度声誉受损，失去公众信任；g）不得擅自更改证书内容；

h）不得伪造、涂改、出借、出租、转让、倒卖、部分出示、部分复印证书；

i）获证客户应妥善保管好认证证书，以免丢失、损坏；

j）获证客户的管理体系若发生重大变化时，应及时报告 ZXB ，接受 ZXB 的调查或监督 检查。对经监督检查不合格者，不得继续使用认证证书；

k）在认证范围被缩小时，应及时修改所有的广告宣传材料；

l）认证证书被暂停期间，相应的认证领域的管理体系认证暂时无效。认证客户应停止 使用认证证书和认证标志，直到造成暂停的问题得到解决。如果客户在规定的时限内未能解 决造成暂停的问题，ZXB 将撤销或缩小相应领域的认证范围；

m）证书被 ZXB 撤销，获证客户应按 ZXB 的要求将证书交还给 ZXB ，并同时使用所有引 用认证资格的广告材料。停止在文件、网站、广告和宣传资料中或广告宣传等商业活动，以 及在工作场所、销售场所展示认证证书；

n）不应允许其标志被获证客户用于实验室检测、校准或检验的报告或证书；

o）标志不应用于产品或产品包装之上，或以任何其它可解释为表示产品符合性的方式 使用；注：产品包装的判别标准是其可从产品上移除且不会导致产品分裂、破裂或损坏。

p）认证证书和认证标志的使用应符合《认证证书和认证标志管理程序》的规定；

q）认证标志使用时可以等比例放大或缩小，但不允许变形、变色；

r）证书持有人应对认证证书和认证标志的使用和展示进行有效的控制。

十三、信息通报

获证组织应建立向 ZXB 通报最新信息的程序，并及时通报顾客的重大投诉、国家监督检查结果、重大事故及组织变更的各种信息等变更信息包括(但不限于)以下:法律地位、经营状况、组织状态或所有权取得的行政许可资格、强制性认证或其他资质变更;组织和管理层(如关键的管理、决策或技术人员);联系地址和场所获证隐私信息管理体系覆盖的范围;隐私信息管理体系和重要过程的重大变更。

十四、受理申诉和投诉

获证组织对认证决定有异议时，ZXB 应接受获证组织申诉并且及时进行处理，在 60 日内将处

理结果形成书面通知交获认证组织。书面通知应当告知获证组织，若认为 ZXB 未遵守认证相关法律法规或本规则并导致自身合法权益受到严重侵害的，可以直接向所在地认证监管部门或国家认监委投诉，也可以向相关认可机构投诉。

十五、记录管理

15.1 ZXB 应当建立认证纪录保持制度，记录认证活动全过程并妥善保存。

15.2 记录应当真实准确以正式认证活动得到有效实施。保存时间至少应当与认证证书有效期一致。

15.3 记录可以用纸质或电子文档的方式加以保存。

附录 A：隐私信息管理体系认证审核时间表

有效人数	审核时间（第 1 阶段 + 第 2 阶段，天）
1 - 50	1.5
51- 100	2.5
101 - 150	3.5
151 - 200	4.5
>200	遵循上述递进规律

注：可根据因企业规模、复杂程度实际情况调整。

版本	编修	审核	批准	编写/修订日期	生效日期
A/0	崔朝敏	李　蒙	白金泽	2018-03-27	2018-04-01
A/1	崔朝敏	李　浩	刘　东	2019-01-01	2019-01-01
B/0	崔朝敏	李　浩	刘　东	2019-06-12	2019-06-20
B/1	张　鑫	李　浩	刘　东	2020-03-06	2020-03-11
C/0	罗　焕	张京梅	李　浩	2021-03-02	2021-03-03
C/1	毕金霞	张京梅	李　浩	2021-11-16	2021-11-16
D/0	马　林	张京梅	李　浩	2022-02-14	2022-02-15
D/1	马　林	张京梅	郑宇兵	2023-11-21	2023-11-21
D/2	张京梅	张京梅	郑宇兵	2025-08-07	2025-08-07

1、范围

本程序规定了对组织进行质量管理体系(QMS)、环境管理体系(EMS)、职业健康安全管理体系(OHSMS)、信息安全管理体系（ISMS）、基于 ISO/IEC 20000-1 的服务管理体系（SMS）、能源管理体系（EnMS）实施认证审核的全过程管理，以规范和控制认证审核活动。

本程序适用于初次审核、监督审核和再认证审核。

2、职责

运营部负责对组织的管理体系进行初次审核、监督审核和再认证审核实施全过程的管理。

3、引用文件

下列文件中的条款通过本文件的引用而成为本文件的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本文件。凡是不注日期的

引用文件，其最新版本适用于本文件。

1、 CNAS-CC01:2015 《管理体系认证机构要求》（ISO/IEC 17021-1:2015）

2、 CNAS-CC121:2017 《环境管理体系审核及认证的能力要求》（ISO/IEC 17021-2:2016）

3、 CNAS-CC131:2017《质量管理体系审核及认证的能力要求》（ISO/IEC 17021-3:2017）

4、 CNAS-CC125_2018《职业健康安全管理体系审核及认证的能力要求》

5、 CNAS-CC170:2015《信息安全管理体系认证机构要求》

6、 CNAS-CC175:2017《基于 ISO-IEC 20000-1 的服务管理体系认证机构要求》

7、 CNAS-CC190：2021《能源管理体系认证机构要求》

8、 CNAS-CC11_2018《多场所组织的管理体系审核与认证》

9、 CNAS-CC106_2023《CNAS-CC01 在一体化管理体系审核中的应用》

10、 GB/T 19011-2021 《管理体系审核指南》(ISO19011:2018,IDT)

11、 GB/T19001-2016 《质量管理体系 要求》（ISO9001:2015,IDT）

12、 GB/T50430-2017 《工程建设施工企业质量管理规范》

13、 GB/T24001-2016 《环境管理体系 要求及使用指南》（ISO14001:2015,IDT）

14、 GB/T45001-2020《职业健康安全管理体系 要求及使用指南》（ISO 45001:2018，IDT）

15、 GB/T 22080-2016 《信息技术 安全技术 信息安全管理体系 要求》（ISO/IEC 27001-2013,IDT）

16、 ISO/IEC 20000-1:2018《信息技术 服务管理 第 1 部分：服务管理体系要求》

17、 GB/T 23331-2020 《能源管理体系 要求及使用指南》

18、 《质量管理体系认证规则》

19、 《信息技术服务管理体系认证实施规则》

20、 CNAS-SC125_2020《职业健康安全管理体系认证机构认可方案》

21、 CNAS-SC15:2018《工程建设施工企业质量管理体系认证机构认可方案》

22、 CNAS-SC170:2017 《信息安全管理体系认证机构认可方案》

23、 CNAS-SC175:2017《基于 ISO/IEC 20000-1 服务管理体系认证机构认可方案》

24、 CNAS-SC190:2021《能源管理体系认证机构认可方案》

25、 CNAS-SC25：2023《服务认证机构认可方案》

4、术语和定义

ISO 9000、ISO 19011、ISO 9001、ISO 14001、ISO 45001、GB/T 50430、ISO/IEC 27001、ISO/IEC 20000-1 和 ISO/IEC 17021-1、ISO/IEC 17021-2、ISO/IEC 17021-3、ISO/IEC 27006 等中给出的术语和定义适用于本文件。

5、 工作流程

5.1 审核准备

5.1.1 认证申请

由 ZXB 运营部负责向客户提供公开文件，并接收申请客户的认证申请。认证申请的具体实施，按《受理认证申请及申请评审程序》执行。

5.1.2 认证申请评审

由 ZXB 运营部负责在签订认证协议前对认证申请进行评审。申请评审的具体实施，按《受理认证申请及申请评审程序》执行。

5.1.3 ZXB 运营部在认证申请评审后，应作出接受或拒绝申请的决定。当基于申请评审的结果是拒绝认证申请时，应记录拒绝申请的原因并使客户清楚拒绝的原因。

5.1.4 当接受认证申请时，认证审核方案管理人员应对整个认证周期制定审核方案，以清晰地识别所需的审核活动，这些审核活动用以证实客户的管理体系符合认证所依据标准或其他规范性文件的要求。认证周期的审核方案应覆盖全部的管理体系要求。初次认证审核方案应包括两阶段初次审核、认证决定之后的第一年与第二年的监督审核和第三年在认证到期前进行的再认证审核。第一个三年的认证周期从初次认证决定算起，以后的周期从再认证决定算起。如果特定的行业认证方案有规定，认证周期可以不为 3 年。审核方案的确定和任何后续调整应考虑组织的规模，其管理体系、产品和过程的范围与复杂程度，生产过程和产品的安全风险程度，以及经过证实的管理体系有效性水平和以前审核的结果。如果申请客户采用轮班作业，应在建立审核方案时考虑在轮班工作中发生的活动。为了解组织是否已具备实施认证审核的条件，必要时可安排进行预访问。

对于信息安全管理体系审核方案除了上述要求外，ZXB 还需符合以下要求：

a）ISMS 审核的审核方案应考虑所确定的信息安全控制；

b）对于审核方法不预先假定 ISMS 实施的特殊方式或文件和记录的特殊格式，而是要

求将重点放在确定客户的 ISMS 满足 ISO/IEC 27001 的要求和客户的策略与目标；（ISO/IEC 27007《信息技术 安全技术 信息安全管理体系审核指南》为 ISMS 审核方案管理、审核实施等内容提供了指南，ZXB 将会参考采用。）

c）在初次审核的总体准备时，运营部应要求客户为调阅内部审核报告和信息安全独立评审报告做出所有必要的安排。在认证审核的一阶段，客户应至少提供以下信息：ISMS 和其所覆盖活动的一般信息；ISO/IEC 27001 所规定的、必要的 ISMS 文件的副本，及必要的相关文件；

d）评审周期：如果一个 ISMS 没有至少实施过一次覆盖认证范围的管理评审和内部审核，运营部不予安排对该 ISMS 实施认证；

e）认证范围：审核组应根据所有适用的认证要求，对包含在确定范围内的客户 ISMS 进行审核。审核组应确认客户在其 ISMS 范围内满足了 ISO/IEC 27001 中 4.3 的要求。如不能满足要求时，需及时向运营部反馈；

运营部和审核组应确保：客户的信息安全风险评估和风险处置准确地体现了认证范围所界定的活动并扩展到活动的边界。运营部和审核组应确认这在客户的 ISMS 范围和适用性声明中得到了体现。运营部应验证每个认证范围至少有一个适用性声明。

运营部和审核组应确保：与不完全包含在 ISMS 范围内的服务或活动的接口，已在寻求认证的 ISMS 中得到说明，并已包括在客户的信息安全风险评估中。与其他机构共享设施（如：IT 系统、数据库和通讯系统或外包一项业务职能），是这类情形的一个示例。

f）认证审核准则：客户 ISMS 接受审核的准则应是 ISMS 标准 ISO/IEC 27001。与所实施的业务相关的其他文件，也可以作为认证要求。

对于能源管理体系还应根据组织的规模，供能、用能过程的复杂性、能源管理体系成熟度及其他因素对认证全过程进行策划，制定审核方案。还应满足以下内容：

a）明确审核项目特定能力的需求，包括涉及技术领域的专业能力，专业能力包括与客户组织的能源使用和能源消耗、用能设施、设备、系统和过程的特点相关的能力；

b）基于客户能源管理体系文件界定的能源管理体系边界与范围的信息，确定 “能源管理体系边界”与“审核范围” ，以便审核策划；

c）包括多场所的抽样方案，抽样方法详见 CNAS-CC190:2021 附录 B。

5.1.5 运营部应在审核实施前与申请客户提前联系，确定审核目的、范围和准则，商定审核日期并负责组成审核组，选择审核组长。在商定审核日期时，应确保现场审核在生产期间进行：初次和再认证审核应安排在审核范围覆盖的所有产品/服务/活动的生产期进行；每

次监督审核应尽可能安排在认证范围内的所有产品/服务/活动的生产期进行，由于产品/服务/活动的季节性原因，在每次监督审核时难以覆盖所有产品/服务/活动的，应考虑在认证证书有效期内的监督审核必须覆盖管理体系认证范围内的所有产品/服务/活动。对于 ISMS 审核时间，运营部宜与拟审核的组织就选择一个能最有效地证实其整个 ISMS 范围的审核时间达成一致意见。适当时，可考虑季度、月份、日期和班次。在组建审核组时，应根据评定的专业代码以及体系类型与对审核组能力要求的程度及其他信息，使组成的审核组整体能力满足专业能力要求。

当客户管理体系包含具有相同或相近的活动的多场所或临时场所时，且这些场所都处于受审核方授权和控制下，可以进行抽样，但制定抽样方案且应符合《多现场审核管理规定》的要求，以确保对所抽样本进行的审核对管理体系包含的所有场所具有代表性及对该管理体系的正确审核，并记录抽样计划的合理性，但当多场所不是覆盖相同的活动时，抽样是不适宜的。如果不同场所的活动存在明显差异、或不同场所间存在可能对质量管理有显著影响的区域性因素，则不能采用抽样审核的方法，应当逐一到各现场进行审核。

当客户符合如下条件时，可适当考虑实施远程审核，并要求客户填写《实施远程审核认证客户信息调查表》：

a）ZXB 运营部经过评估，对于认证低风险审核项目，如生产/服务过程较为简单的；或

b）不适宜现场审核的情况，如出于安全原因、旅行限制等，典型示例如疫情、洪水、地震等；或

c）在某些多场所的情况，在限定的时间内审核组很难完成全部场所的现场审核；或

d）临时变更审核员或受审核方的日程安排发生了不可避免的变化，如审核员个人发生了突发事件、受审核方涉及管理体系的重要人员如最高管理者有重要业务需外出洽谈等；或

e）无论工作在何处进行审核，企业的记录、数据等均可在任何地点进行查看；或

f）无法完成现场审核计划的一项或多项活动，延长现场审核并非最佳、最经济的解决方案；或

g）ZXB 有审核员已熟悉受审核方管理体系及其实际运作情况；或

h）发现有遗漏审核过程或发现审核的完整性有缺失，审核组需返回现场进行补充审核，但在短期内返回现场不易实现的情况等。

运营部在策划依据多个管理体系标准进行认证时，应确保充分的现场审核，以提供对认证的信任。对 ISMS 文件与其他管理体系文件的整合，只要能够清楚地识别 ISMS 以及 ISMS 与其他管理体系的适当接口，ZXB 可以接受多个管理体系文件相结合的文件（例如，对信息安全、基于 ISO/IEC 20000-1 的服务、质量、环境和职业健康安全管理体系等）。只要能

够证实审核满足了 ISMS 认证的所有要求，ISMS 审核可以和其他管理体系审核相结合。在审核报告中，所有对 ISMS 重要的要素应清晰地体现并易于识别。审核的质量不应因结合审核而受到负面影响。

对于 SMS，应考虑客户可以将 SMS 文件和其他管理体系文件进行整合，例如：质量管理体系、信息安全管理体系。如果多个管理体系的文件是结合的，则应能清晰地识别出客户的 SMS。SMS 审核可以和其他管理体系审核相结合。结合审核或一体化审核应确保审核证据在审核范围内满足 ISO/IEC 20000-1 的要求。在审核报告中，应容易辨识出与 ISO/IEC 20000-1 相关的所有审核发现。ISO/IEC 20000-1 审核的完整性，不应因结合审核而受到负面影响。

在 ISO/IEC 27001 和 ISO/IEC 20000-1 的结合审核时，应审核 ISO/IEC 20000-1 中的信息安全管理过程，以确保：信息安全方针是与 SMS 和服务相关的；识别相关的信息安全风险并实施信息安全控制，以支持 SMS 和服务；审核员可以从信息安全管理体系（ISMS）中找到一些支持性的证据。

如果 ISMS 的范围是在 SMS 的范围之外，则 ISO/IEC 20000-1 中的信息安全管理过程是没有 ISMS 支持的，应作为一个独立的过程来审核。应审核信息安全方针、风险和控制，以确保它们与客户 SMS 范围内的服务相适宜。

对于信息安全管理体系和基于 ISO/IEC 20000-1 的服务管理体系，有关多场所的抽样比质量管理体系认证领域更加复杂。具体见《多现场审核管理规定》的相关要求。

对于能源管理体系审核组应具备实施能源管理体系认证审核的能力。审核组中应指定一名有能力的审核员担任审核组长,并至少有一名相应认证业务范围的能源管理体系专业审核员，在必要时还应配备相关行业的能源管理技术专家，以保证审核组的整体能力覆盖组织的能源管理体系范围所需的专业审核能力要求。

5.1.6 确定审核目的、范围和准则

5.1.6.1 审核目的由 ZXB 运营部确定。审核范围和准则，包括任何更改，应由运营部在与客户商讨后确定。

5.1.6.2 审核目的应说明审核要完成什么，并应包括下列内容：

a）确定客户管理体系或其中的一部分与确定管理体系标准及作为审核准则的其他文件的符合性；

b）确定管理体系确保客户满足适用的法律、法规及合同要求的能力，但管理体系认证审核不是合规性审核；

c）确定管理体系在确保客户可以合理预期实现其规定目标方面的有效性；

d）适用时，识别管理体系的潜在改进区域；

e）ISMS 审核目的还应包括确定管理体系有效性，以确保客户已根据风险评估实施了适用的控制并实现了所设立的信息安全目标；

f）SMS 审核目的应包括检查客户识别和控制了其与参与 SMS 活动的其他方在 SMS 边界内的接口。运营部还应确保客户知晓并管理了来自于这些接口的、对 SMS 和服务的风险。

5.1.6.3 审核范围应说明审核的内容和界限，例如拟审核的实际位置（或场所）、组织单元、活动及过程。当初次认证或再认证过程包含一次以上审核（例如覆盖不同位置或场所的审核）时，单次审核的范围可能并不覆盖整个认证范围，但整个审核所覆盖的范围应与认证证书中所界定的范围一致。

对于 SMS，审核组应根据适用的认证要求审核所确定范围内的客户 ISMS。运营部应确保根据业务特征、组织、组织的物理位置、资产和技术清晰地界定了客户 ISMS 的范围和边界，并考虑了 ISO/IEC 20000-3。运营部应证实客户考虑了其 SMS 范围内所规定的要求。

对于 OHSMS 应包括客户组织控制下或施加影响的、对客户组织的 OHSMS 绩效有影响的活动，产品和服务。客户组织的 OHSMS 应覆盖其控制的临时场所，例如建筑工地，不论其位于何处。

5.1.6.4 审核准则应被用作确定符合性的依据，并应包括：

a）所确定的管理体系标准和规范性文件的要求；

b）所确定的由客户制定的管理体系的过程和文件；

如果需要对 ISO/IEC 20000-1 的应用做出解释，这种解释应由 ZXB 技术部给出，并由 ZXB 正式发布。

5.1.7 运营部负责至少提前 5 天将《审核通知书》提交申请组织，并提请申请组织对所指派人员是否有异议。申请组织有权对审核组（包括技术专家）人选任命提出质询或异议，审核组的派遣应尽量满足其正当要求，使审核组为申请组织所接受。

运营部在为调查投诉、对客户的变更作出回应或对被暂停的客户进行追踪的审核进行策划并实施时。由于客户缺乏对审核组成员的任命表示反对的机会，运营部应在指派审核组时给予更多的关注。

5.1.8 审核组的能力要求

根据组织的规模、体系特点组成审核组，审核组应具备实现审核目的所需的能力以及符合公正性要求（包括审核组长以及必要的技术专家），并为其提供相应的工作文件。运

营部应明确地规定审核组的任务,并使客户知晓。通常情况下，审核组由审核组长和审核员组成。必要时，也可配备技术专家。审核组中的审核员承担审核任务和责任。如果仅有一名审核员，该审核员应有能力履行适用于该审核的审核组长职责和相应体系所规定的能力要求中全部准则。审核组应整体上具备运营部按照申请评审确定的审核能力。

5.1.8.1 决定审核组的规模和组成时，应考虑下列因素：

a）审核目的、范围、准则和预计的审核时间；

b）是否是结合、一体化或联合审核，若是结合审核或一体化审核，那么其审核组长宜至少对一个标准有深入的知识，并了解该审核所使用的其他标准；

c）实现审核目的所需的审核组整体能力；

d）认证要求（包括任何适用的法律、法规或合同要求）；

e）语言和文化；

f）在审核安排时应识别审核组成员是否与受审核方存在利益冲突，不应安排与受审核方存在利益冲突的审核人员，如审核组成员以前是否审核过该客户的管理体系。

5.1.8.2 所有审核组成员应具备以下能力：

a）熟悉一般的管理体系概念和相关的认证标准；

b）掌握和理解组织专业特点；

c）在审核期间，对可能遇到的风险进行识别和评价的能力。

5.1.8.3 审核组至少有一名具备以下能力的专业审核员：

a）掌握相关的行业实践、过程和技能知识；

b）掌握和理解相关法律、作业规程和标准知识。

5.1.8.4 当审核组不具备专业能力时，应配备技术专家并具有与组织相关的专业知识。审核组长和审核员所需的知识和技能可以通过技术专家和翻译人员补充。技术专家和翻译人员应在审核员的指导下工作。使用翻译人员时，翻译人员的选择要避免他们对审核产生不正当影响。技术专家的选择准则根据每次审核的审核组和审核范围的需要为基础确定。运营部应在实施审核前与客户就技术专家在审核活动中的作用达成一致。技术专家主要负责提供认证审核的技术支持，必须由审核员陪同，但不作为审核员实施审核，不计入审核时间，其在审核过程中的活动由审核组中的审核员承担责任。技术专家可以就审核准备、策划或审核向审核组提出建议。

5.1.8.5 如果审核组中包含实习审核员，则要指派一名审核员作为评价人员，实习审核员在评价人员的指导下参与审核，不计入审核时间，不单独出具记录等审核文件。评价人员应

有能力接管实习审核员的任务，并对实习审核员的活动和审核发现最终负责。

5.1.8.6 审核组长在与审核组商议后，应向每个审核组成员分配对特定过程、职能、场所、区域或活动实施审核的职责。所进行的分配应考虑到所需的能力、有效并高效地使用审核组以及审核员、实习审核员和技术专家的不同作用和职责。在审核进程中，为确保实现审核目的，可以改变工作分配。

5.1.8.7 质量管理体系认证审核的审核组应满足的 QMS 审核能力要求：

a）从事质量管理体系审核的人员应具有能力，能力包括 ISO/IEC17021-1:2015 所述的通用能力；以及质量管理术语、原则、实务和技术，质量管理体系标准和规范性文件，经营管理实务，客户的行业类别，客户的产品、过程和组织中所述的质量管理体系方面的知识；

b）所有实施 QMS 审核的人员的技术领域能力已经得到 ZXB 的评定；

c）审核组应由审核员（和技术专家，必要时）组成，具有承担审核的整体能力。该能力应包括 GB / T 27021.1-2017 所述的通用能力和 ISO/IEC 17021-3:2017 中 5.2 至 5.4 所述的基本概念和质量管理原则、组织环境、客户的产品、服务、过程和组织等 QMS 知识。

注：审核组的每位成员不必具有相同的能力，然而审核组的整体能力需要足以实现审核目标。

5.1.8.8 环境管理体系认证审核的审核组应满足针对特定因素的 EMS 审核能力要求：

a）每位 EMS 审核员应具备一定的、与 ZXB 所确定的技术领域相关的能力水平，包括 ISO/IEC17021-1:2015 中描述的通用能力；以及环境术语，环境计量，环境监视和测量技术，环境因素和环境影响，生命周期观点，环境绩效评价，合规义务，应急准备和响应，运行控制，与场所相关的因素，范围，交流的信息，组织所处的环境，风险和机遇条款中描述的 EMS 知识；

b）所有实施 EMS 审核的人员的技术领域能力已经得到 ZXB 的评定；

c）审核组的任命应使审核组成员的组成（需要时配备技术专家）能够整体满足实施审核的能力要求。ZXB 应确定与其运作的 EMS 技术领域相适应的每个因素相关的特定能力准则，并与 ISO/IEC 17021-2:2016 中向大气的排放（气体、气溶胶和颗粒物、运行控制、监视与测量），向土地的排放（液体或固体的排放、运行控制、监视和测量），向水体的排放（地表水和地下水、运行控制、监视和测量），原材料、能源和自然资源的使用（上游管理、下游管理、运行控制、监视和测量），能量释放（能量释放源、运行控制、监视和测量），废物（废物源、运行控制、监视和测量），空间利用（物理属性、运行控制、监

视和测量）等条款所规定的要求相一致。

注：并不需要审核组中的每位审核员都具备同样的能力，然而，审核组的整体能力应足以实现审核目的。

5.1.8.9 职业健康安全管理体系认证审核的审核组应满足的 OHSMS 审核能力要求：

a）从事职业健康安全管理体系审核的人员应具有能力，能力包括 ISO/IEC17021-1:2015 所述的通用能力；以及职业健康安全管理术语、原则、过程和概念，职业健康安全管理体系标准和规范性文件，业务管理实践，客户的业务领域，客户的产品、过程和组织中所述的职业健康安全管理体系方面的知识。每个职业健康安全管理体系审核员应了解职业健康安全管理体系内的协同作用，及过程间如何相互作用，以达到预期的结果，即提供安全健康的工作场所和预防伤害和健康损害；

b）所有实施 OHSMS 审核的人员的技术领域能力已经得到 ZXB 的评定；

c）审核组应由审核员（和技术专家，必要时）组成，具有承担审核的整体能力。该能力应包括 GB / T 27021.1-2017 所述的通用能力和 ISO/IEC TS 17021-10:2018 中 5.2 至 5.10 所述的职业健康安全术语、原则、过程和概念，组织环境，领导作用、工作人员协商和参与，法律要求和其他要求，职业健康安全风险和机遇及其他风险和机遇（风险和机遇、危险源识别、职业健康安全风险评价、职业健康安全机遇），应急准备和响应，绩效评价，消除危险源、降低职业健康安全风险，事件调查等 OHSMS 知识。

注：审核组应由审核员（和技术专家，必要时）组成，具有承担审核的整体能力。审核组中的每一个审核员不一定都需要具备相同的能力，然而审核组的整体能力需要足以实现审核目标。

5.1.8.10 信息安全管理体系认证审核的审核组应满足的 ISMS 审核能力要求：

a）从事信息安全理体系审核的人员应具有能力，能力包括 ISO/IEC17021-1:2015 所述的通用能力；以及信息安全管理术语、原则、实践和技术，信息安全管理体系标准和规范性文件，业务管理实务，客户的业务领域，客户的产品、过程和组织中所述的信息安全管理体系方面的知识；

b）具备①信息安全的知识；②与受审核的活动相关的技术知识；③管理体系的知识；④审核原则的知识；⑤ISMS 监视、测量、分析和评价的知识。除了②可以在作为审核组成员的审核员之间共享外，以上①-⑤适用于作为审核组成员的所有审核员。审核组应有能力将客户 ISMS 中信息安全事件的现象追溯到 ISMS 的相应要素；

c）所有实施 ISMS 审核的人员的技术领域能力已经得到 ZXB 的评定；

注：审核组中的每一个审核员不一定都需要具备相同的能力，然而审核组的整体能力需要足以实现审核目标。

另外，ISMS 审核组能力（除 4.1.8 上述要求外，还包括以下要求）

ISO/IEC 27006:2015 文件 7.1.2 的要求适用。对于监督和特殊审核活动，仅那些与所安排的监督活动和特殊审核活动相关的要求适用。当为特定认证审核选择审核组时，运营部应确保每次委派时审核组的能力是适宜的。审核组应：

a）对拟认证 ISMS 范围内的特定活动具备适当的技术知识，以及相关时，对这些活动的相关规程和其潜在信息安全风险具备适当的技术知识 （技术专家可以履行此项职责）；

b）理解客户，足以基于客户 ISMS 范围和组织环境对 ISMS（该体系管理着客户活动、产品和服务的信息安全）进行可靠的认证审核；

c）适当地理解适用于客户 ISMS 的法律法规要求。

注：适当地理解法规要求不意味着要有深厚的法律背景。

5.1.8.11 基于 ISO/IEC 20000-1 的服务管理体系认证审核的审核组应满足的 ISMS 审核能力要求：

a）从事基于 ISO/IEC 20000-1 的服务管理体系审核的人员应具有能力，能力包括 ISO/IEC17021-1:2015 所述的通用能力；以及信息技术服务管理术语、原则、实践和技术，基于 ISO/IEC 20000-1 的服务管理体系标准和规范性文件，业务管理实务，客户的业务领域，客户的产品、过程和组织中所述的基于 ISO/IEC 20000-1 的服务管理体系方面的知识；

b）所有实施 SMS 审核的人员的技术领域能力已经得到 ZXB 的评定；

注：审核组中的每一个审核员不一定都需要具备相同的能力，然而审核组的整体能力需要足以实现审核目标。

c）在以下每个方面，至少有一名审核组成员满足 ZXB 能力准则并在审核组内承担相应责任：

1）管理审核组；

2）适用于 SMS 的管理体系和过程；

3）SMS 过程及其实施的相关知识；

4）SMS 有效性评审和测量的相关知识；

5）SMS 标准，行业最佳实践和程序的相关知识；

6）事件处理方法的相关知识；

7）当前服务管理涉及的相关技术；

8）风险管理过程和方法的相关知识。

d）审核组应具备将组织的服务级别协议（SLA）的各个方面对应到 SMS 中相应条款进行评审的能力；

e）审核组应具有服务管理过程相适应的工作经验和能力。（这不意味着每一个审核员必须具备服务管理所有领域的经验和能力，但审核组整体上应具备受审核的 ISMS 范围内所覆盖的经验和能力

5.1.8.12 能源管理体系认证审核的审核组审核组应具备实施能源管理体系认证审核的能力。审核组中应指定一名有能力的审核员担任审核组长,并至少有一名相应认证业务范围的能源管理体系专业审核员，在必要时还应配备相关行业的能源管理技术专家，以保证审核组的整体能力覆盖组织的能源管理体系范围所需的专业审核能力要求：从事能源管理体系认证的审核员除应具备能源管理体系通用知识要求外，还应具备能源管理体系特定技术领域的知识和技能，包括：

a）特定技术领域业务活动、产品/服务实现过程、工艺流程，特别是能源加工、转换和使用的流程；

b）特定技术领域的主要能源使用和能源消耗、能源绩效参数、专用的用能设施、设备和系统及运行特性等；

c）特定技术领域与能源有关的法律、法规、标准及其他要求；

d）特定技术领域有关的节能技术和能效优化技术等。

5.1.8.13 ZXB 运营部与客户应在实施审核前就审核活动中观察员的到场及理由达成一致。审核组应确保观察员不对审核过程或审核结果造成不当影响或干预。观察员可以是客户的成员、咨询人员、实施见证的认可机构人员、监管人员或其他有合理理由的人员。

5.1.8.14 为了方便审核的实施，同一审核小组的审核员至少应由一名客户安排的向导陪同，除非审核组长与客户另行达成一致。审核组应确保向导不影响或不干预审核过程或审核结果。向导的职责包括（不限于）：为面谈建立联系或安排时间；安排对现场或客户的特定部分的访问；确保审核组成员知道并遵守关于现场安全和安保程序的规则；代表客户观察审核；应审核员请求提供澄清或信息。适宜时，受审核方也可以担任向导。

5.2 接受审核任务

5.2.1 审核任务由 ZXB 运营部统一安排。

审核组长只能接受 ZXB 运营部安排的审核任务。审核任务以《审核计划》（指“现场审核计划”首页）的形式下达。

5.2.1.1 《审核计划》总则

运营部应按本文件的要求，确保为审核方案中确定的每次审核编制《审核计划》，以便为有关各方就审核活动的日程安排和实施达成一致提供依据。但是，运营部不会在建立审核方案时，就为每次审核都编制审核计划。

对于 SMS 审核计划，运营部和审核组通过识别以下方面的差异，在初始合同评审和后续审核活动时应确定适当的抽样水平：

a）地点，例如：场所规模，或在 SMS 内但不在认证范围内的临时场所的使用；

b）服务；

c）顾客；

d）参与服务提供的其他方（例如：内部团体、供方、作为供方的顾客）；

e）语言；

f）所有班次之间工作方式的一致性。如果每个班次的运行方式相同时，审核有大量人员倒班的客户所需的时间可以少些。这要有记录审查，以证实所有班次之间工作方式的一致性。如果各班次之间是一致的，所有班次可被视为是一组活动且一个班次可作为审核样本。

g）SMS 的局部变化；

h）法律法规要求。

应从客户 SMS 范围中选择有代表性的样本。该选择应基于 HXQC 的决定，并体现了 a）中所述的因素和随机因素。审核计划的策划应考虑 a）和 b）中的要求。计划应在认证审核间的 3 年周期内覆盖 SMS 全部范围内有代表性的样本。

5.2.1.2 编制《审核计划》

5.2.1.2.1 运营部编制的《审核计划》应与“审核目的和范围”相适应。《审核计划》至少应包括或引用：

a) 受审核方名称、地址、联系人和电话/传真，以及审核时间；

b）审核类型（初审/再认证/监督/扩大等）；

c）审核依据；

d）审核目的；

e）审核范围，包括识别拟审核的客户和职能单元或过程；

f）专业代码；

g）人日及体系覆盖人数；

h）其他说明；

i）审核组成员（分工；姓名；注册资格和证书号；专业代码；技术专家应标明工作单位及专业技术职称；兼职审核员如果在职应注明其服务的单位；电话等），特殊情况下，还包括与审核组同行的人员（例如观察员或翻译）的角色和职责；

j）文件评审负责人及更改确认；

k）受审核方确认；

l）审核安排人员（签章）等等;

m）考虑所确定的信息安全控制措施（仅适用于 ISMS）。

如适宜，审核计划应识别在审核中使用的网络支持的审核技术（远程审核技术）。（注：网络支持的审核技术可包括：例如，电话会议、网络会议、基于网络的交互式通信和远程电子访问管理体系文件和（或）管理体系过程。对这些技术的关注，将提高审核的有效性和效率，并支持审核过程的完整性。）

5.2.1.2.2 对于 SMS 审核计划，运营部和审核组通过识别以下方面的差异，在初始合同评审和后续审核活动时应确定适当的抽样水平：

a）地点，例如：场所规模，或在 SMS 内但不在认证范围内的临时场所的使用；

b）服务；

c）顾客；

d）参与服务提供的其他方（例如：内部团体、供方、作为供方的顾客）；

e）语言；

f）所有班次之间工作方式的一致性。如果每个班次的运行方式相同时，审核有大量人员倒班的客户所需的时间可以少些。这要有记录审查，以证实所有班次之间工作方式的一致性。如果各班次之间是一致的，所有班次可被视为是一组活动且一个班次可作为审核样本。

g）SMS 的局部变化；

h）法律法规要求。

应从客户 SMS 范围中选择有代表性的样本。该选择应基于 ZXB 的决定，并体现了 a）中所述的因素和随机因素。审核计划的策划应考虑 a）和 b）中的要求。计划应在认证审核间的 3 年周期内覆盖 SMS 全部范围内有代表性的样本。

5.2.2 《审核计划》是编制“现场审核计划”的主要依据之一，审核组长接到《审核计划》后应确认其内容是否明确/合理，若无疑义/问题，由审核组长确认《审核计划》即可，无

需运营部确认；若有对疑义/问题应反馈至运营部进行确认，未经运营部同意，审核组长不得擅自修改《审核计划》。

5.2.3 审核组长接到审核任务后，应熟悉或索取下述文件：

1）受审核方所属专业的审核作业指导书（必要时）；

2）审核项目所必须的全套文件包，并检查确认；

3）对于再认证的获证客户，审核组长应了解获证客户上一周期管理体系运行情况，包括调阅以前的“审核报告”等，并填写《对再认证组织上一周期的绩效评价》表。

5.3 文件评审

5.3.1 文件评审的时机：

在下述情况下，应在现场审核前进行文件评审：

1）初次审核、再认证审核、认证转换审核；

2）监督审核遇到获证客户机构重大调整、管理体系文件较大修改或换版等管理体系发生重大变更影响认证基础的；

3）获证客户申请扩大或变更认证范围的；

4）审核策划人员识别确认的需文件审核的其他情况。

5.3.2 文件评审一般应由审核组长进行，当审核组长没有专业时，应有专业审核员或技术专家参加并进行复核确认。

5.3.3 文件评审的实施：

5.3.3.1 初次认证的文件评审结合一阶段审核进行，由审核组长实施并填写《文件评审报告》。

5.3.3.2 再认证审核、扩大或变更认证范围以及监督审核文件发生换版的文件评审由审核组长在现场审核之前进行，审核任务安排人员在审核通知中注明“再认证”、“扩大”及“文件换版”等提示字样，由审核组长填写《文件评审报告》。

5.3.3.3 当文件评审结论为不符合标准要求，需要修改再次提交文件评审时，或涉及现场审核日期的变更时，审核组长应和运营部审核任务安排人员联系调整现场审核日期。

5.3.3.4 文件评审应对下述方面进行审核，并形成结论：

（1）客户提交的认证申请文件资料是否满足要求，是否有效；

（2）客户申请认证范围的表述是否明确、具体，是否在客户法律文件许可范围内；

（3）客户的管理体系是否覆盖申请的认证范围；

（4）客户的管理体系文件是否符合法律法规和标准要求；

（5）客户的管理体系运行时间是否满足 3 个月的要求（建筑行业/能源管理体系 6 个月）；

（6）各认证领域文件评审的具体内容见《文件评审报告》；

（7）对文件评审时的不明情况，文件评审人员应与受审核客户进行沟通，或在现场审核时落实；

（8）文件评审应形成《文件评审报告》，并提交给受审核客户；

（9）对文件评审中发现的问题应提出整改要求，并对整改结果进行验证关闭；关闭证据应充分，并归入审核案卷。

5.4 现场审核准备

5.4.1 编制“现场审核计划”

5.4.1.1“现场审核计划”编制前，审核组长应和受审核方进行充分沟通，确认审核范围，了解受审核方的工作时间、工作场所的分布情况、多现场情况，以及是否处于生产状态、是否有远程审核活动、是否按规定至少进行了一次内部审核和管理评审等有关信息；对建筑业等具有临时场所的组织，还应索取《在建和竣工项目清单》；对多场所组织，还应索取《多场所清单》。

5.4.1.2“现场审核计划”应按过程方法编制，包括预计的实施现场审核活动的审核组成员及相应的时间安排，对多场所和（或）含有临时场所的受审核方，应在“现场审核计划”中体现抽样；适用时还应包括远程审核活动的日期和场所；受审核方无任何生产现场或未生产时，不能进场审核。当没有生产现场，或未生产时，或未按规定进行内部审核和管理评审时，审核组长应及时向运营部报告调整审核安排。

5.4.1.3“现场审核计划”应明确审核的关键区域及若需配置的特殊资源；当两名及以上级别审核员安排在同一小组内审核时，在“现场审核计划”中应分别明确各自审核内容，并分别做好审核记录。如果受审核方采用轮班作业，应在编制审核计划时考虑在轮班工作中发生的活动。能源管理体系现场审核计划还应考虑以下内容：重点审核主要用能设施、设备、系统和过程；应通过关注相关数据了解能源使用和能源消耗情况；评价客户对主要能源使用的识别和管理；安排能源绩效核查，评价能源绩效改进活动的策划、实施及效果。

5.4.1.4 在编制监督审核的“现场审核计划”时，必需关注受审核方的内部审核、管理评审、持续改进、投诉处理、认证证书和标志的使用、对上次不符合项的验证、持续运作控制、变更情况、目标和各管理体系预期结果方面的实现情况、基础设施以及监视和测量设备的控制等内容。

5.4.1.5 一般情况下，“现场审核计划”应至少在现场审核前 5 天内发送给受审核方。受审核方的任何异议由审核组长协商解决，如审核组长无法解决应和运营部审核任务安排人员联系。

5.4.1.6 审核组长在审核现场时，可以在不打破原“现场审核计划”的总体安排的前提下对“现场审核计划”进行调整，但应在实施前征得受审核方同意（重大调整应获得主管部门同意，并经再确认），并在现场审核沟通记录表中予以记录。同时，审核组长应将调整后的“现场审核计划”分别提供给审核组成员和受审核方，并纳入审核档案。

5.4.1.7 当审核日期和审核组成员需要发生变化时，审核组长应与运营部审核任务安排人员沟通，获得同意后才能实施调整。除不可预见的特殊情况外，审核过程中不得更换审核计划确定的审核员（技术专家和实习审核员除外）。

5.4.1.8“现场审核计划”编制时间应在《审核计划》安排的时间之后（或当天），在现场审核前 5 天内（或当天）的时间里。

5.4.2 现场审核前的准备

5.4.2.1 现场审核前，审核组长应召集准备会议，完成如下工作（当审核组只有 1 人时可不进行此项活动）：

a）由审核组长做受审核方情况介绍，并进一步明确审核产品/服务的范围、审核分工、审核要求和审核注意事项等；

b）由专业审核员或技术专家对审核组内其他成员进行专业培训。专业培训应突出产品的主要工艺流程/服务过程（包括关键过程及需确认的过程/重要环境因素/不可接受风险/关键控制点及其控制要点），检验/检测依据和要求，与审核范围有关的法律、法规及标准等内容，且具有针对性。审核组应做好相关的《审前沟通与培训记录》。

5.4.2.2 召集审核组成员签署《公正性与保密声明》。

5.4.2.3 获得受审核方的管理体系文件，按照“现场审核计划”，安排审核组成员编制现场审核检查表。

5.5 审核的实施

5.5.1 审核总要求

5.5.1.1 现场审核应与审核目的、范围、准则保持一致。

5.5.1.2 对初审和再认证，现场审核应覆盖认证范围，包括：产品/服务/活动范围、场所范围（对多场所审核，按抽样规则进行抽样）、以及认证标准全部要求。对监督审核，现场

审核应对管理体系范围内有代表性的区域和职能进行审核；原则上应覆盖认证范围内的产品/服务/活动范围和场所范围（对多场所审核，按抽样规则进行抽样）；对季节性客户，应在生产季节进行审核；对建筑业等周期性客户，应在具有典型活动期间进行审核；当监督审核时，难以覆盖认证范围内的全部产品/服务/活动/场所时，应在一个认证周期内的各次监督审核活动完整覆盖认证范围内的全部产品/服务/活动/场所。

5.5.1.3 现场审核时，应现场观察审核范围内的产品/服务/活动的开展情况。现场审核应思路清晰，证据充分，抽样应具有代表性；收集的信息应全面反映客户管理体系运行状况，包括正面和负面的信息；对认证范围内的每一或每种产品/服务/活动，应有足够的证据链支持审核结论和认证决定，应能为管理体系满足法律法规和标准要求提供充分信心。

5.5.1.4 现场审核应重点突出，把握关键，关注有效性，具体要求详见《管理体系认证通用审核指南》。

5.5.1.5 一阶段应编制《第一阶段审核报告》、二阶段应编制“审核报告”，一、二阶段的审核记录应分开整理。

5.5.1.6 多现场（包括多场所、临时场所等情况）抽样应符合抽样规则要求。

5.5.1.7 结合审核应符合“结合审核规则”要求。

5.5.1.8 审核记录应符合《管理体系认证通用审核指南》，应特别关注硬性证据。

5.5.1.9 现场审核时及审核报告中，审核组可为客户识别改进机会，但不应提出具体改进的建议。

5.5.2 初次认证审核

管理体系初次认证审核分两个阶段进行，第一阶段和第二阶段。

5.5.2.1 第一阶段审核

（1）第一阶段审核的目的是调查申请受审核方是否已具备实施认证审核的条件，并为第二阶段审核提供必要的信息。

（2）第一阶段重点审核内容

①QMS、EMS 和 OHSMS 第一阶段重点审核内容：

a）核实申请受审核方的法律地位与资质，了解受审核方对适用法律法规的识别情况，从事的活动是否符合相关法律法规的规定；

b）实施文件评审（见 4.3），对管理体系文件化信息不符合现场实际（特别是体系成文信息中描述的产品和服务、部门设置和职责与权限、生产或服务过程等）、相关体系运行尚未超过 3 个月或者无法证明超过 3 个月的（建筑行业 6 个月），以及其他不具备二阶

段审核条件的，不应实施二阶段审核；

c）评价受审核方的运作场所和现场的具体情况，并与受审核方的人员进行讨论，以确定第二阶段审核的准备情况；

d）审查受审核方理解和实施标准要求的情况，特别是对管理体系的关键绩效或重要的因素、过程、目标和运作的识别情况；

e）收集关于受审核方的管理体系范围的必要信息，包括客户的场所、体系覆盖范围内有效人数、使用的过程和设备、所建立的控制的水平（特别是客户为多场所时）及适用的法律法规标准要求和遵守情况；

f）审查第二阶段审核所需资源的配置情况，并与受审核方商定第二阶段审核的细节；

g）结合管理体系标准或其他规范性文件充分了解受审核方的管理体系和现场运作，以便为策划第二阶段审核提供关注点；结合管理体系覆盖产品和服务的特点识别对管理体系方针和目标的实现具有重要影响的关键点，并结合其他因素，科学确定重要审核点；

h）评价受审核方是否策划和实施了内部审核与管理评审，以及管理体系的实施程度能否证明受审核方已为第二阶段审核做好准备。

②对于 ISMS 体系的第一阶段审核中，审核组应获取有关 ISMS 设计的文件，其中包括 ISO/IEC 27001 所要求的文件。除了上述①相关内容外，还应关注但不限于以下方面内容：

a)充分了解在组织环境下所进行的 ISMS 设计、风险评估和处置(包括所确定的控制)、信息安全方针和目标，以及特别是客户的审核准备情况。在此基础上，才能进行第二阶段的策划；

b）ISMS 初次认证审核的第一阶段审核宜包括在客户现场实施的审核活动，现场审核时间不宜少于 1 个审核人日。当客户由于信息安全的原因在申请评审阶段不能提供给运营部足够的信息时，运营部应通过第一阶段审核在客户的现场补充对上述信息的确认，并完成申请评审任务。这种情况下，运营部应增加第一阶段现场审核时间。

③对于 SMS 体系的第一阶段审核中，审核组应获得客户有关 SMS 设计的文件。该文件应包括 ISO/IEC 20000-1 的 4.3.1 中所要求的文件。 除了上述①相关内容外，还应关注但不限于以下方面内容：

a）结合客户的 SMS 方针和目标，尤其是其所声称的审核准备情况，了解客户的 ISMS，为二阶段审核提供关注点；

b)一阶段审核包括但不限于文件评审。当客户由于信息安全的原因在申请评审阶段不能提供给运营部足够的信息时，运营部应通过第一阶段审核在客户的现场补充对上述信息

的确认，并完成申请评审。这种情况下，运营部应增加第一阶段现场审核时间。

④对于 EnMS 第一阶段审核还应包括：

a) 确认拟认证能源管理体系的范围和边界；

b) 对已识别的范围和边界，评审组织设施、设备、系统和过程的图表或文字说明；

c) 确认能源管理体系有效人员的数量、能源种类、主要能源使用和年度综合能耗，以确定审核时间；

d) 评审能源策划过程形成的文件化结果；

e) 评审经识别的能源绩效改进机会的清单，以及相关的目标、指标以及实施方案。

f)对已识别的范围和边界，评审组织架构及人员的图标或文字说明，并进一步确认组织的技术领域。

g)审查及确认：

①客户能源管理体系文件；

②能源使用、主要能源使用、能源基准、能源绩效参数及其与体系各要素的关系；

③能源方针与目标指标、能源绩效参数、能源监视、测量和分析机制的建立与运行；

④最高管理者对于能源管理在组织经营活动中的地位、策略和行动，对管理者代表和能源管理团队的任命和批准；

⑤主要适用的能源法律、法规和产业政策的符合性；

⑥客户能源管理体系的建立及能源管理方针的一致性；

⑦客户的内部审核和管理评审的策划和实施情况。

（3）第一阶段审核的策划

①为确保满足第一阶段审核的目标要求，针对管理体系的初次认证审核，符合下列情况应现场实施第一阶段审核：

a)复杂的管理体系，如：

● 受审核方的规模、结构及其职能复杂，如：集团公司（具有不同等级体系及其层面的活动）。

● 受审核方的运作场所及现场复杂多样，如具有多个临时场所和/或多场所的受审核方。

● 管理体系覆盖了相当数量的产品/服务范围，或具有高度复杂的活动和过程。

● 多个管理体系的结合审核。

b)新扩展的技术或认证领域。

c)对组织产品/服务、过程或活动中的相关技术或问题缺乏足够的了解或经验不足。

d)高风险项目，如：

● 法规、环境或社会关注程度较高的特殊专业技术领域，如：食品、、核工业、制药、汽车、船舶、建设、航空航天、运输、医疗等。

● 基于质量、环境、职业健康安全管理体系等相关因素性质及其具有高风险的特性。

e) ISMS/SMS/EnMS 一阶段审核必须在受审核方的现场进行。

② 在下列情况，第一阶段审核可以不在受审核方现场进行，但应记录未在现场进行的原因：

a）受审核方已获 ZXB 颁发的其他有效认证证书，审核组已对受审核方管理体系有充分了解；

b）ZXB 运营部有充足的理由证明受审核方的生产经营或服务的技术特征明显、过程简单，通过对其提交文件和资料的审查可以达到第一阶段审核的目的和要求；

c）申请组织获得了其他经认可机构认可的认证机构颁发的有效的管理体系认证证书，通过对其文件和资料的审查可以达到第一阶段审核的目的和要求；

d) 受审核方规模较小，如几十人或十几人；现场范围较小，如一个作坊或车间，且所生产的产品质量风险属于低风险；

e）审核组长对受审核方情况非常熟悉。如审核组长曾参与过受审核方其他领域的审核，对受审核方现场极其质量风险熟悉；

f) 审核组有充分的资源保证。如有充分的人力资源或时间，足以保证在二阶段现场审核是能够满足审核准则的全部要求。

除以上情况之外，第一阶段审核应在受审核方的生产经营或服务现场进行。

③ ZXB 运营部根据上述条件进行一阶段审核策划，当策划的结果为不到现场审核时，应填写《一阶段审核不到现场策划书》。如果确定不到现场，运营部审核任务安排人员应下达《审核计划》，明确审核类型和内容，审核组长应完成在现场审核要达到的所有目标。

（4）一阶段审核问题提出

一阶段审核发现的问题不开具《不符合报告》，对于不符合审核准则等方面以问题清单的方式提出，填写《第一阶段审核问题汇总表》；对于一阶段审核发现问题的整改，在验证方式栏，若选择“书面”验证，需要在二阶段审核之前提交书面整改材料，审核组长验证合格后方可进入二阶段审核；若选择“现场”验证，需要在二阶段审核之前提交书面整改计划，经审核组长确认后，在二阶段审核现场验证整改结果。

当出现下列情况时，必须选择“书面”验证：

a）法律、法规规定的营业执照，法定的资质、许可、评价、验收报告不全或失效；

b）出现了重大产品质量、环境、职业健康安全事故、信息安全事件、能源相关事故仍在处理期的；

c）质量、环境、职业健康安全法律法规规定的监测报告不全、失效或不合格的；

d）内部审核、管理评审未进行的；

e）审核组认为其他必需整改的。

除上述之外的问题，由审核组长决定选择“书面”或“现场”验证。

审核组长负责对提交的资料进行验证，验证结果填写《第一阶段审核问题汇总表》的验证栏内。

（5）一阶段审核结论

第一阶段审核后应编制《第一阶段审核报告》，审核报告应对是否达到第一阶段目的及第二阶段是否准备就绪即具备第二阶段审核条件作出结论，并应告知受审核方第一阶段审核的结果可能导致推迟或取消第二阶段审核。对审核中发现的问题，应开具问题清单，通知受审核方进行整改，整改结果应有证据并经验证。对在第二阶段审核中可能被判定为不符合项的重要关键点，要及时提醒受审核方特别关注。在决定进行第二阶段之前，运营部应审查第一阶段的审核报告，以决定是否实施二阶段审核并为第二阶段选择具有所需必要能力的审核组成员。审核组和运营部还应让客户知晓第二阶段可以要求对更进一步的信息或文件和记录做详细检查。

（6）一、二阶段的时间间隔

在确定第一阶段审核和第二阶段审核的间隔时间时，应考虑受审核方解决第一阶段审核中发现的问题整改所需的时间。也可能需要调整第二阶段审核的安排。如果发生任何将影响管理体系的重要变更，运营部应考虑是否有必要重复整个或部分第一阶段审核。一般情况下，当第一阶段审核中发现的问题得到整改后，便可进行第二阶段审核的安排，通常第一阶段审核和第二阶段审核的间隔时间不超过 3 个月，若特殊情况超过 3 个月，需由受审核方提出延期申请，审核组长确认，报运营部批准，但第一阶段审核时间与第二阶段审核时间间隔最长不得超过 6 个月。如果超过 6 个月，应重新安排第一阶段审核。对于SMS，第一阶段与第二阶段现场审核间隔应不少于 5 个工作日且不多于 60 个工作日。

5.5.2.2 第二阶段审核

第二阶段审核的目的是评价受审核方管理体系的实施情况，包括有效性和符合性。而

ISMS 除了评价 ISMS 的有效实施之外，第二阶段的目的还有：确认客户遵守自身的方针、策略和规程。第二阶段审核应在受审核方的现场进行：

（1）实施前提：对于第一阶段审核中发现的问题，审核组应在进入第二阶段审核前解决并进行验证确认，验证确认的方式可根据问题的性质确定。存在不符合法规要求、监测不达标的情况时,不能进行第二阶段审核。审核组长确定可以实施第二阶段现场审核时，提请运营部安排《审核计划》。

（2）审核目的：评价受审核方管理体系的实施情况（包括有效性），是否满足认证准则要求，确定是否推荐认证注册。

（3）审核的重点：第二阶段审核应依据认证准则的要求并基于第一阶段审核的结果，对受审核方的管理体系进行全面的符合性、适宜性和有效性评价，从而决定是否推荐认证注册。

（4）审核至少覆盖以下方面：

a）与适用的管理体系标准或其他规范性文件的所有要求的符合情况及证据，特别是在第一阶段审核中识别的重要审核点的过程控制的有效性；

b） 根据关键绩效目标和指标（与适用的管理体系标准或其他规范性文件的期望一致），对绩效进行监视、测量、报告和评审的情况；

c）受审核方的管理体系的能力以及在符合适用法律法规要求和合同要求方面的绩效；

d）受审核方过程和活动的运作控制以及应急预案的可操作性；

e）内部审核和管理评审；

f）针对客户方针的管理职责；为实现方针而在相关职能、层次和过程上建立的目标是否具体适用、可测量并得到沟通、监视；

g）受审核方实际工作记录的真实性。对于审核发现的真实性存疑的证据应予以记录并在做出审核结论及认证决定时予以考虑。

（5）对 ISMS 二阶段审核除了应满足（4）的要求，还应重点关注但不限于以下方面：

a）最高管理者的领导力和对信息安全方针与信息安全目标的承诺；

b）ISO/IEC 27001 中所列的文件要求；

c）评估与信息安全有关的风险，以及评估可产生一致的、有效的、在重复评估时可比较的结果；

d）基于风险评估和风险处置过程，确定控制目标和控制；

e）信息安全绩效和 ISMS 有效性，以及根据信息安全目标对其进行评审；

f）所确定的控制、适用性声明、风险评估与风险处置过程的结果、信息安全方针与目标，它们相互之间的一致性；

g）控制的实施（见 ISO/IEC 27006:2015 附录 D），考虑了外部环境、内部环境与相关的风险，以及组织对信息安全过程和控制的监视、测量与分析，以确定控制是否得以实施、有效并达到其所规定的目标；

h)方案、过程、规程、记录、内部审核和对 ISMS 有效性的评审，以确保其可被追溯至管理决定和信息安全方针与目标。

（6）对 SMS 二阶段审核除了应满足（4）的要求，还应重点关注但不限于以下方面：

a）ISO/IEC 20000-1 的 4.3.1 中的文件要求；

b）对实施、监视、测量和评审服务管理目标计划和过程的有效控制；

c）SMS 内部审核和管理评审；

d）方针的管理责任；

e）客户的服务管理过程之间的相互作用，证实其对信息技术服务管理过程的分析和组织运作实施了适当的控制措施，应包括：

①服务交付过程(服务级别管理，服务报告，服务连续性和可用性管理，信息技术服务的预算和核算，能力管理，信息安全管理)；

②关系过程(业务关系管理，供方管理)；

③处理过程(事件管理，问题管理)；

④控制过程(配置管理，变更管理)；

⑤发布过程(发布管理)。

f）应获取客户识别了参与服务提供的其他方和客户如何按照 ISO/IEC 20000-1 对其他方进行管理的证据。

（7）对 EnMS 管理体系第二阶段审核除了应满足（4）的要求，还应重点关注但不限于以下方面：

a)对能源使用的识别和随后对主要能源使用的判定；

b）经评审以后而制定的绩效参数、能源目标、指标、能源管理实施方案，对照能源目标、指标、绩效参数而实施的测量、分析、报告和评价情况，以及能源绩效的改进情况包括可比综合能耗指标及变化的情况；

c）关注不同行业的能源认证要求；

d）不符合的识别与评价，纠正措施和预防措施的完成情况；

e）对能源绩效参数的确定和调整情况；能源绩效出现重大偏差时，是否进行了原因分析并采取了相应的改进措施，改进效果的验证;

f)能源评审的时间间隔的合理性及能源评审的充分性和有效性；能源管理体系的自我改进及完善机制的持续性和有效性。

(8) 对第一阶段已审核过的要素，注意识别两个阶段审核侧重点的不同和衔接；有些在第一阶段已取证充分的内容可在第二阶段审核时简化或不再重复取证，但应注意最终对受审核方的管理体系有效性、适宜性和充分性进行评价和做出审核结论时，应将第一阶段审核的信息输入。

5.5.3 监督审核

5.5.3.1 审核的目的是评价获证客户的管理体系是否持续保持满足认证准则要求。

5.5.3.2 每次监督现场审核必审下列内容：

a）获证客户的变更（包括体系覆盖的活动及影响体系的重要变更及运行体系的资源等）、体系文件变化及体系的更新等任何变更和保持；

b）上次不符合项的跟踪验证；

c）顾客及相关方投诉、质量/环境/职业健康安全/信息安全/能源相关等事故及处理；针对体系运行中发现的问题或投诉，及时制定并实施了有效的改进措施；

d）认证证书及标志的使用及任何其他对认证资格的引用，是否符合《中华人民共和国认证认可条例》（现行有效版本）及其他相关规定；

e）内部审核、管理评审；

f）预防和纠正措施及其他为持续改进而策划的活动的进展；

g）管理体系在实现获证客户目标和各管理体系的预期结果方面的有效性；目标及绩效是否达到管理体系确定值。如果没有达到，获证客户是否运行内审机制识别了原因、是否运行管理评审机制确定并实施了改进措施。

h）持续的运作控制，包括遵守法律法规和其他要求、质量的关键/特殊过程控制、环境因素识别与控制、危险源辨识与风险控制措施评价，以及临时场所管理体系的控制、多个场所的拟抽取样本的合理性等等。

i）服务目录的变化情况；适当时，其它选定的范围。（适用 SMS）

ISMS 监督审核除上述内容外，还应重点关注但不限于以下内容：

a）体系变化和保持情况；

b）服务目录的变化情况；

c）适当时，其它选定的范围。

SMS 监督审核除上述内容外，还应重点关注但不限于以下内容：

a）体系变化和保持情况；

b）服务目录的变化情况；

c）适当时，其它选定的范围。

另外，ISMS 监督的目的是验证已被认证的 ISMS 得到持续实施、考虑获证客户运作变化所引起的管理体系变化的影响并确认与认证要求的持续符合。监督审核方案应至少包括：

a）管理体系的保持要素，如信息安全风险评估与控制的维护、ISMS 内部审核、管理评审和纠正措施；

b）根据 ISMS 标准 ISO/IEC 27001 和认证所需的其他文件的要求，与来自外部各方沟通；

c）文件化管理体系的变更；

d）发生变更的区域；

e）所选择的 ISO/IEC 27001 的要求；

f）适宜时，其他所选择的区域。

而 ISMS 每一次监督应至少审查以下方面：

a）ISMS 在实现获证客户信息安全方针的目标方面的有效性；

b）对与相关信息安全法律法规的符合性进行定期评价与评审的规程的运行情况；

c）所确定的控制的变更，及其引起的 SoA 的变更；

d）控制的实施和有效性（根据审核方案来审查）。

能源管理体系监督审核应收集必要的证据以确定能源绩效的持续改进已得到证实， 且至少应包括对以下方面的审查：

a) 内部审核和管理评审；

b) 对上次审核中确定的不符合采取的措施的实施情况及有效性；

c) 投诉的处理；

d) 获证客户的主要能源使用的运行情况、能源计量及统计、能源绩效考评和能源管理方案的实施情况；

e) 能源管理的目标、指标的实现和调整情况；

f) 按照能源方针，持续改善整体能源绩效所采取措施的进展情况及所取得的能源绩效改进情况，包括对能源绩效的量化评估；

g）能源法律法规和行业要求变化及对能源管理体系的影响，合规性评价情况，有无受到处罚和产生负面影响等；

h）能源基准的变化情况；

i）能源管理相关信息对外交流情况；

j）能源审计、节能技术改造、淘汰落后设备和工艺等情况；

k）能源管理岗位和能源管理负责人变化情况；

l）管理体系认证范围变更情况， 包括获证客户能源绩效情况 （即本次审核时间期限内的综合能耗及能源管理体系边界） ；

m）其他变更；

n）标志的使用和（或）任何其他对认证资格的引用。

运营部应能够针对与信息安全问题相关的风险及其对客户的影响来调整监督方案，并说明监督方案的合理性。监督审核可以与其他管理体系的审核相结合。报告应清晰地指出与每个管理体系相关的方面。在监督审核过程中，审核组应检查获证客户提交的申诉和投诉记录，并且在发现任何不符合或不满足认证要求时，还应检查获证客户是否对其自身的ISMS 和规程进行了调查并采取了适当的纠正措施。特别是，监督报告应包括有关消除以往出现的不符合、SoA 版本和从上次审核之后发生的重大变更的信息。监督审核报告应至少完全覆盖上述 ISMS 相关要求。

5.5.3.3 监督审核的过程要求

a）每次监督审核的必审过程，见《审核信息传递表》；

b）必审过程外的其他过程，由审核组长根据获证客户管理体系运行和以往审核结果等情况策划。

5.5.3.4 监督审核的覆盖范围要求

a）部门/场所范围：每次监督必审管理层、必审过程的主控部门、生产/服务提供控制部门及场所等，认证周期内监督应覆盖全部部门/场所；

b）产品范围：每次监督原则上应覆盖认证范围内的全部产品/服务/活动，认证周期内的历次监督应覆盖全部产品/服务/活动的全过程；当监督审核难以覆盖认证范围内的全部产品/服务/活动时，应在一个认证周期内的各次监督审核活动完整覆盖认证范围内的全部产品/服务/活动。

5.5.3.5 监督审核时机

ZXB 为确保达到对持有其颁发的管理体系认证证书的客户（以下称获证客户）进行有效

跟踪，监督获证客户通过认证的管理体系持续符合要求的目的。根据获证客户及体系覆盖的产品或服务的风险程度或其他特性，合理确定对获证客户的监督审核的频次。为了考虑诸如市场、季节或有限时段的管理体系认证（例如临时施工场所）等因素，可能有必要调整监督审核的频次。对于能源管理体系 ZXB 根据获证客户的供能、用能复杂性、能源管理体系成熟度及稳定性等确定监督审核频次。对于能源管理体系 ZXB 根据获证客户的供能、用能复杂性、能源管理体系成熟度及稳定性等确定监督审核频次。

监督审核应至少每个日历年（应进行再认证的年份除外）进行一次。初次认证后的第一次监督审核应在认证决定日期起 12 个月内进行。此后，监督审核应至少每个日历年（应进行再认证的年份除外）进行一次，且两次监督审核的时间间隔不得超过 15 个月。监督审核时间亦在获证客户的生产季节进行，建筑企业应在其具有代表性的在建项目施工期间进行审核。需要时，监督审核可以在一年中进行一次以上的监督审核，以覆盖监督审核的所有要求。当获证客户管理体系发生重大变更、或发生重大问题、重大质量/环境/职业健康安全/信息技术服务质量/能源绩效/信息安全事件、重大客户投诉等情况时，应增加监督频次，由运营部组织实施。获证客户的产品在产品质量国家监督抽查中被查出不合格时，自国家质检总局发出通报起 30 日内，运营部应对该企业实施监督审核。

组织若需推迟监督审核，应在监督到期 30 天前提出书面申请，并填写《ZXB 监督审核延期申请表》，阐明推迟的理由和期限，由运营部负责人批准，但延期不宜超过 3 个月。可接受的推迟监督理由可能是：不可抗力（如自然灾害）造成审核无法按期实施，获证客户的管理体系（或其一部分）因正常停工、停业（如季节性停工）暂停运行等，但对质量、环境、职业健康安全、信息安全等方面没有实质性影响的。

5.5.4 再认证审核

5.5.4.1 再认证审核包括获证客户最近一个认证周期体系运行绩效评价和现场审核。

5.5.4.2 通常再认证审核只进行一次现场审核；当获证客户、管理体系或管理体系的运作环境发生重大变更时（如法律法规标准变更、人员和区域重大变更、组织机构重大变更或产品范围变更、能源设施、设备、系统或过程发生重大变化等）可以考虑实施一阶段审核。此类变更可能在认证周期中的任何时间发生，运营部可能需要实施特殊审核，该特殊审核可能需要或不需要两阶段审核。

5.5.4.3 最近一个认证周期体系运行绩效评价应在再认证审核前进行，包括调阅以前的监督审核报告。运营部组织策划和实施再认证审核，以评价获证客户是否持续满足相关管理体系标准或其他规范性文件的所有要求。上述策划和实施应及时进行，以便认证能在到期前

及时更新。现场审核要求同上。

5.5.4.4 再认证审核目的是确认获证客户管理体系作为一个整体的持续符合性与有效性，以及与认证范围的持续相关性和适宜性。

5.5.4.5 再认证现场审核应关注

a）结合内部和外部变更来看的整个管理体系的有效性，以及认证范围的持续相关性和适宜性；

b）经证实的对保持管理体系有效性并改进管理体系，以提高整体绩效的承诺；

c）管理体系在获证客户方针目标和管理体系预期结果方面实现的有效性。

再认证审核应在认证证书到期前进行，在认证证书有效期满前三个月，获证客户应以书面的形式向 ZXB 提出再认证申请，再认证现场审核应至少在认证证书到期前一个半月进行，且与上次监督审核的时间间隔不得超过 12 个月，不符合项的关闭及认证决定应在证书期满前完成，新认证的终止日期可以基于当前认证的终止日期，新证书上的颁证日期应不早于再认证决定日期。如果在认证终止日期前，ZXB 不能对获证客户完成再认证审核或不能验证对严重不符合实施的纠正和纠正措施，则不应推荐再认证，也不应延长认证的效力。审核组应报告运营部，并告知客户及解释后果。在认证到期后，如果在 6 个月内完成未尽的再认证活动（即不符合项的关闭或认证决定），则可以恢复认证，否则应至少进行一次第二阶段才能恢复认证。证书的生效日期应不早于再认证决定日期，终止日期应基于上一个认证周期。

ISMS 再认证审核，应与本文件中有关客户 ISMS 的初次认证审核的要求保持一致。ISMS 允许采取纠正措施的时间，应与不符合的严重程度和相关的信息安全风险相一致。

SMS 再认证程序应与 ZXB 基于 ISO/IEC 20000-1 的服务管理体系认证审核的要求和指南保持一致。SMS 允许采取纠正措施的时间，应与不符合的严重程度和风险相适宜，以确保组织的服务满足规定要求。 如果纠正措施没有在同意的时间内完成，认证范围应被缩小，或暂停、撤销认证证书。

能源管理体系再认证审核，还应确定客户能源绩效的持续改进是否已得到证实。再认证审核也应考虑到设施、设备、系统或过程发生的重大变化。对能源绩效持续改进的确认是授予再认证的条件。注：能源绩效改进可能受到设施、设备、系统或过程变化、业务变化、或其他条件（导致能源基准的变更或产生变更需求）的影响。还应关注客户整个认证周期的能源管理绩效，获证组织能耗及核算边界的变化情况，包括管理体系有效人员的重大变化对能源绩效的影响等。

5.6 现场审核实施

5.6.1 举行首次会议

5.6.1.1 审核组应与受审核方的管理层（包括最高管理者及拟审核职能或过程的负责人员）召开正式的首次会议，审核组应当提供首次会议签到表，参会人员应签到并保存记录。在首次会议开始前，审核组成员应主动向受审核方出示身份证明文件。首次会议通常由审核组长主持，会议目的是简要解释将如何进行本次审核活动，详略程度可视客户对审核过程的熟悉程度而调整。首次会议应包括以下内容，并填写《首次会议记录》表。

a）审核组和受审核方各自介绍参会人员，包括简要介绍其角色；

b）确认认证范围；

c）确认审核计划（包括审核的类型、范围、目的和准则）及其任何变化，以及与受审核方的其他相关安排，例如末次会议的日期和时间，审核期间审核组与受审核方管理层进行沟通的时间安排；

d）确认审核组与受审核方之间的正式沟通渠道；

e）确认审核组可获得所需的资源和设施；

f）确认与保密有关的事宜；

g）确认适用于审核组的相关的工作安全、应急和安保程序；

h）确认可得到向导和观察员并明确其职责；

i）报告的方法，包括对审核发现的任何分级；

j）说明可能提前终止审核的条件；

k）确认审核组长和审核组代表 ZXB 对审核负责，并应控制《审核计划》（包括审核活动和审核路径）的执行；

l）适用时，确认以往评审或审核的发现的状态；

m）基于抽样实施审核的方法和程序；

n）确认在审核中将告知受审核方审核进程及任何关注点；

o）确认审核中使用的语言（适用时）；

p）给受审核方提问的机会。

5.6.1.2 应特别注意：在首次会议上，审核组长应再次和受审核方确认审核范围，包括产品/服务/活动范围、场所范围，以及有多现场时的分布情况等。

5.6.2 审核过程中的沟通

5.6.2.1 在审核过程中，依据《审核计划》，审核组内部或审核组与受审核方之间应进行必要的沟通，以交换审核信息或评估审核进展情况。审核组长应在需要时在审核组成员之间重新安排审核任务，并将审核进程及任何关注告知受审核方。

5.6.2.2 当可获得的审核证据显示受审核方违反了法律法规，或审核目的将无法实现，或显示存在紧急和重大的风险（例如安全风险）、或终止审核、或推荐不通过/延期推荐等情况时，审核组长应向受审核方（如果可能还应报告 ZXB 运营部，得到同意后与受审核方进行沟通）报告这一情况，以确定如何采取适当的行动。该行动可以包括重新确认或修改《审核计划》，改变审核目的或审核范围，或者终止审核。审核组长应向 ZXB 运营部报告所采取行动的结果。

5.6.2.3 如果在现场审核活动中发现需要改变审核范围，审核组长应与受审核方核查该需要，并报告 ZXB 运营部。

5.6.2.4 在现场审核时，审核组长不能自行做出扩大审核范围的决定。如需扩大审核范围，应报告运营部同意后方可扩大审核。

5.6.2.5 在现场审核时，发现不适用受审核方的 QMS 的认证标准的某些要求与实际不符合、人数与合同不符且影响到人日数时，审核组长应及时与运营部沟通。

5.6.2.6 在现场审核时，发现受审核方资质证书、校准证书、检定证书等即将到期，审核组应告知受审核方在换发新证书后，应第一时间提交至运营部。如到期未及时提交有效资质、校准、检定等证书影响审核有效性的，将对证书作出暂停处理。

5.6.3 收集审核证据，形成审核发现

5.6.3.1 在审核过程中，通过适当的抽样来获取与审核目的、范围和准则相关的信息（包括与职能、活动和过程之间的接口有关的信息），并对这些信息进行验证，使之成为审核证据。收集审核证据，且只有可证实的信息方可作为审核证据。审核证据可以是：对活动/过程、环境和条件等观察的结果；面谈获得的信息；查阅有关文件、记录获得的信息等。另外，SMS 认证审核所使用的信息收集方法还宜包括对 SMS 过程有效性的测试。对于 OHSMS 审核时，审核组应面谈以下人员：负有 OHS 法律责任的管理者；负责 OHS 的员工代表；负责监视员工健康的人员，如医生和护士，远程面谈的理由应被记录；管理人员、长期和临时员工。还宜面谈其他人员：从事与预防 OHS 风险相关活动的管理人员和员工，和承包方的管理者和员工。

5.6.3.2 应基于审核准则和审核证据，评价过程/活动的符合性，即形成审核发现，审核发现应简述符合性，详细描述不符合以及为其提供支持的审核证据，并予以分级、记录和报

告，以便为认证决定或保持认证提供充分的信息。审核记录要求，见 ZXB-GZ-01《管理体系认证通用审核指南》。

5.6.3.3 对不符合的判定不能偏离和超出审核准则的要求，应对照审核准则的具体要求予以记录，包含对不符合的清晰陈述，并详细标识不符合所基于的客观证据。不符合项的开具是否合理应由审核组长在审核组内部会议上讨论确定，并由审核员签字、审核组长签字确认、受审核方签字确认。当发现不符合有关法规要求时应将这类不符合立即通知给受审核组织，进行原因分析和采取纠正和纠正措施。

5.6.3.4 在与组织领导层进行沟通时，应就不符合的审核发现与受审核方进行沟通和讨论，以确保证据准确且使组织理解不符合报告的内容并提出纠正/纠正措施要求，但是，审核员应避免提示不符合的原因或解决方法。审核组长应尝试解决审核组与受审核方之间关于审核证据或审核发现的任何分歧意见，未解决的分歧点应予以记录。审核组可以识别和记录改进机会，除非某一管理体系认证方案的要求禁止这样做。但是属于不符合的审核发现不应作为改进机会予以记录。审核组可以指出改进机会，但不应提出具体解决办法的建议。

5.6.3.5 审核组长应监督、检查、协调、指导审核组成员按《审核计划》进行审核，沟通审核信息。应特别注意检查审核证据的充分性、审核记录的符合性。

5.6.3.6 在现场审核过程中应特别注意：

a）核查体系覆盖的人数；

b）确认认证审核的范围；

c）确认 QMS 认证标准不适用的合理性；

d）对涉及 3C 认证、生产/制造/安装/餐饮服务许可证、安全生产许可证、食品生产许可证等纳入国家行政许可的产品，应特别注意收集相关证据并核查。如果受审核方不能提供时，应及时和运营部联系，取消相应认证审核范围。如相关证书即将到期时，审核组应通过 ERP 系统将即将到期信息传递至运营部。另外，审核范围涉及的各类证明文件的复印件应是在原件上复印的，并经审核员签字确认与原件一致。

e)对于 ISMS 审核，审核组还应特别关注以下的特定要素，

1）要求受审核方证实对信息安全相关风险的评估与 ISMS 范围内的 ISMS 运行是相关的和充分的；

2）确定受审核方识别、 检查和评价信息安全相关风险的规程及其实施结果是否与受审核方的方针、目标和指标相一致。

另外审核组还应确定用于风险评估的规程是否健全并得到正确实施。

5.6.4 准备审核结论

在末次会议前，审核组长应组织审核组成员对照审核目的和审核准则审查审核发现和审核中获得的任何其他适用的信息并对不符合分级；考虑审核过程中内在的不确定性，就审核结论达成一致；就任何必要的跟踪活动达成一致；确认审核方案的适宜性，或识别任何为将来的审核所需要的修改（例如认证范围、审核时间或日期、监督频次、审核组能力）。

5.6.5 与受审核方领导层的沟通

由审核组长主持，审核组成员参加，向受审核方领导层通报审核情况和审核结论，充分沟通并达成共识。对于审核中发现的不符合，审核组应要求受审核方在规定期限内分析原因，并说明为消除不符合已采取或拟采取的具体纠正和纠正措施。一般不符合项关闭时间为 30 日内完成，如遇有特殊情况，一般不符合项关闭时间不宜超过 90 日内完成。对于严重不符合项，初审二阶段应在最多不超过 6 个月内关闭。如果未能在第二阶段结束后 6 个月内验证对严重不符合实施的纠正和纠正措施，则应按不予通过认证，或者重新实施第二阶段审核。监督、再认证等其他审核时严重不符合项关闭时间一般为 15 日内完成，并且再认证审核时严重不符合应在认证到期前关闭。

5.6.6 召开末次会议

5.6.6.1 审核组全体成员、受审核方有关领导及人员（包括最高管理者及所审核职能或过程的负责人员）召开正式的末次会议，审核组应当提供末次会议签到表，参会人员应签到并保存记录，由审核组长主持，报告审核发现和审核结论，包括关于认证的推荐性意见。不符合应以使其被理解的方式提出，并应就回应的时间表达成一致，并保存相关记录。

另外，对于 OHSMS，应要求受审核方代表邀请负有 OHS 法律责任的管理者，负责监视员工健康的人员、负责 OHS 的员工代表参加末次会议。如未出席应记录缺席的理由。

注：“被理解”不一定意味着受审核方已经接受了不符合。

5.6.6.2 末次会议的详略程度应与受审核方对审核过程的熟悉程度一致，应包括如下要素，具体内容见《末次会议记录》表。

a）向受审核方说明所获取的审核证据基于对信息的抽样，因而会有一定的不确定性；

b）进行报告的方法和时间表，包括审核发现的任何分级；

c）ZXB 处理不符合（包括与受审核方认证状态有关的任何结果）的过程；

d）受审核方为审核中发现的任何不符合的纠正和纠正措施提出计划的时间表；

e）ZXB 在审核后的活动；

f）说明投诉处理过程和申诉过程。

5.6.6.3 受审核方应有机会提出问题。审核组与受审核方之间关于审核发现或结论的任何分歧意见，应得到充分讨论并尽可能获得解决。任何未解决的分歧意见，应予以记录并提交ZXB 技术部。

5.6.7 编制审核报告

5.6.7.1 ZXB 应为每次审核向受审核方提供书面报告，并拥有对审核报告的所有权。审核组长应确保“审核报告”的编制，并应对“审核报告”的内容负责；“审核报告”应提供对审核的准确、简明和清晰的记录，以便为认证决定提供充分的信息；审核报告应由审核组组长签字，审核结论应有审核证据的充分支持。一般情况下，“审核报告”宜包括或引用下列内容，具体见《管理体系审核报告》：

a）注明认证机构；

b）受审核方的名称和地址及受审核方的代表；

c）审核的类型（例如初次、监督、再认证或特殊审核）；

d）审核准则；

e）审核目的；

f）审核范围，特别是标识出所审核的受审核方组织或职能单元或过程，以及审核时间；

g）任何偏离审核计划的情况及其理由，包括对审核风险及影响审核结论的不确定性的客观陈述；

h）任何影响审核方案的重要事项；

i）注明审核组长、审核组成员及其个人注册信息及任何与审核组同行的人员；

j）审核活动（现场或非现场，永久或临时场所）的实施日期和地点；

k）与审核类型的要求一致的审核发现、对审核证据的引用以及审核结论；对目标和过程及绩效实现情况进行评价；

l）如有时，在上次审核后发生的影响受审核方管理体系的重要变更；

m）已识别出的任何未解决的问题；

n）适用时，是否为结合、联合或一体化审核；

o）说明审核基于对可获得信息的抽样过程的免责声明；

p）审核组的推荐意见；

q）适用时，接受审核的受审核方对认证证书和标志及审核报告的使用进行着有效的控制；

r）适用时，对以前不符合采取的纠正措施有效性的验证情况；

s）识别出的不符合项。不符合项的表述，应基于客观证据和审核依据，用写实的方法准确、具体、清晰描述，易于被申请组织理解。不得用概念化的、不确定的、含糊的语言表述不符合项；

t）关于管理体系符合性与有效性的声明以及对下列方面相关证据的总结：

-- 管理体系满足适用要求和实现预期结果的能力；

-- 内部审核和管理评审的过程；

u）对认证范围适宜性的结论；

v）确认是否达到审核目的；

ISMS 审核报告除满足上述通用要求外，还应提供以下信息或对这些信息的引用：审核的说明，其中包括了文件评审摘要；对客户信息安全风险分析进行认证审核的说明；与审核计划的偏离（例如：在某一预定的活动上花费更多或更少的时间）；ISMS 的范围。审核报告应足够详细，以帮助和支持认证决定。审核报告应包括：所采用的主要审核路线和所使用的审核方法；形成的观察结果，包括正面的（例如值得注意的特征）和负面的（例如，潜在的不符合）；对客户 ISMS 与认证要求的符合性的评价意见、对不符合的清楚说明、所引用的适用性声明的版本，以及适用时，与客户以往认证审核结果的任何有用的对照。完整的问卷、检查清单、观察结果、日志或审核员笔记可以构成完整的审核报告的一部分。在审核过程中，有关被评价的样本的信息应包含在审核报告或其他认证资料中；报告应考虑客户所采用的内部组织和规程的充分性，以便对其 ISMS 建立信心。报告还应包括：关于 ISMS 要求和信息安全控制的实施与有效性的、最重要的观察（正面的和负面的）的摘要。审核组关于客户的 ISMS 是否获得认证的建议，以及支持该建议的信息。

SMS 审核报告除满足上述通用要求外，还应足够详细，以支持认证决定。审核报告应包含认证范围的界定，提及范围的任何变更，并描述所遵循的重要审核路线和所使用的审核方法。报告应包括审核组对客户 SMS 认证的推荐意见，以及证实该推荐意见的信息。这种证实应包括对与 SMS 的实施和有效性相关的不符合和改进机会的总结。

能源管理体系审核报告除满足上述通用要求外，还应包括所审核的能源管理体系的范围和边界，对能源管理体系持续改进成果和能源绩效改进成果的陈述，以及支持这些陈述的审核证据。能源管理体系的认证范围包括相关的活动、设施和过程等。审核报告应对组织能源管理体系的符合性和有效性进行全面描述和评价，至少应详细描述《能源管理体系认证规则》6.4.2 条明确的重点关注内容。其中，对能源目标、能源指标、能源绩效情况应有量化表述，对测量和验证方法进行简要描述，并对组织的能源管理体系在促进能源绩效

持续改进方面的作用做出评价。

ZXB 应保留用于证实审核报告中相关信息的证据。

5.6.7.2 审核报告编制的注意事项：

a）栏目填写、签字、盖章齐全准确；

b）受审核方名称、地址应与营业执照一致，地址不一致时应予以说明；

c）各栏目填写内容应与审核证据保持一致，并应逐项就审核证据、审核发现和审核结论进行详细描述；

d）确认的审核范围应与认证证书、审核计划书一致，与计划书不一致时应予以说明；

e）如涉及多现场时，要按要求填写清楚；

f）需要子证书时，其分支机构的名称、地址、覆盖的产品/服务/活动范围要和认证证书保持一致；

g）审核报告应随附必要的用于证明相关事实的证据或记录，包括文字或照片摄像等音像资料

h）对于监督审核，如发生组织结构调整、体系文件修改、主要负责人更换、场所/产品覆盖范围发生扩大/缩小时，应具体说明；

i）对暂停恢复等特殊审核，应给出是否推荐恢复等意见。

5.6.7.3 第一阶段审核、第二阶段审核、监督审核、再认证或其他非例行监督审核时，应编制“审核报告”。

5.6.7.4 ZXB 应在作出认证决定后 30 个工作日内将审核报告提交受审核方，并保留签收或提交的证据。

5.6.8 现场审核过程中异常/突发事件的处理

5.6.8.1 涉及受审核方有关事宜，均由审核组长出面处理。审核组其他成员不得擅自处理，但应主动配合审核组长工作。审核组内部事务应以审核组长意见为准。

5.6.8.2 若审核组发现受审核方人员中有人拒绝回答审核员所提问题、拒绝提供所需资料、故意答非所问或以其它方式不予以合作时，审核组长应立即与受审核方的管理者代表或负责人员沟通解决。

5.6.8.3 若审核组内部或与受审核方之间发生了无法处理或协调的异常/突发事件时，审核组长应立即上报运营部审核任务安排人员。

5.7 终止现场审核规定

5.7.1 终止现场审核的条件

现场审核时，当受审核方出现下述情况之一时，应终止现场审核：

5.7.1.1 现场审核时发现：

a）组织不能提供或提供的资质证书、3C 证书、生产/制造/安装/餐饮服务许可证、安全生产许可证、食品生产许可证等证照、证件、证书、证明无效的；

b）管理体系未运行或运行未满 3 个月（建筑施工企业/能源管理体系未满 6 个月）的；

c）没有按规定进行内部审核或管理评审的；

d）受审核方实际情况与申请材料有重大不一致。

5.7.1.2 无人接受审核或对审核活动不予配合等致使审核活动无法进行的。

5.7.1.3 受审核方提出终止审核的。

5.7.1.4 发现受审核方存在重大质量/环境/职业健康/信息安全问题或有其他严重违法违规行为。

5.7.1.5 出现其他无法继续审核情况的。

5.7.2 终止现场审核的办理

5.7.2.1 当终止现场审核条件出现时，由审核组长向运营部提出终止现场审核申请，并说明理由。

5.7.2.2 由运营部经理同意后，通知审核组长终止现场审核。

5.7.2.3 由审核组长与受审核方协商解决与审核有关的后续事宜。

5.7.2.4 对终止现场审核的项目，审核组应将已开展的工作情况形成报告，ZXB 应将此报告及终止现场审核的原因提交给受审核方，并保留签收或提交的证据。

5.8 现场审核时对生产/服务/活动现场的要求

5.8.1 审核安排与实施审核时对生产现场的要求

5.8.1.1 运营部在安排审核任务前，应与受审核方联系确认生产/服务/活动现场情况，没有生产现场不得安排现场审核。

5.8.1.2 审核组长在实施现场审核前应再次与受审核方联系确认生产/服务/活动现场情况，没有生产现场不得进场实施现场审核。

5.8.1.3 当审核组已经进驻现场后发现没有任何生产/服务/活动现场的，审核组长应与运营部、受审核方充分沟通后终止现场审核。

5.8.2 认证决定时对生产/服务/活动现场的要求

生产现场情况	初审/再认证	监督
申请一种产品/服务/活动，但无现场。	不能推荐注册	不能推荐保持注册
申请多种产品/服务/活动，其中部分种类有资料无现场。	无现场的种类 不能推荐注册	可推荐保持注册，但应 3 年覆盖。
申请系列产品/服务/活动，系列内一种有现场。	若无现场的产品除现场外的其他证据充分，且有现场产品的控制符合标准要求，则可推荐注册，但监督应考虑 3 年覆盖；无现场，亦无其他充分证据的，不可推荐注册。	可推荐保持注册
申请了设计，但设计活动有资料没有现场。	推荐注册	推荐保持注册
建筑业组织，有全部工程类型现场，但每类工程只有部分施工过程现场，其余施工过程有资料。	推荐注册	推荐保持注册
建筑业组织，不能提供认证范围内的所有工程类型现场，但有资料。	无现场的工程类型， 不能推荐注册。	可推荐保持注册，但应 3 年覆盖。
设计院具有多方面设计能力（如化工、电子工程）、软件公司具有多行业软件开发能力（如银行、电讯），审核时只能见到部分项目活动，其余有资料。	推荐注册	推荐保持注册
监督时，不能提供任何生产/服务现场（或生产/服务活动）。	/	不能推荐保持注册

说明：对因没有生产/服务/活动现场，而不能推荐注册或不能推荐保持注册的，可在有生产/服务/活动现场并补充现场审核满足要求后推荐注册或推荐保持注册。

5.8.3 组织的服务点在审核中的管理要求(适用于 SMS)

5.8.3.1 服务点的抽样

通过在服务点观察客户的服务状况、与相关人员（如驻场的服务工程师、客户的顾客等）面谈以及调阅现场服务记录，认证机构可以收集客户 SMS 运行和有效 性的证据。

5.8.3.2 抽样条件

当客户拥有满足以下条件的多个服务点时，认证机构可以考虑使用基于抽样的方法对服务点进行审核：

a）所有场所的工作人员均在同一个 SMS 下进行管理，客户对人员具有分配和调配的权力，有权要求场所内提供服务的工作人员提供工作量和工作质量的数据；

b）客户在所有的场所提供的服务和活动的变动，或场所的成立和撤销不影响客户的 SMS 运行的完整性；

c）所有的场所都包含在客户的 SMS 内部审核方案和管理评审方案中。

5.8.3.3 抽样方法

1）在确定服务点的抽样量时，针对审核时客户所具有的服务点，认证机构可先考虑确保样本覆盖认证范围内的业务类别，然后再根据服务点数量适当增加 抽样量。

a）初次认证审核、监督审核和再认证审核时，样本覆盖认证范围内所涉及到的表 A.1 中的中类；

b）初次认证审核和再认证审核时，在满足 a）的基础上按照下表增加抽样量：

服务点数量（个）	增加的服务点抽样量（个）
5 ~10	1
11 ~20	2
21 ~40	3
41 ~60	4

注：当服务点的数量超过 60 时，可沿用上表的规律确定应增加的抽样量。

2）抽样时，优先选取同种业务类型中业务复杂程度高且服务交付风险大的服务点；

3）对出现审核组无法访问服务点的情形规定了应对措施。

5.8.3.4 审核时间

1）认证机构分配给每个服务点的审核时间宜与审核组在该服务点所需完成的审核活动相匹配。

2）通常，每个服务点的审核宜不少于 0.25 个人天。

3）每个服务点的审核时间不含审核员的旅途时间。

5.9 现场审核结束后有关信息的收集

5.9.1 初次/再认证/扩大或缩小认证范围的监督等涉及认证证书发放的审核，审核组长应请受审核方填写《认证证书中英文稿》，并请受审核方负责人签字盖章，审核组长签字确认。受审核方名称、地址、体系覆盖人数、认证范围、分支机构等应和“审核报告”一致，不一致时应予以说明。审核组长对中文表述的正确性负责。

5.9.2《廉洁自律声明》请受审核方评价、签字盖章和封存后，随审核资料交回。

5.9.3 运营部请受审核方填写“认证客户满意度调查”并统计。

5.10 审核资料的整理与上报

5.10.1 现场审核结束后，审核组长负责将审核案卷进行整理、复核，对受审核方提交的整改材料验证有效关闭后一并提交认证机构 ERP 系统，文本资料提交至运营部。提交审核案卷的时限要求是现场审核结束后 45 天内，如果案卷 45 天仍旧不能关闭，审核组长应说明情况后将案卷交技术部。

5.10.2 审核组长在接到受审核方的整改资料后，对于所有严重不符合，审核组已审查、接受和验证了纠正和纠正措施；对于所有轻微不符合，审核组已审查和接受了客户对纠正和纠正措施的计划。审核组应将审查和验证的结果告知受审核方。

如果为了验证纠正和纠正措施的有效性而且在审核发现不够充分的情况下，需要进行全面或部分的补充审核，或需要受审核方提供形成文件的证据（在将来的监督或再认证审核中予以确认），则审核组或运营部应告知受审核方。

5.10.3 对技术部在认证决定过程中提出的问题，审核组长有责任积极采取补救措施。

5.10.4 第一、二阶段审核案卷应分别整理后提交运营部。

5.10.5 ZXB 所有认证人员应当遵守与从业相关的法律法规，对认证审核活动及相关认证审核记录和认证审核报告的真实性承担相应的法律责任。为了提供效率，节省资源，部分资料可进行无纸化归档，《案卷盖章/签字汇总表》作为主要的签字文件。

6、相关记录

1)、 ZXB《认证组织审核案卷目录》

2)、 ZXB《认证申请评审表》

3)、 ZXB《多场所清单》

4)、 ZXB《临时场所清单》

5)、 ZXB《在建和竣工项目清单》

6)、 ZXB《审核通知书》

7)、 ZXB《审核计划》

8)、 ZXB《现场审核计划》

9)、 ZXB《文件评审报告》

10)、 ZXB《对再认证组织上一周期的绩效评价》

11)、 ZXB《公正性与保密声明》

12)、 ZXB《审前沟通与培训记录》

13)、 ZXB《现场审核会议签到表》

14)、 ZXB《一阶段首次会议记录》

15)、 ZXB《一阶段末次会议记录》

16)、 ZXB《首次会议记录》

17)、 ZXB《末次会议记录》

18)、 ZXB《一阶段不到现场审核计划与记录》

19)、 ZXB《现场审核记录》

20)、 ZXB《第一阶段审核问题汇总表》

21)、 ZXB《不符合报告》

22)、 ZXB《观察项报告》

23)、 ZXB《第一阶段审核报告》

24)、 ZXB《管理体系审核报告》

25)、 ZXB《非例行现场审核记录及报告》

26)、 ZXB《管理体系终止审核报告》

27)、 ZXB《不符合项分布统计表》

28)、 ZXB《审核信息传递表》

29)、 ZXB《认证证书中英文稿》

30)、 ZXB《廉洁自律声明》

程 序 文 件

认证证书和认证标志管理程序

文件编号： ZXB-CX-08

文件状态： 受 控

版本	编修	审核	批准	编写/修订日期	生效日期
A/0	崔朝敏	李蒙	白金泽	2018-03-27	2018-04-01
B/0	杨雅兰	李浩	刘东	2019-06-12	2019-06-20
B/1	赵学菊	李浩	刘东	2020-03-06	2020-03-10
B/2	张京梅	李浩	刘东	2020-9-4	2020-9-10
C/0	毕金霞	张京梅	李浩	2021-04-26	2021-04-26
D/0	马 林	张京梅	李浩	2022-02-14	2022-02-15
D/1	马 林	张京梅	郑宇兵	2024-04-16	2024-04-16

1 范围

本程序规定了对管理体系认证证书和认证标志的基本要求和管理办法。

本程序适用于 ZXB 颁发管理体系认证证书和认证标志的管理工作。

2 引用文件

下列文件中的条款通过本文件的引用而成为本文件的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本程序。凡是不注日期的引用文件，其最新版本适用于本文件。

2.1 《质量管理体系认证规则》（现行有效版本）

2.2 《基于 ISO/IEC 20000-1 的服务管理体系认证实施规则》（现行有效版本）

2.3 《认证证书和认证标志管理办法》（现行有效版本）

2.4 CNAS-CC01-2015《管理体系认证机构要求》

2.5 CNAS-CC02_2013《产品、过程和服务认证机构要求》

2.6 CNAS-CC131_2017《质量管理体系审核及认证的能力要求》

2.7 CNAS-CC121_2017《环境管理体系审核及认证的能力要求》

2.8 CNAS-CC125_2018《职业健康安全管理体系审核及认证的能力要求》

2.9 CNAS-CC170:2015《信息安全管理体系认证机构要求》

2.10 CNAS-CC175:2017《基于 ISO-IEC 20000-1 的服务管理体系认证机构要求》

2.11 CNAS-CC190:2021《能源管理体系认证机构要求》

2.12 CNAS-SC25:2023《服务认证机构认可方案》

2.13 CNAS-R01《认可标识使用和认可状态声明规则》

2.14 CNAS-RC01《认证机构认可规则》

2.15 服务认证实施规则

3 术语和定义

引用文件等给出的术语和定义适用于本文件。

4 职责

4.1 综合部负责认证证书、ZXB 认证徽标的样式设计。

4.2 运营部负责认证证书制作、发放。

4.3 运营部负责对获证客户使用认证证书和认证标志情况实施监督检查。

4.4 运营部及审核组长负责告知获证客户按照本程序的要求使用认证证书和认证标志。

4.5 当发现获证客户错误使用认证证书和认证标志时，由技术部调查处理。此类措施可以包括要求纠正或采取纠正措施、暂停认证证书、撤销认证证书、公告违规行为以及必要的法律措施。

4.6 运营部负责认证证书及相关信息的上报工作。

4.7 运营部负责认证证书暂停、恢复、撤销工作的处理。

5 认证证书使用管理规定

5.1 获证客户使用认证证书时的权利和义务

5.1.1 获证客户在认证证书的有效期内有权正确使用认证证书，包括：

a) 认证证书可以展示在文件、网站、广告和宣传资料中或广告宣传等商业活动，以及通过认证的工作场所、销售场所；

b) 获证客户可以在有效的管理体系认证证书覆盖的领域和业务范围内以准确的文字描述认证证书中所承载的有关信息，如：“本组织（或企业）通过众信标（北京）认证有限公司的×××（即获证客户获得的相应管理体系认证标准的名称或标准编号）管理体系认证，证书号为××××”；

c) 在符合 b）项要求的情况下，可将 ZXB 认证徽标使用在运输产品的大箱子（等）上和用作广告宣传的小册子（等）中；

d) 对其他单位和个人妨碍本组织使用认证证书的行为可以向 ZXB 提出投诉。

5.1.2 获证客户使用认证证书和认证标志时应承担以下义务：

a）获证客户在传播媒介(如互联网、宣传册或广告)或其他文件中引用认证状态时，应符合 ZXB 的要求。

b）使用 ZXB 的认证标志，需向 ZXB 提出申请。在使用时，其图案必须按照 ZXB 提供的图案的比例放大或缩小，并且做到颜色一致。未经 ZXB 许可不得使用认证标志.获证组织不能单独使用 CNAS 认可标识，必须和 ZXB 认证标志以及获证客户的标志或名称结合使用。

c) 不得在任何资料中有关于其认证资格的误导性说明；

d）不得以误导性方式使用认证文件或其任何部分；

e) 不得利用管理体系认证证书和相关文字、符号，暗示或误导公众认为认证证书覆盖

范围外的管理体系、产品或服务、过程、活动和场所获得 ZXB 的认证；

f）宣传认证结果时不得损害 ZXB 的声誉和（或）使认证制度声誉受损，失去公众信任；

g）不得擅自更改证书内容；

h）不得伪造、涂改、出借、出租、转让、倒卖、部分出示、部分复印证书；

i）获证客户应妥善保管好认证证书，以免丢失、损坏；

j）获证客户的管理体系若发生重大变化时，应及时报告 ZXB ，接受 ZXB 的调查或监督检查。对经监督检查不合格者，不得继续使用认证证书；

k）在认证范围被缩小时，应及时修改所有的广告宣传材料；

l）认证证书被暂停期间，相应的认证领域的管理体系认证暂时无效。认证客户应停止使用认证证书和认证标志，直到造成暂停的问题得到解决。如果客户在规定的时限内未能解决造成暂停的问题，ZXB 将撤销或缩小相应领域的认证范围；

m）证书被 ZXB 撤销，获证客户应按 ZXB 的要求将证书交还给 ZXB ，并同时使用所有引用认证资格的广告材料。停止在文件、网站、广告和宣传资料中或广告宣传等商业活动，以及在工作场所、销售场所展示认证证书；

n）不应允许其标志被获证客户用于实验室检测、校准或检验的报告或证书；

o）标志不应用于产品或产品包装之上，或以任何其它可解释为表示产品符合性的方式使用；注：产品包装的判别标准是其可从产品上移除且不会导致产品分裂、破裂或损坏。

p）认证证书和认证标志的使用应符合《认证证书和认证标志管理办法》的规定；

q）认证标志使用时可以等比例放大或缩小，但不允许变形、变色；

r）证书持有人应对认证证书和认证标志的使用和展示进行有效的控制。

6 要求

6.1 认证证书的基本内容

6.1.1 认证证书应至少涵盖以下基本内容：

a）证书编号、证书名称（管理体系认证证书）、有效期的起止年月日；

b）获证组织名称、地理位置（或多场所认证范围内总部和所有场所的地理位置）、统一社会信用代码（或组织机构代码）。该信息应与其法律地位证明文件的信息一致；

c）认证审核时所用的管理体系标准和（或）其他规范性文件，包括发布状态的标示（例如修订时间或编号）。应清晰地表述获证组织所获认证的管理体系符合相应管理体系认证的

标准和（或）认证要求等。

d）管理体系认证所覆盖的范围，（对多场所组织还应在证书上或附件中明确注明已获准认证的分场所名称，地址，活动、产品和服务类型等相关认证范围；该信息应与相应的法律地位证明文件信息一致；

ISMS 认证证书中宜从客户的业务、组织结构、位置和技术特点等方面清晰地界定认证所覆盖的 ISMS 范围。如果由于客户的信息安全的原因不能在认证证书上明示上述全部与客户 ISMS 范围相关的信息时，通过在认证证书上引用客户的适用性声明的方式是一种可以采取的间接方式。客户的 ISMS 认证范围和适用性声明中要体现认证范围所界定的活动并扩展到活动的边界。

SMS 认证证书中所覆盖的范围宜基于服务提供者对 SMS 范围的描述界定。在界定范围时，宜应用 ISO/IEC 20000-3 中的指南；SMS 认证证书内容应包括通过认证的服务类别。

EnMS 认证所覆盖范围应表明主要的能源生产、供应和使用场所。应表明与产品（包括服务）、过程等相关的认证范围，即特定场所的能源管理控制下的具体活动；适用时，获证客户的认证文件应包括总部以外的每个场所相应的认证范围，即多场所组织的每个场所的特定信息（如名称和地理位置等），及该场所能源管理控制下的具体活动。应分别描述特定场所的信息，并使具体活动与特定场所信息形成对应关系。明确表述获证组织能源管理体系边界和能源绩效。

e）授予认证、扩大或缩小认证范围、更新认证的生效日期，生效日期不应早于相关的认证决定的日期；

（注：当证书失效一段时间时，ZXB 在清晰标示了当前认证周期的开始时间和截止时间，并把上一认证周期截止时间连同再认证审核的时间一起标示时，可在证书上保留原始的认证日期。）

f）认证有效期或与认证周期一致的应进行再认证的日期（包括证书签发日期及有效期的起止年月日，对初次认证以来未中断过的再认证证书，可表述该获证组织初次获得认证证书的年月日）；

g）证书编号；

h）ZXB 名称、地址和 ZXB 认证徽标；

i）ZXB 签章和董事长授权人员签字；

j）CNAS 认可标识及认可注册号（适用于获得 CNAS 认可的业务范围）；

k）认可机构已签署国际互认协议领域，应与认可机构签订协议并经许可，可附加国际认可论坛 IAF-MLA 国际互认标识。

l）证书查询方式:

证书上注明：“本证书信息可在国家认证认可监督管理委员会官方网站（www.cnca.gov.cn）和 www.cnas.org.cn 和 www.zhongxinbiao.com 上查询”，以便于社会监督。

m）认证证书在有效期内的监督情况。应在证书上注明：获证组织在证书有效期内须每年至少接受一次监督审核并将监督审核合格标识粘贴于证书指定位置，此证书方为有效的提示。

n）认证用标准和（或）其他规范性文件所要求的任何其他信息；

o）在颁发经过修改的认证文件时，区分新文件与任何已作废文件的方法；

p）ISMS 认证证书应包括适用性声明的版本（如果适用性声明的变更没有改变认证范围中控制措施的覆盖范围，则不要求更新认证证书）。ISMS 认证证书也可以包括所使用的行业特定标准。

q）ZXB 的名称、地址和认证标志。

r) 服务认证证书应至少包括以下基本内容：

（1）ZXB 的名称及其认证标志；

（2）认可标识（适用时）；

（3）获证组织的名称、地址及其服务提供场所的地址；

（4）认证范围；

（5）服务认证依据的标准；

（6）服务认证方案（适用时）；

（7）发证日期和认证有效期（适用时）；

（8）证书编号， 服务认证证书有效期三年，证书应注明：获证组织必须定期接受监督评价并经评价合格此证书方继续有效的提示信息。

（9）其他需要标注的内容。

6.1.2 如果认证所覆盖产品（或服务）的类别及其所涉及的过程和覆盖的场所较多，可在证书附件上加以注明。

6.1.3 初次认证认证证书有效期最长为 3 年。再认证的认证证书有效期不超过最近一次有效认证证书截止期再加三年。

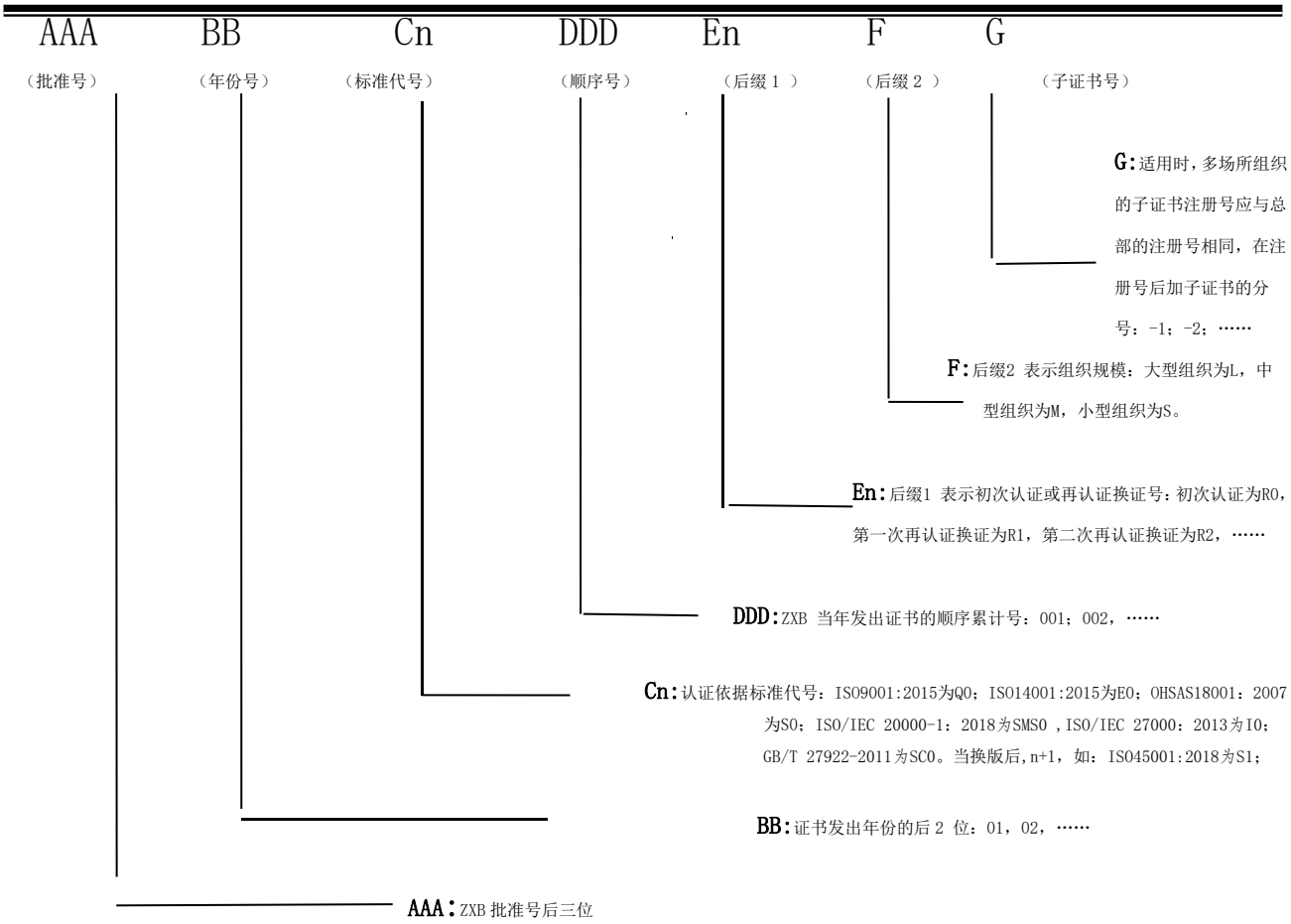
6.1.4 ZXB 建立证书信息披露制度。除向申请组织、认证监管部门等执法监管部门提供

认证证书信息外，还应当根据社会相关方的请求向其提供证书信息，接受社会监督。

6.2 认证证书的规定格式

6.2.1 认证证书编号的规定格式

6.2.1.1 认证证书编号的规定格式（适用于 QMS/EMS/OHSMS/ISMS//SMS/EnMS/SC）：



6.2.1.2 对同一个组织实施的同一个管理体系认证，赋予一个认证证书编号。

6.2.1.3 同一个组织的认证范围覆盖多个场所并需要颁发子证书时，在子认证证书编号后加上“-”和序号，如-1(-2，-3，… ）。

6.2.1.4 有效期内换发证书，认证证书编号中的机构注册号、年份号、顺序号和认证的有效期保持不变，应注明换证日期。

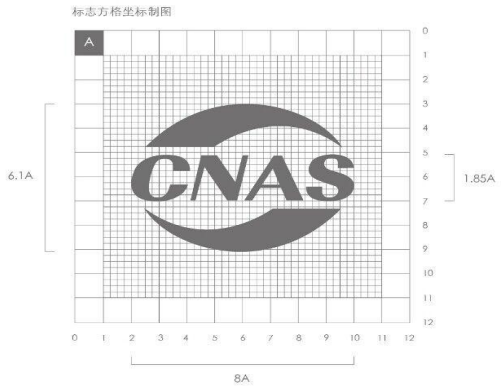
6.2.1.5 再认证完成后换发证书，按 6.2.1 规定重新赋予认证证书编号，第一次再认证为“R1”，第二次再认证为“R2”，依此类推。

6.2.1.6 撤销证书后，原认证证书编号废止，不再它用。

6.2.1.7 认证证书上的认证机构名称应与相应的认证机构批准书上的名称一致。

6.2.2 认可徽标/标识和 IAF-MLA 标识的规定格式/式样：

6.2.2.1 CNAS 徽标的规定格式：



a) CNAS 徽标的规格如图所示，可成比例放大缩小，应清晰可辨。

b）CNAS 徽标的颜色：

CNAS 徽标的基本颜色为蓝色或黑色。

蓝色：C：100 M：95 Y：25 K：0 （标准色）

C：100 M：56 Y：0 K：0 （标准色）

黑色：C：0 M：0 Y：0 K：100 （标准色）

c) CNAS 徽标代表 CNAS 机构的特定图形，CNAS 拥有其所有权和使用权，并受法律保护，其他机构和个人未经 CNAS 的书面允许不得使用 CNAS 徽标。

d)CNAS 徽标可用于 CNA 认可证书、公开出版物、文件、办公用品、宣传品、网页宣 S 传等，可采用印刷和电子图文等方式使用。

6.2.2.2 CNAS 认可标识的式样：

认证机构 CNAS 认可标识由 CNAS 徽标和标明基本认可制度的文字、注册号组成，文字和注册号置于 CNAS 徽标的右方，汉字使用宋体，英文和数字使用 Arial 字体。CNAS 认可标识的基本颜色为蓝色或黑色。组成认可标识的文字和注册号的颜色(色值)应与 CNAS 徽标一致。

机构认可标识式样如下图：

中国认可
管理体系
MANAGEMENT SYSTEM
CNAS CXXXX-M

其中，“MANAGEMENT SYSTEM”代表管理体系基本认可制度，“C”代表认证机构认可，“XXXX”为认证机构认可注册流水号，M 代表管理体系。

a)CNAS 拥有 CNAS 认可标识的所有权，并授权 ZXB 在认可范围和认可有效期内按

照 CNAS-R01《认可标识使用和认可状态声明规则》以及相关要求的规定使用认可标识或声明认可状态。ZXB 应对认可标识的使用进行管理和控制，并不得将认可标识使用在与被认

可的范围无关的其他业务中。CNAS 对 ZXB 的认可标识使用情况进行监督。

b)当管理体系认证机构获准 CNAS 认可时，认证机构应按照 CNAS-CC01:2015 8.3.1 要求，不得允许获得认证的组织将 CNAS 认可标识用于产品或消费者所见的产品包装之上，或以任何其他可解释为表示产品符合性的方式使用。

6.2.2.3 国际认可论坛 IAF-MLA 标识的规定样式及规格：

a)IAF MLA 标识的规格如图，可成比例放大缩小，应清晰可辨。

b)IAF-MLA 标志颜色：

IAF-MLA 标志的基本颜色为蓝色或黑色。

蓝色：C:100 M:80 Y:0 K:0

C:100 M:56 Y:0 K:0

黑色：C:0 M:0 Y:0 K:100

c)只可按照 CNAS-R01《认可标识使用和认可状态声明规则》中列明的式样，将 IAF-MLA 标识与 CNAS 认可标识组合使用，由 IAF-MLA 国际互认标志和 CNAS 认可标识并列组成。式样如下图：

d)ZXB 可将国际互认联合认可标识用于报告、证书、公开出版物、文件、办公用品、宣传品、网页宣传等。可采用印刷和电子图文等方式使用。

e)ZXB 不允许获证客户在产品或产品包装上使用 IAF-MLA/CNAS 标识和(或)IAF-MLA 国际互认标识。

6.3 换证

6.3.1 在认证证书有效期内，有下列情况之一时，获证客户应办理换证手续：

认证要求变更；

获证客户相关信息变更（包括组织名称、地址、认证范围、组织规模、更换

认证机构、统一信用代码等）；

其他。

6.3.2 获证客户应提出书面的换证申请，说明理由并附上有关资料及换证所需的费用。

6.3.3 运营部核准确定是否需要重新审核。

6.3.4 对于需重新审核的申请方，如扩大认证范围，组织机构、过程、资源条件作了较大的更改等，则按有关认证审核的程序执行；不需重新审核的申请方，如证书丢失或破损、更换法人而管理体系未作更改等情况，由运营部换发新证（原证书号不变）。

6.4 暂停

当获证客户符合暂停认证的条件时，由运营部填写《获证组织认证证书和标志处理审批表》，并报总经理批准后，由运营部向该获证客户发出《认证证书和标志暂停使用通知书》，获证客户应停止对外宣传认证资格，停止使用认证证书和标志。

6.5 恢复

6.5.1 被暂停的获证客户按规定期限采取纠正措施，并将纠正措施落实情况和凭证材料报技术部，经技术部评审符合暂停恢复条件的，方可恢复其认证证书和标志使用。

6.5.2 对需要安排现场检查的，经认证人员检查合格后，报技术部审议和总经理批准，运营部发出《认证证书和标志恢复使用通知书》。恢复其认证证书和标志使用。

6.6 撤销

当获证客户符合撤销认证的条件时，运营部应填写《获证组织认证证书和标志处理审批表》报总经理批准后，由运营部向该获证客户发出《认证证书和标志撤销通知书》，撤销其证书注册号，并通过媒介予以公告。运营部收回原发放的认证证书。

6.7 信息公开

对换证、暂停/恢复、撤销认证证书的客户，由运营部按规定定期上报 CNCA//CNAS/ CCAA。当相关方提出查询需求时，ZXB 应向其正确说明获证客户认证证书被暂停、撤销或缩小的有关情况。

6.8 发现标志被误用/滥用时 ZXB 采取的纠正措施

如发现获证客户在认证证书和认证标志的使用及宣传上违反本程序的要求，误用或有意错用，造成误导时，运营部应：

责令其限期采取纠正措施，以消除造成的不良影响；

按 ZXB 公开文件说明中有关暂停、撤销认证的规定暂停或撤销该违规客户的证书；

在 ZXB 网站及相关媒体上公告违规行为；

必要时按相关法律法规追究违规客户的法律责任。

6.9 认证证书和标志的监督检查和处罚

运营部负责对认证证书和认证标志的使用情况实施监督检查，对伪造、冒用、转让和非法买卖 ZXB 认证证书和认证标志等违法、违规行为，向国家认监委或者地方认证监督管理部门报告。

7 记录、表格

ZXB《认证证书和标志暂停使用通知书》

ZXB《认证证书和标志恢复使用通知书》

ZXB《认证证书和标志撤销通知书》

ZXB《获证客户认证证书和标志处理审批表》

1 范围

本规定规定了对多现场（含临时场所）客户实施管理和审核的通用要求。

本规定适用于多现场组织的审核，包括多场所组织和含有临时场所的组织。本规定是对通用审核规范的补充，在本规定中仅对多现场审核的特殊要求作出了规定，需要而在本规定中未作出规定的方面，按通用审核规范执行。

注：本文件并不覆盖如下情况的多场所组织，即一个多场所组织部署了多个管理体系且每个场所应被看作一个单一场所组织并据此实施审核的情况。本文件不应在如下情况使用，即多个独立组织被另外一个独立组织（如：咨询公司或虚构的组织）集合在一个管理体系范围之下的情况。

2 引用文件

下列文件中的条款通过本文件的引用而成为本程序的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本程序。凡是不注日期的引用文件，其最新版本适用于本文件。

2.1 质量管理体系认证规则

2.2 CNAS-CC01:2015 《管理体系认证机构要求》（ISO/IEC17021-1:2015,IDT）

2.3 CNAS-CC02:2013 《产品、过程和服务认证机构要求》（ISO/IEC 17065:2012）

2.4 CNAS-CC11:2018《多场所组织的管理体系审核与认证》

2.5 CNAS-CC105:2020《确定管理体系审核时间》

2.6 CNAS-CC170:2015《信息安全管理体系认证机构要求》

2.7 CNAS-CC175:2017《基于 ISO/IEC 20000-1 的服务管理体系认证机构要求》

2.8 CNAS-SC175:2017《基于 ISO/IEC 20000-1 的服务管理体系认证机构认可方案》

2.9 CNAS-SC125:2020 《职业健康安全管理体系认证机构认可方案》

2.10 CNAS-CC190:2021《能源管理体系认证机构要求》

2.11 《审核人日管理规定》

2.12 《结合审核管理规定》

3 术语和定义

3.1 组织

为实现目标，由职责、权限和相互关系构成自身功能的一个人或一组人。

3.2 多场所组织

1)某单一管理体系覆盖的一个组织，其构成包括经识别的中心职能以及多个场所， 中心职能（并不必须是组织的总部）对某些过程、活动进行策划和控制，在多个场所（常设的、临时的或虚拟的）中这些过程、活动得到全部或部分实施。

2) 一个多场所组织可以包含一个以上的法律实体，但该组织的所有场所应与该组织的中心职能具有法律或合同联系，并服从于单一管理体系。该管理体系应由中心职能制定、建立，并服从于中心职能的持续监督和内部审核。这意味着中心职能有权要求任何场所在必要时采取纠正措施。适用时，中心职能与各场所的正式协议宜对此作出规定。

3）场所可以包括所有土地，在其上的特定地点实现组织所控制的过程、活动，包括任何相关联或附属的仓库，用以储存原材料、副产品、中间产品、最终产品和废料，以及上述过程、活动涉及的任何固定的或活动的设备或设施。另外，如果法律有要求，场所的定义应以国家或地方的相关注册登记制度的定义为准。

4）在无法确定地点时（如：服务提供组织可能会有这种情况），认证的覆盖范围宜考虑组织总部的过程、活动以及服务的交付。适用时，认证机构可以决定仅在组织交付服务的地方进行认证审核。此时，认证机构应识别并审核所有与中心职能有关的接口。

3.3 中心职能

对管理体系负责并对管理体系集中控制的职能。

3.4 常设场所

客户组织持续进行工作或提供服务的场所（有形或虚拟）。

3.5 虚拟场所

虚拟地点指客户组织完成工作或提供服务所用到的，允许处于不同物理地点的人员执行过程的在线环境。

注 1：当某过程必须在某一有形环境实现时不能将其考虑为虚拟场所，如：仓储、 物理检测实验、安装或维修有形产品等。

注 2：这类虚拟场所的一个例子是，一个设计和开发组织的所有员工在远程位置开展工作，在云环境中工作。

注 3：一个虚拟场所（如：一个组织的内部网络）被当作一个独立场所来计算审核时

间。

注 4：更进一步信息见 CNAS-CC14（IAF MD4）《计算机辅助审核技术在获得认可的管理体系认证中的使用》。

3.6 子范围

单个场所的范围

注 1：单个场所的范围可能与多场所组织的全部范围相同，但也有可能是多场所组织范围的一小部分。

注 2：本文件中所说的“子范围”针对认证范围而言，而非针对认可范围。

3.6 最高管理者

在最高层指挥和控制组织的一个人或一组人。

3.7 临时场所

1)客户组织为在有限时期内进行特定工作或提供服务而设立的场所（有形或虚拟），该场所不准备作为常设场所。

2）认证机构应通过抽样对组织管理体系覆盖的临时场所进行审核，以获得管理体系运行和有效性的证据。当认证机构和客户组织协商一致时，多场所认证的范围以及认证文件中也可以包括临时场所。当认证文件中显示临时场所时，应注明该场所是临时的。

4 管理规定

4.1 多现场组织信息的获取

合同提交人员负责识别申请组织是否为多现场组织，向多现场组织介绍多现场认证准则及抽样方法，了解分场所的数量与分布情况、各分场所的人数、体系覆盖范围及各分场所之间的差异等信息，并指导申请组织填写《多场所/临时场所/多名称组织清单》，并作为必备文件资料之一提交合同评审。

4.2 多现场组织的合同评审与合同签订、以及审核方案

1）对多现场组织，认证申请评审人员应注意识别各分场所的差异，如产品/服务/活动范围、场所范围、体系覆盖范围内员工人数等方面的差异，依据本文件“4.5 多现场组织的分场所抽样”要求确定分场所的抽样数量，依据 ZXB《审核人日管理规定》中关于多现场组织审核人日计算规则计算审核人日。具体如下：

认证申请评审人员应获得有关申请组织的必要信息，以：

●确认贯穿组织部署了单一管理体系；

●确定管理体系运行范围及寻求认证的范围，以及适用时的子范围；

●理解每个场所的法律与合同安排；

●理解“在哪里发生了什么”，即：确定每个场所提供的过程、活动，并识别中心职能；

●确定向所有场所提供的过程、活动（如：采购）的集中化程度；

●确定在不同场所之间的接口；

●确定哪些场所适用抽样（即，哪些场所提供非常相似的过程、活动），以及哪些场所不具备抽样资格；

●纳入考虑的其他相关因素（见 CNAS-CC14、CNAS-CC105、CNAS-CC106、GB/T27204）

●确定组织的审核时间；

●确定审核组的能力要求；

●识别管理体系覆盖的过程、活动的复杂程度和规模范围（如：一个或多个）。

2）对多场所组织，认证合同应与其总部签订，且认证合同应覆盖认证范围内的所有场所（即，认证合同应列明认证覆盖的每个分场所，每个分场所均应在合同上盖章）；当分场所需要子证书时，应在认证合同中明确。对临时场所不需在合同中体现，也不得颁发子证书。

3）如果服务提供组织进行拟认证活动的所有现场不能同时接受认证，认证申请评审人员应向该组织进行沟通并明确哪些场所被纳入认证范围，哪些场所将不纳入认证范围。

4）审核方案

除了 CNAS-CC01：2015 第 9.1.3 条的要求外，审核方案还应至少包括或引用下述内容：

●每个场所的过程、活动；

●识别哪些场所可以被抽样、哪些场所不能；

●识别哪些场所被抽样覆盖、哪些场所未被抽样覆盖。

当确定审核方案时，由于被审核组织的特定结构审核方案管理人员应为额外活动给予充分的时间，这些活动的时间不计入审核时间，例如：用于路途、审核组成员之间联系、审核后会议等。

注：假如拟审核过程的属性适用于远程审核（见 CNAS-CC01 及 CNAS-CC14）， 可使用远程审核技术。

在任何时候使用多于一名成员构成审核组时，审核方案管理人员应有责任与审核组长协同识别出对每个场所及每一部分审核所需的技术能力，并为审核的每一部分分派适当的审核组成员。

4.3 多现场组织的审核实施

1）对多现场组织，在安排审核任务和编制审核计划时应考虑往来各场所之间的路途时间。如果派出一个以上的审核组对多场所网络实施审核，那么宜为这些审核组指定唯一的审核组长，他的职责是汇总审核组的发现，并编制综合报告。

2）在编制审核计划前，审核组长应与组织再次确认多现场情况，以及认证范围以及每个场所的子范围；在考虑多个管理体系标准的情况下，对每个场所的管理体系标准；拟审核的过程、活动；每个场所的审核时间；分派审核组等内容的考虑。

3）在编制审核计划时，应按本文件“4.5 多现场组织的分场所抽样”考虑抽样，并对分场所的审核人日安排符合 ZXB《审核人日管理规定》的要求。

4）对多现场组织的现场审核，分场所的抽样应符合本文件“4.5 多现场组织的分场所抽样”要求。

5）现场审核应证实：

a）总部已按标准建立管理体系，满足了标准要求和考虑相关法律法规的要求。

b）组织具有能从所有场所收集和分析数据的能力及实施变更的权力和能力：包括体系文件和体系的变更、管理评审、投诉、纠正措施的评价、内部审核策划和结果评价。

c）组织的管理体系应在集中控制下进行管理，并由总部进行管理评审和执行总部的内审方案，认证前相关场所（包括总部）已实施了内审。

6）考虑到认证标准中的有些条款与具体的分场所无关，只需在总部审核，不必对标准中的所有条款均在所有分场所中审核到，如管理评审和管理体系策划等。

7）审核组应现场确认组织的规模和产品范围、各场所的人员和现场产品覆盖范围，如发现产品/服务/活动范围、场所范围、体系覆盖范围内有效人数等方面与《审核计划》有出入时，应及时向运营部反馈，以便进行处理。

8）在审核报告中应对多场所的情况予以最终确认。

9）当组织管理体系使用电子化文件、电子化过程控制或其他电子化过程时，也适用本要求，但应记录进行多场所审核的适当理由。

10）审核组通过第一阶段审核应完善信息以： 确认审核方案； 策划第二段审核，考虑对每个场所拟审核的过程、活动；确认承担第二阶段审核的审核组具备必要的能力。

第二阶段：初次认证审核的输出中，审核组应将在每个场所审核了哪些过程形成文件。这些信息将用于修正审核方案以及后续监督审核的审核计划。

4.4 不符合的处理

4.4.1 在任何独立场所发现不符合（如 CNAS-CC01 中规定），无论是由内部审核发现或经由 ZXB 的审核发现，应开展调查以确定其他场所是否可能受到影响。因此，ZXB 应要求组织对不符合评审，以确定这些不符合是否指出了适用于其他场所的总体上的系统不足。如果发现确实如此，应同时对中心职能及受到影响的独立场所实施纠正措施并验证。如果发现并非如此，组织应能够向 ZXB 证明其限定后续纠正措施范围的正当理由。

4.4.2 ZXB 应要求提供这些措施的证据并增加其抽样频率和/或抽样数量，直到 ZXB 确信恢复了控制。

4.4.2 在作出决定的过程中，如果任一场所出现严重不符合，在得到满意的纠正措施之前 ZXB 应拒绝对整个多场所组织所列的场所进行认证。

4.4.3 在认证过程中，ZXB 不应允许组织为克服由于某个场所存在不符合造成的问题，而从认证范围中删除存在问题的场所。

4.5 多现场组织的分场所抽样

4.5.1 多场所抽样原则

4.5.1.1 多场所抽样原则（QMS/EMS/OHSMS ISMS/SMS/EnMS）

1） 抽样应遵循相似性原则，即不是所有的分场所都适用于抽样，所有场所的过程应实质上属于同一类，并按照相似的方法和程序运作。当每个场所均运行非常相似的过程、活动时，允许对这组场所抽样。如果其中某些场所实施的过程与其他场所相似，但过程的数量少于其他场所，那么在实施大多数过程或关键过程的场所要接受完整审核的前提下，可以对上述过程数量较少的场所采用多场所认证。

当组织通过位于不同地点但相互关联的过程开展业务时，如果满足本文件的所有其他规定，也可以进行抽样。如果各个地点的过程虽不相似，但明显相互关联，那么抽样计划应至少包括组织实施的每个过程的一个样本（例如，组织在一个地点生产电子元器件，在其他几个地点组装这些电子元器件）。

对于开展不同业务活动或专业性质差异较大的业务活动的分支机构（如土建分公司、市政工程分公司等），宜根据组织的认证范围及其所涉及的不同业务活动和类别，分别对这类分支机构进行抽样审核。非覆盖相同活动的多场所不适于抽样。

虽然一个场所与其他场所有类似的过程或制造类似的产品，但应考虑每个场所的业务活动（技术、设备、使用和存储的危险材料的数量、工作环境、场所等）之间的差异。当

允许抽样时，运营部应确保将被审核的场所样本具有被审核组织现存的过程、活动和环境因素、OHS 风险的代表性。组织的 QMS/EMS/OHSMS 覆盖的临时场所应以抽样方式进行审核，为管理体系运行和有效性提供证据。

2）总部不适用于抽样，即在每次认证审核时都应审核总部。

3）至少 25%的样本应随机选择，其余样本的选择应使在证书有效期内选择场所的差异尽可能大。并且其结果应选到在有代表性的不同场所，确保认证范围内覆盖的所有过程将被审核到。

4）在初次的合同评审时， 最大程度地识别场所之间的差异， 以便确定适宜的抽样水平；在初审、监督和再认证中，应尽量避免在历次审核中重复选择同一样本场所，而有的场所又多次未被审核到。

5）场所选取可以考虑以下方面（但不限于以下方面）：

a) 场所内部审核、管理评审或以前认证审核的结果；
b) 场所是常设的、临时的或虚拟的；
c) 管理体系的成熟度和组织的理解程度；
d) 投诉记录以及纠正和预防措施的其他相关方面；
e) 对于职业健康安全管理体系，考虑活动和过程的性质相关的职业健康安全风险程度；
f) 各场所在规模上的显著差异；
g) 管理体系以及在场所实施过程的复杂程度；
h) 工作程序的差异及运行方式的变化；
i) 在倒班安排和工作程序上的差异；
j) 职能的重复性；
k) 活动的变化或差异；
l) 组织的人员在场所的分布情况；
m) 上次认证审核后的变化；
n) 对于环境管理体系，考虑环境问题和环境因素及其关联影响的程度；
o) 与敏感环境潜在的相互作用；
p) 文化、语言和法律法规方面的差异；
q) 相关方的意见；
r) 地理位置的分散程度；
s) 风险的重要性；
t) 事故率的差别；
u) 能源种类、能源使用与能源消耗的复杂程度；

v) 与关键的信息系统或处理敏感信息的信息系统之间的潜在交互；

w) 发生在特定场所的信息安全事件；

x) 各场所业务目的的差异；场所的风险状况；

y) 不同场所的信息系统的复杂程度；

z) 工作实践的差异；控制的设计与运行的差异；

aa) 与关键的信息系统或处理敏感信息的信息系统之间的潜在交互。

6) 并不是必须在审核过程一开始就完成抽样。也可能在完成对中心职能的审核时完成抽样。不论哪种情况，应将样本中所包括的场所通知中心职能。这可能是在相对较短时间内通知，但应给出充分的时间用于审核准备。

4.5.1.2 对于ISMS多场所抽样，还需满足以下要求：

（1）当客户拥有满足以下a)至c)的多个场所时，ZXB可以考虑使用基于抽样的方法进行多场所认证审核：

a）所有的场所在同一ISMS下运行，并接受统一的管理、内部审核和管理评审；

b）所有的场所都包含在客户的ISMS内部审核方案中；

c）所有的场所都包含在客户的ISMS管理评审方案中。

（2）从客户ISMS范围内的所有场所中选择具有代表性的样本，该选择应基于一个可体现上述4.5.1.1 5）中所列因素的判定，同时也考虑随机因素；

（3）在授予认证之前，运营部安排审核组审核了ISMS中每个具有重大风险的场所；

（4）根据上述要求设计审核方案，且审核方案要在三年内覆盖ISMS认证范围内的代表性样本；

（5）无论是在总部还是在单个场所发现不符合，纠正措施规程的实施适用于包括在认证范围内的总部和所有场所。

（6）审核应关注客户总部为确保一个ISMS运用于所有场所并在运行层面上实施统一管理所进行的活动。审核应关注上述所有事项。

4.5.1.3 对于SMS多场所抽样，还需满足以下要求：

（1）如果客户具有多个地点且所有的地点满足以下条件时，ZXB 可以使用基于抽样的方法来实施多场所认证审核：

a）在同一个实施集中管理的SMS下运行；

b）包含在客户的内部审核方案中；

c）包含在客户的管理评审方案中。

当一个多场所组织在不同的场所或一组场所里运作一些不相似的过程或活动时，运营部需要证明其决定在管理体系认证中实施抽样的理由的合理性，并予以记录。这应证实认证机构对所有场所的管理体系符合性获得了同等程度的信心。 还须关注对“虚拟地点”的审核，如非永久场所、在线场所等等。在这类场所中，抽样可能是适宜的，或不适宜的。

（2）服务点的抽样

通过在服务点观察客户的服务状况、与相关人员（如驻场的服务工程师、客户的顾客等）面谈以及调阅现场服务记录，ZXB审核组可以收集客户SMS运行和有效性的证据。

①服务点抽样条件：当客户拥有满足以下条件的多个服务点时，运营部可以考虑使用基于抽样的方法对服务点进行审核：

a) 所有场所的工作人员均在同一个 SMS 下进行管理，客户对人员具有分配和调配的权力，有权要求场所内提供服务的工作人员提供工作量和工作质量的数据；

b) 客户在所有的场所提供的服务和活动的变动，或场所的成立和撤销不影响客户的 SMS 运行的完整性；

c) 所有的场所都包含在客户的 SMS 内部审核方案和管理评审方案中。

②服务点的抽样方法： 在确定服务点的抽样量时，针对审核时客户所具有的服务点，运营部可先考虑确保样本覆盖认证范围内的业务类别，然后再根据服务点数量适当增加抽样量。

a）初次认证审核、监督审核和再认证审核时，样本覆盖认证范围内所涉及到的CNAS-SC175:2017附录A《SMS认证机构认证业务范围分类》表 A.1 中的中类；

b）初次认证审核和再认证审核时，在满足a）的基础上按照下表增加抽样量：

服务点数量（个）	增加的服务点抽样量（个）
5 ~ 10	1
11~ 20	2
21~ 40	3
41~ 60	4

注：当服务点的数量超过60 时，可沿用上表的规律确定应增加的抽样量。

抽样时，优先选取同种业务类型中业务复杂程度高且服务交付风险大的服务点。对出现审核组无法访问服务点的情形可根据实际情况采取适宜的应对措施。

② 服务点抽样的审核时间：运营部分配给每个服务点的审核时间宜与审核组在该服务点所需完成的审核活动相匹配。通常，每个服务点的审核宜不少于0.25 个

人天。每个服务点的审核时间不含审核员的旅途时间。

4.5.1.4 并非说有满足“多场所组织”定义的组织都具备抽样的资格，并非所有的管理体系标准都适合于多场所认证。例如，当标准要求对差异性的当地因素审核时，对多场所的抽样是不适宜的。如包括航空业（AS 9100 系列）或汽车业（IATF 16949），这些方案的要求应被优先考虑。

ZXB宜从以下方面规定抽样限制，以便在抽样将会影响对管理体系有效性的充分信心时，对抽样加以限制。

（1）范围类别或过程、活动（即，基于对该类别或该活动相关的风险或复杂程度的评估）；

（2）具备多场所审核资格的场所规模；

（3）为处理不同的过程、活动或不同的合同与法规系统，在当地运行管理体系的差异；

（4）在组织管理体系之下运行的临时场所，即便这些临时场所未列入认证文件。

4.5.2 多场所样本的数量（QMS/EMS/OHSMS/ISMS/SMS/EnMS）

下面是一个样本数量计算的实例。假设活动风险水平为低到中，每次审核抽样的场所的最低数量为：（Y：抽取场所数量、X 为场所总数）

1）初审样本量应为场所数量的平方根（$Y=\sqrt{x}$），计算结果向上取整为最接近的整数。

2）监督审核样本量应为场所数量的平方根乘以系数 0.6（$Y=0.6\sqrt{x}$），计算结果向上取整为最接近的整数。

3）再认证样本量应与初审相同，然而，如果证明管理体系在认证周期中是有效的，样本量可减少至场所数量平方根乘以系数 0.8（$Y=0.8\sqrt{x}$），计算结果向上取整为最接近的整数。

4）当对拟认证或获证管理体系涵盖的过程、活动进行风险分析，发现涉及下列因素的特殊情况时，应增加抽样的数量或频率:

a）场所的规模和员工的数量；

b）过程、活动以及管理体系复杂程度和风险水平；

c）工作方式的差异（如：倒班）；

d）所从事过程、活动的差异；

e）投诉记录，以及纠正措施和预防措施的其他相关方面；

f）与跨国经营有关的任何方面；

g）内部审核和管理评审的结果；

h）各场所地域上的分布及地理位置的分散程度

i）分包情况

j）对于环境管理体系，环境因素及其关联影响的重要性和程度。

k）对于职业健康安全管理体系，考虑职业健康安全管理体系中危险源的变化及其关联影响的程度。

l）能源使用与能源消耗，特别是主要能源使用的差异；

m）能源使用的复杂程度；

n）纠正与预防措施的记录；

o）证实能源绩效和能源管理体系改进的能力。

5）在初次认证审核每次再认证审核以及作为监督的一部分在每个日历年至少一次的审核中，都应对中心职能审核。ZXB 应对每个多场所组织每次应用抽样形成记录，该记录应证明 ZXB 是按照本文件进行操作的。

6）如果组织的分支机构分为不同等级（如：总部办公室/中心办公室，全国性办公室，地区办公室，地方分支），上述的初次认证审核抽样模式适用于每个等级的场所。

示例：

1 个总部办公室：每个审核周期（初次审核、监督审核或再认证审核）都访问；

4 个全国性办公室：样本数量＝2，至少 1 个为随机抽样；

27 个地区办公室：样本数量＝6，至少 2 个为随机抽样；

1700 个地方分支：样本数量＝42，至少 11 个为随机抽样。

地区办公室的样本中宜至少覆盖到每个全国办公室控制的地区办公室。地方分支的样本中宜至少覆盖到每个地区办公室控制的地区分支。这样可能导致每个等级的场所抽样数量超过按照第 4.5.2 （1）-（3）条计算的最小抽样数量。

7）抽样过程应作为审核方案管理的一部分。在任何时候（即：在策划监督审核之前、或组织的任何场所变更其结构时、或将在认证边界之内增加新的场所时），ZXB 应预先评审审核方案中的抽样安排，以便在为保持认证对样本审核之前能确定抽样数量调整的需求。

4.5.3 多场所抽样样本量视其风险、难度等因素，对某些专业范围可按如下原则确定，但最高抽样量至场所样本量总数。

1）对于医药、医疗器械（植入人体部分）、锅炉及压力容器、武器弹药等高风险、

高难度专业多场所宜增加抽样数量。

2）对于建筑、监理等高风险、高难度专业多场所宜增加抽样数量。

4.6 对不适用 4.5 条款多场所抽样的多场所组织审核的方法

4.6.1 审核方案的构成应包括对所有场所的初次认证审核和再认证审核。在监督审核中，应在每个日历年覆盖 30%的场所（向上取整至整数）。每次审核都包括中心职能。第二次监督审核选取的场所通常不同于第一次监督审核所选取的场所。

4.6.2 审核方案的设计应确保在认证范围覆盖的所有过程在每个周期内被审核到。

4.6.3 增加场所 如果对已认证的多场所组织增加新场所或增加一组新的场所，认证机构应确定在证书中增加这些新场所前所需实施的必要活动。这应包括考虑是否对新场所审核。 在新场所纳入证书后，需要确定后续监督或再认证审核的抽样数量。

4.6.4 不适用场所抽样可能有多种原因，例如：

●所有场所实施的过程、活动与管理体系的范围有关且存在显著差别；

●客户要求对每个场所审核；

●有专门的方案或法规要求规定了系统性地对每个场所审核。 处于这两种极端情况之间还有很多多场所组织，他们的一部分场所运行相似的过程、活动，而其他场所专注于非常特殊并且不在组织的其他部分运行的过程。与任何 抽样过程一样，恰当的场所抽样仅限于对组织范围内运行非常相似过程、活动的场所。

4.7 对场所构成中部分可抽样部分不可以抽样的多场所组织审核的方法

应按照第 4.5 条对可抽样的场所并按照第 4.6 条对组织中剩余不适用抽样的场所建立审核方案。

4.8 审核时间计算

按照 ZXB《审核人日管理规定》中关于“多场所组织审核人日数”和“临时场所的审核人日数”执行。除非特定认证方案另有规定，单个被抽样场所审核时间的减少量不应超过 50%。 例如，CNAS-CC105 允许审核时间减少量最大为 30%，另外 20%是由于单一管理体系所运行中心职能以及任何可能的集中化过程（如：采购）而考虑允许缩减的最大值。对于较小的服务/施工的临时现场，QMS/EMS/OHSMS/ISMS/SMS 每体系各增加 0.5-1 人日。

4.9 认证文件

4.9.1 认证文件应反映认证范围以及多场所认证所覆盖的场所、法律实体（适用时）。

4.9.2 认证文件应包含所有场所的名称和地址，反映出组织与认证文件相关。范围 或认证文件引用的其他信息应清晰表明经认证的活动由清单中所列场所实施。然而，如果某

一场所的活动仅是包含于组织范围内的一部分，认证文件应包括该场所的子范围。当在认证文件上展示临时场所时，应注明这些场所为临时场所。

4.9.3 如果向一个场所颁发认证文件，其中应包括：

a)管理体系针对被认证的整个组织；

b)该认证所覆盖对特定场所、法律实体的活动；

c)与主证书之间的可追溯性，如：编号/代码；

d)声明：本证书的有效性取决于主证书有效。

在任何情况下，都不得以该场所、该法律实体的名义颁发认证文件，或误导该场所、该法律实体被认证（被认证的是客户组织），也不应包括该场所、该法律实体的过程、活动符合规范文件的声明。

4.9.4 一旦任何场所不能满足保持认证的必要规定，认证文件将被整体撤销。

4.9.5 多场所组织颁发子证书

1）审核组长应对认证证书和证书附件的内容进行确认，包括产品范围、规模。如需对各场所颁发子证书，则应在认证证书的中英文稿中予以明确。

2）应向多场所组织颁发一份带有组织总部名称和地址的认证证书。与认证相关的所有场所的名单发布在认证证书上，或者在认证证书的附录上，或者在认证证书中引用。在认证证书的范围或其它引用中应清楚地注明认证的活动是在名单上的所有场所进行的。如果场所的认证范围只是组织总范围的一部分，在认证证书和任何附录中应清楚地表明其对所有场所的适用性。

3）可向认证所覆盖的每个场所颁发子证书，它包含与主认证证书相同的范围或部分范围，并清楚地引用主认证证书；以及于主证书证书之间的可追溯性，如子证书注册号与主证书的注册号相同，在注册好后加子证书分号：-1；-2；……；子证书的有效性取决于主证书有效的声明，如：子证书有效期与主证书的有效期相同。

4）如果总部或任何场所不能保持认证的必要条件，应撤销所有的认证文件。

5）ZXB 应保持最新的场所名单，为此应要求组织通报任何被关闭的场所，未能提供而仍按原证书范围使用的视为证书误用，ZXB 将按证书使用有关规定进行处理。

6）增加场所可通过监督/再认证活动增加到证书中。当一个/一组新场所需要追加到已认证的多场所组织时，每一个/一组新场所都应独立确定样本量。在以后的监督、再认证中将新增场所加上以前的场所来确定样本量。

4.9.5 含有临时场所的组织

4.9.5.1 对临时场所的审核仅是为了确认需认证的固定场所的管理体系活动，不能为临时场所颁发证书，如果认证范围包含临时场所，认证文件中应注明该场所为临时场所。

4.9.5.2 临时场所抽样（QMS/EMS/OHSMS）

1） 对于初次认证审核通常情况下，初次认证审核活动宜完整覆盖组织拟申请的认证范围。如果组织拟进行认证活动的范围不能同时提供所有现场，应与组织协商并提前告知组织哪些业务活动和场所（分支机构）将不被纳入认证范围。

2）对于监督审核在一个认证周期内的各次监督审核活动宜完整覆盖组织认证范围内的所有业务活动和场所（分支机构）。

3）对再认证审核活动通常也宜完整覆盖组织认证范围内的所有业务活动和场所（分支机构）。

4）临时场所的抽样量

考虑一般风险活动的情况，本文件给出了每次审核至少宜抽取的临时场所数量。

① 初次审核：第一阶段现场审核至少宜抽取一个临时场所，该场所的选择宜基于对相关工程项目的复杂程度及其风险等级来考虑。第二阶段审核抽样量至少为完整覆盖组织管理体系下认证范围内所涉及的全部业务范围；

② 监督审核：难以覆盖认证范围内的全部业务范围时，应在一个认证周期内的各次监督审核活动完整覆盖认证范围内的全部业务范围；

③ 再认证审核：再认证审核抽样量至少为完整覆盖组织管理体系下认证范围内所涉及的全部业务范围；

以下情况可适当考虑增加临时场所的抽样量：

④ 对于具有高复杂程度和一级风险的项目（如核工业、冶金、电力、化工、铁道、水利、石化、海洋石油、航天航空等）；

⑤ 组织在上一年度发生了重大质量、环境、职业健康安全事故的情况。

5）针对结合审核的情况，鉴于质量管理体系、环境管理体系和职业健康安全管理体系所关注的对象及其审核重点的差异性,在确定对临时场所的抽样样本时,宜基于 4.5.2 中 4）条款的原则,并充分考虑不同管理体系的特定要求及其风险情况，以确保对每个管理体系审核的完整性。

5 上述所建议方法的基本原理

5.1 本文件处理单一管理体系下的多场所组织的审核。

5.2 任何一个场所可以实施管理体系范围所覆盖的全部或部分过程、活动，并且不同

的场所可以属于相同的或不同的法律实体。

5.3 关于组织的管理体系涉及单独一个的法律实体或多个法律实体的任何法律考虑，通常与管理体系审核不相关，并且除非另有声明否则不包含于本文件。

5.4 须被审核与认证的是组织的管理体系，而且根据定义管理体系审核只是基于可获得信息的有限样本。然而，必须证实管理体系有能力让所有参与的场所达到预期结果。

5.5 因此，合逻辑的是从组织及其实施的管理体系，以及如果可行哪种抽样方式是适用的开始考虑。

5.6 当多场所组织的每个场所均实施非常相似的过程、活动时，这可能是比较明确的适用场所抽样的情况（如：一系列特许经营店或银行分支机构网络）。另一方面，本文件也包括了不适用场所抽样的情况。不适用场所抽样可能有多种原因，例如：

●所有场所实施的过程、活动与管理体系的范围有关且存在显著差别；

●客户要求对每个场所审核；

●有专门的方案或法规要求规定了系统性地对每个场所审核。

处于这两种极端情况之间还有很多多场所组织，他们的一部分场所运行相似的过程、活动，而其他场所专注于非常特殊并且不在组织的其他部分运行的过程。与任何 抽样过程一样，恰当的场所抽样仅限于对组织范围内运行非常相似过程、活动的场所。

6 多场所组织认证的资格要求

6.1 组织应具有单一管理体系。

6.2 组织应识别其中心职能。中心职能是组织的一部分并且不应被分包给外部的组织。

6.3 中心职能应获得组织的授权以规定、建立并保持该单一管理体系。

6.4 组织的单一管理体系应服从集中的管理评审。

6.5 所有场所应服从组织的内部审核程序。

6.6 中心职能应有责任确保来自于所有场所的数据得到收集和分析，并且应能够证明其权威和能力，以便在需要时（包括但不限于下述情况）发起组织的变更。

(i)体系文件和体系变更；

(ii)管理评审；

(iii)投诉；

(iv)纠正措施的评价；

(v)内部审核的策划和对结果的评价；

(vi)与适用标准有关的法律法规要求。

注：中心职能是实施控制并得到组织最高管理者授权的，是对所有场所产生影响的。并没有要求中心职能仅处于某个单一场所

ISO/IEC 27701
第一版
2019-08

安全技术
针对 ISO/IEC 27001 和 ISO/IEC 27002
在隐私信息管理的扩展
要求和指南

Security techniques - Extension to

ISO/IEC 27001 and ISO/IEC 27002 for

privacy information management - Requirements and guidelines

（ISO/IEC 27701:2019）

目录

前言

ISO（国际标准化组织）和 IEC（国际电工委员会）是为国际标准化制定专门体制的国际组织。国家机构是 ISO 或 IEC 的成员，他们通过各自的组织建立技术委员会通过处理特定领域的技术活动来参与国际标准的制定。ISO 和 IEC 技术委员会在共同感兴趣的领域合作。其他国际组织、政府和非政府等机构，通过联络 ISO 和 IEC 参与这项工作。

ISO/IEC 导则第 1 部分中描述了用于开发本标准的过程以及进一步维护的过程。特别是，应注意不同类型的 ISO 文档依据不同的批准标准。本国际标准遵照 ISO/IEC 导则第 2 部分的规则起草。（参见 www .iso .org / directives）。

本标准中的某些内容有可能涉及一些专利权问题，这一点应该引起注意。ISO 和 IEC 不负责识别任何这样的专利权问题。在标准制定过程中确定的任何专利权的细节将被列在引言中和/或在收到的 ISO 专利声明中（见 www.iso.org/patents）或收到的 IEC 的专利声明清单中（见 http://patents.iec.ch）.

本标准中使用的任何商标名称是为方便用户而提供的信息，并不构成认可。

有关标准的自愿性的解释，与符合性评估相关的 ISO 特定术语和表达的含义，以及 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 www.iso.org/iso/foreword.html.

本标准由联合技术委员会 ISO/IEC JTC1（信息技术）分委员会 SC27（安全技术）起草。

有关本标准的任何反馈或问题，请直接与本国家的标准组织联系。有关这些机构的完整列表，请访问：www.iso.org/members.html.

引言

0.1 总则

几乎每个组织都会处理个人身份信息（PII）。此外，处理的 PII 的数量和种类以及组织需要与其他组织合作处理 PII 的情况均在增加。在处理 PII 的时候，保护隐私是一项社会需求，也是成为全世界立法和/或法规的主题。

信息安全管理体系（ISMS）ISO/IEC 27001 被设计成为容许追加特定领域的要求，而无需开发新的管理体系。ISO 管理体系标准，包括行业特定标准，旨在单独实施或作为综合管理体系实施。

PII 保护的要求和指南取决于组织的背景，特别是所在国的国家有立法和/或法规要求的情况。ISO/ IEC 27001 要求理解并考虑该背景。本标准包括映射到：

-ISO/IEC 29100 中定义的隐私框架和原则;

-ISO/IEC 27018;

-ISO/IEC 29151;和

-欧盟通用数据保护条例。

但是，这些可能需要解释为考虑到当地立法和/或法规。

本标准可供 PII 控制者（包括 PII 联合控制者）和 PII 处理者（包括使用分包的 PII 处理者和作为分包商处理 PII 的处理者）使用。符合本标准要求的组织将生成有关如何处理 PII 的书面证据。这些证据可用于促进与业务伙伴达成的协议，其中 PII 的处理是相互关联的。这也可以帮助与其他利益相关者建立关系。如果需要，可以将本标准与 ISO/IEC 27001 结合使用，对该证据进行独立验证。

本标准最初是作为 ISO/IEC 27552 开发的。

0.2 与其他管理体系标准的兼容性

本标准应用 ISO 开发的框架，以改善与其管理体系之间的一致性。

本标准使组织能够将其 PIMS 与其他管理体系的要求相协调或整合。

安全技术 - 针对 ISO/IEC 27001 和 ISO/IEC 27002 在隐私信息管理的扩展 - 要求和指南

1 范围

本标准规定了要求，并以 ISO/IEC 27001 和 ISO/IEC 27002 扩展的形式为建立，实施，维护和持续改进隐私信息管理体系（PIMS）提供了指南，以便在组织环境内实施隐私管理。

本标准规定了与 PIMS 相关的要求, 并为 PII 控制者和 PII 处理者提供了 PII 处理的责任提供了问责的指导。

本标准适用于所有类型和规模的组织，包括公共和私营公司，政府实体和非营利组织，它们是在 ISMS 中处理 PII 的 PII 控制者和/或 PII 处理者。

2 规范性引用文件

下列文件全部或部分通过引用而成为本标准的条款。凡是注明日期的引用文件，只有指定版本用于本标准。凡是不注明日期的引用文件，其最新版本（包括对其的任何修订）都适用于本标准。

ISO/IEC 27000，信息技术 - 安全技术 - 信息安全管理体系 - 总则和词汇

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

ISO/IEC 27002:2013，信息技术 - 安全技术 - 信息安全控制实用规则

ISO/IEC 29100，信息技术 - 安全技术 - 隐私框架

3 术语，定义和缩写

就本标准而言，ISO/IEC 27000 和 ISO/IEC 29100 中给出的术语和定义同样适用。

ISO/IEC 在以下地址维护用于标准化的术语数据库：

— ISO 在线浏览平台：可从 https://www.iso.org/obp 获得

— IEC Electropedia：可在 http://www.electropedia.org/获得

3.1PII 联合控制者

与一个或多个 PII 控制者共同决定处理 PII 的目的和方法的 PII 控制者。

3.2 隐私信息管理体系 PIMS

藉由处置 PII 的过程而可能影响隐私保护的信息安全管理体系。

4 总则

4.1 本标准的结构

这是与 ISO/IEC 27001:2013 和 ISO/IEC 27002:2013 相关特定领域的文档。

本标准专注于 PIMS 领域的要求。遵守本标准的前提是遵守这些要求以及 ISO/IEC 27001:2013 中的要求。在信息安全的基础上，本标准还扩展了 ISO/IEC 27001:2013 的要求，以考虑到可能受 PII 处理影响的 PII 主体的隐私保护。为了更好地理解，还包括了实施指南以及其他与要求相关的信息。

第 5 章提供了适用于无论作为 PII 控制者或 PII 处理者的组织，在实施 ISO/IEC 27001 的要求时与 PIMS 相关的特定要求以及其他信息。

注 1：为了完整性，第 5 章包含 ISO/IEC 27001:2013 中包含要求的每个条款的子条款，即使在没有 PIMS 特定要求或其他信息的情况下也一并罗列出。

第 6 章提供了适用于无论作为 PII 控制者或 PII 处理者的组织在实施 ISO/IEC 27002 的控制时相关的 PIMS 特定指南以及其他信息。

注 2：为了完整性，第 6 章包含 ISO/IEC 27002:2013 中包含目标或控制的每个条款的子条款，即使在没有 PIMS 特定要求或其他信息的情况下也一并罗列出。

第 7 章 为 PII 控制者提供的 ISO/IEC 27002 补充指南，以及第 8 章为 PII 处理者提供的 ISO/IEC 27002 补充指南。

附录 A 列出了作为 PII 控制者的组织在 PIMS 中特定控制目标和控制（无论是否使用 PII 处理者，以及是否与另一个 PII 控制者联合运作）。

附录 B. 列出了作为 PII 处理者的组织在 PIMS 中特定控制目标和控制（无论是否将 PII 处理分包给单独的 PII 处理者，且包括那些对于 PII 处理者将 PII 处理作为 PII 处理分包商的情况）。

附录 C.包含对于 ISO/IEC 29100 的映射。

附录 D.包含本标准中的控制对于 GDPR 的映射。

附录 E.包含对于 ISO/IEC 27018 和 ISO/IEC 29151 的映射。

附录 F.解释了在处理 PII 时如何将 ISO/IEC 27001 和 ISO/IEC 27002 扩展到隐私保护领域

4.2 ISO/IEC 27001:2013 要求的应用

表 1 给出了本标准中与 ISO/IEC 27001 相关的 PIMS 特定要求的位置。

表 1 - PIMS 特定指南的位置和实施 ISO/IEC 27001:2013 中控制的其他信息

ISO/IEC 27001:2013 中的条款	标题	本标准子条款	备注
4	组织的背景	5.2	其他要求
5	领导	5.3	没有特定于 PIMS 的要求
6	规划	5.4	其他要求
7	支持	5.5	没有特定于 PIMS 的要求
8	运行	5.6	没有特定于 PIMS 的要求
9	绩效评估	5.7	没有特定于 PIMS 的要求
10	改进	5.8	没有特定于 PIMS 的要求

注意：根据 5.1 中的“信息安全”的扩展解释，即使没有特定于 PIMS 的要求，也始终适用。

4.3 ISO/IEC 27002：2013 指南的应用

表 2 给出了本标准中与 ISO/IEC 27002 相关的 PIMS 特定指南的位置。

表 2 - PIMS 特定指南的位置和实施在 ISO/IEC 27002：2013 中控制的其他信息

ISO/IEC27002：2013 条款	标题	文档子条款	备注
5	信息安全策略	6.2	补充指南
6	信息安全组织	6.3	补充指南
7	人力资源安全	6.4	补充指南
8	资产管理	6.5	补充指南
9	访问控制	6.6	补充指南
10	密码	6.7	补充指南
11	物理安全和环境安全	6.8	补充指南
12	运行安全	6.9	补充指南
13	通信安全	6.10	补充指南
14	信息系统获取，开发和维护	6.11	补充指南
15	供应商关系	6.12	补充指南
16	信息安全事件管理	6.13	补充指南
17	业务连续性管理的信息安全方面	6.14	没有特定于 PIMS 的指南
18	符合性	6.15	补充指南

注意根据 6.1 的“信息安全”的扩展解释，即使没有特定于 PIMS 的要求，也始终适用。

4.4 客户

根据组织的角色（见 5.2.1），“客户”可以理解为：

a）与 PII 控制者签订合同的组织（例如 PII 控制者的客户）；

注 1 组织可以作为联合控制者。

注 2 与组织建立企业对消费者关系的个人在本文档中称为“PII 主体”。

b）与 PII 处理者签订合同的 PII 控制者（例如，PII 处理者的客户）;或

c）与 PII 处理的分包商签订合同的 PII 处理者（例如，PII 分包处理者的客户）。

注 3 第 6 章中提到的“客户”，相关条款可适用于 a），b）或 c）的环境中。

注 4 第 7 章和附录 A 中提到的“客户”，相关条款可适用于 a）的环境中。

注 5 第 8 章和附录 B 中提到的“客户”，相关条款可适用于 b）和/或 c）的环境中。

5 与 ISO/IEC 27001 相关的 PIMS 特定要求

5.1 总则

ISO/IEC 27001:2013 中提及的“信息安全”的要求应扩展到经由 PII 过程可能影响的隐私保护。

注意 在实践中，ISO/IEC 27001:2013 中所使用的“信息安全”，相当于“信息安全和隐私”（见附录 F）。

5.2 组织环境

5.2.1 了解组织及其环境

ISO/IEC 27001:2013， 4.1 的附加要求是：

组织应确定其作为 PII 控制者（包括作为 PII 联合控制者）和/或 PII 处理者的角色。

组织应确定与其环境相关，影响其实现 PIMS 预期结果的能力的外部和内部因素。例如，可包括：

— 适用的隐私法律;

— 适用的法规;

— 适用的司法判决;

— 适用的组织环境，治理，政策和规程;

— 适用的行政决定;

— 适用的合同要求。

如果组织在两个角色中都扮演（例如 PII 控制者和 PII 处理者），每个的角色应该被定义，每个角色都应作为一组独立控制的对象。

注：对于 PII 处理的每个实例，组织的角色可能不同，因为角色取决于有谁来决定处理的目的和方式。

5.2.2 理解相关方的需求和期望

ISO/IEC 27001:2013，4.2 的附加要求是：

组织应包括其相关方（参见 ISO/IEC 27001:2013，4.2），包括：与 PII 处理有关的、有利益关系或负有责任的各方，甚至是 PII 主体。

注 1 其他利益相关方可以包括客户（见 4.4），监管机构，其他 PII 控制者，PII 处理者及其分包商。

注 2 与 PII 处理相关的要求可以有法律法规，合同义务和组织自己规定的目标来确定。在 ISO/IEC 29100 中规定的隐私原则提供了有关 PII 处理的指导。

注 3 作为组织符合某一个义务的证明，一些利益相关方可以期望组织符合特定标准，例如本标准中规定的管理体系和/或任何相关的规范。利益相关方可以要求对这些标准进行独立审核。

5.2.3 确定信息安全管理体系的范围

ISO/IEC 27001:2013，4.3 的附加要求是：

在确定 PIMS 的范围时，组织应包括 PII 的处理。

注：根据 5.1 中“信息安全”的扩展解释，确定 PIMS 的范围可能需要修改信息安全管理体系的范围。

5.2.4 信息安全管理体系

ISO/IEC 27001:2013，4.4 的附加要求是：

组织应根据本标准第 5 章中被扩充的 ISO/IEC 27001:2013 第 4 章至第 10 章的要求建立，实施，维护和持续改进 PIMS。

5.3 领导

5.3.1 领导和承诺

适用 ISO/IEC 27001:2013，5.1 中陈述的要求以及本标准 5.1 中规定的解释。

5.3.2 方针

适用 ISO/IEC 27001:2013，5.2 中陈述的要求以及本标准 5.2 中规定的解释。

5.3.3 组织角色，职责和权限

适用 ISO/IEC 27001:2013，5.3 中陈述的要求以及本标准 5.3 中规定的解释。

5.4 规划

5.4.1 应对风险和机遇的措施

5.4.1.1 总则

适用 ISO/IEC 27001:2013, 6.1.1 中陈述的要求以及本标准 5.1 中规定的解释。

5.4.1.2 信息安全风险评估

适用 ISO/IEC 27001:013,6.1.2 中陈述的要求以及下列改进内容：

ISO/IEC 27001:2013,6.1.2 c）1）改进如下：

组织应在 PIMS 范围内应用信息安全风险评估流程来识别与保密性，完整性和可用性丧失相关的风险。

组织应在 PIMS 范围内应用隐私风险评估流程来识别与 PII 处理相关的风险。

组织应在整个风险评估过程中确保信息安全与 PII 保护之间的关系得到适当管理。

注 组织可以应用整合的信息安全和隐私风险评估流程，也可以应用两个单独的流程来评估信息安全和 PII 处理相关的风险。

ISO/IEC 27001:2013，6.1.2 d）1）改进如下：

如果上述 ISO/IEC 27001:2013,6.1.2 d）中识别的风险实现的话，组织应评估其对组织和 PII 主体的潜在后果。

5.4.1.3 信息安全风险处理

适用 ISO/IEC 27001:2013, 6.1.3 中规定的要求以及以下增补内容：

ISO/IEC 27001:2013，6.1.3 c）改进如下：

ISO/IEC 27001:2013 6.1.3 b）中确定的控制应与附录 A 和/或附录 B，以及 ISO/IEC 27001:2013 的附录 A 进行比较，以确认没有遗漏任何必要的控制。

在评估 ISO/IEC 27001:2013 附录 A 中控制目标和控制对风险处理的适用性时，应在信息安全风险以及处理 PII 的风险包括 PII 主体的风险的背景下考虑控制目标和控制。

ISO/IEC 27001:2013，6.1.3 d）改进如下：

制定适用性声明，其中包含：

— 必要的控制[见 ISO/IEC 27001:2013,6.1.3 b）和 c）];

— 包含它们的理由;

— 是否实施了必要的控制措施;以及

— 根据组织的角色（见 5.2.1），要明确排除任何附录 A 和/或 附录 B 以及 ISO/IEC 27001:2013 附录 A 中的控制的理由。

并非附录中列出的所有控制目标和控制措施都需要包含在 PIMS 实施中。排除的理由可能是根据风险评估而确定的不需要控制的地方，以及法律和/或法规（包括适用于 PII 主体的法律和/或法规）不要求（或不被期待）的地方。

5.4.2 信息安全目标和实现规划

适用 ISO/IEC 27001:2013,6.2 中陈述的要求以及本标准 5.1 中的解释。

5.5 支持

5.5.1 资源

适用 ISO/IEC 27001:2013,7.1 中陈述的要求以及本标准 5.1 中的解释。

5.5.2 能力

适用 ISO/IEC 27001:2013,7.2 中陈述的要求以及本标准 5.1 中的解释。

5.5.3 意识

适用 ISO/IEC 27001:2013,7.3 中陈述的要求以及本标准 5.1 中的解释。

5.5.4 沟通

适用 ISO/IEC 27001:2013,7.4 中陈述的要求以及本标准 5.1 中的解释。

5.5.5 文件记录信息

5.5.5.1 总则

适用 ISO/IEC 27001:2013,7.5 中陈述的要求以及本标准 5.1 中的解释。

5.5.5.2 创建和更新

适用 ISO/IEC 27001:2013,7.5.2 中陈述的要求以及本标准 5.1 中的解释。

5.5.5.3 控制记录的信息

适用 ISO/IEC 27001:2013,7.5.3 中陈述的要求以及本标准 5.1 中的解释。

5.6 运行

5.6.1 运行的规划和控制

适用 ISO/IEC 27001:2013,8.1 中陈述的要求以及本标准 5.1 中的解释。

5.6.2 信息安全风险评估

适用 ISO/IEC 27001:2013,8.2 中陈述的要求以及本标准 5.1 中的解释。

5.6.3 信息安全风险处置

适用 ISO/IEC 27001:2013,8.3 中陈述的要求以及本标准 5.1 中的解释。

5.7 绩效评价

5.7.1 监测，测量，分析和评价

适用 ISO/IEC 27001:2013,9.1 中陈述的要求以及本标准 5.1 中的解释。

5.7.2 内部审核

适用 ISO/IEC 27001:2013,9.2 中陈述的要求以及本标准 5.1 中的解释。

5.7.3 管理评审

适用 ISO/IEC 27001:2013,9.3 中陈述的要求以及本标准 5.1 中的解释。

5.8 改进

5.8.1 不符合和纠正措施

适用 ISO/IEC 27001:2013,10.1 中陈述的要求以及本标准 5.1 中的解释。

5.8.2 持续改进

适用 ISO/IEC 27001:2013,10.2 中陈述的要求以及本标准 5.1 中的解释。

6 与 ISO/IEC 27002 相关的 PIMS 特定指南

6.1 总则

ISO/IEC 27002:2013 中提及“信息安全”的指南应扩展到可能受 PII 处理潜在影响的隐私保护。

注 1 在实际使用中，在 ISO/IEC 27002:2013 中使用的“信息安全”的地方，等同于“信息安全和隐私”（见附录 F）。

所有控制目标和控制都应考虑到信息安全风险以及与 PII 处理相关的隐私风险。

注 2 除非在第 6 章中具体规定，或由组织根据适用的司法管辖区决定，相同的指南适用于 PII 控制者和 PII 处理者。

6.2 信息安全策略

6.2.1 信息安全管理指导

6.2.1.1 信息安全策略

适用 ISO/IEC 27002:2013,5.1.1 中规定的控制，实施指南，其他信息以及以下补充指南：

针对 ISO/IEC 27002:2013 5.1.1 信息安全策略的补充指南是：

无论是制定单独的隐私策略，还是通过增加信息安全策略，组织都应该制定一份声明，说明是否支持并致力于遵守适用的 PII 保护法律和/或法规以及商定的合同条款（商定范围包括组织之间及其合作伙伴，分包商及其合作伙伴适用的第三方如客户，供应商等，且应明确分配它们之间的责任）。

针对 ISO/IEC 27002:2013 5.1.1 信息安全策略补充的其他信息是：

处理 PII 的任何组织，无论是 PII 控制者还是 PII 处理者，都应在制定和维护信息安全策略期间考虑适用的 PII 保护的法律和/或法规。

6.2.1.2 信息安全策略的评审

适用 ISO/IEC 27002:2013,5.1.2 中规定的控制，实施指南和其他信息。

6.3 信息安全组织

6.3.1 内部组织

6.3.1.1 信息安全角色和职责

适用 ISO/IEC 27002:2013,6.1.1 中规定的控制, 实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013 ， 6.1.1 信息安全角色和职责的补充实施指南是：

在处理 PII 方面组织宜指定一个联络点，供客户使用。当组织是 PII 控制者时，组织在处理 PII 方面给 PII 主体指定联络点（参见 7.3.2）。

组织宜指定一名或多名负责制定，实施，维护和监督组织范围的治理和隐私流程(program)的人员，以确保遵守有关处理 PII 的所有适用法律和法规。

在适当时，负责人宜：

— 独立并直接向组织的适当管理层报告，以确保有效管理隐私风险;

— 参与管理与处理 PII 有关的所有问题;

— 是数据保护法律，监管和实践方面的专家;

— 作为监管机构的联络点;

— 告知高层管理层和组织内员工在处理 PII 方面的义务;

— 就组织进行的隐私影响评估提供建议。

注：某些司法管辖区会定义何时需要这样的职位，以及他们的职位和角色，这样的人被称为数据保护官。该职位可由内部工作人员或外包人员履行。

6.3.1.2 职责分离

适用 ISO/IEC 27002:2013,6.1.2 中规定的控制，实施指南和其他信息。

6.3.1.3 与职能机构的联系

适用 ISO/IEC 27002:2013,6.1.3 中规定的控制，实施指南和其他信息。

6.3.1.4 与特殊利益集团联系

适用 ISO/IEC 27002:2013,6.1.4 中规定的控制，实施指南和其他信息。

6.3.1.5 项目管理中的信息安全

适用 ISO/IEC 27002:2013,6.1.5 中规定的控制，实施指南和其他信息。

6.3.2 移动设备和远程工作

6.3.2.1 移动设备策略

适用 ISO/IEC 27002:2013,6.2.1 中规定的控制, 实施指南和其他信息以及以下补充指南。

ISO/IEC 27002:2013,6.2.1 的移动设备策略的补充实施指南是:

组织宜确保移动设备的使用不会导致 PII 的危害。

6.3.2.2 远程办公

适用 ISO/IEC 27002:2013,6.2.2 中规定的控制，实施指南和其他信息。

6.4 人力资源安全

6.4.1 任用前

6.4.1.1 审查

适用 ISO/IEC 27002:2013,7.1.1 中规定的控制，实施指南和其他信息适。

6.4.1.2 任用条款和条件

适用 ISO/IEC 27002:2013,7.1.2 中规定的控制，实施指南和其他信息适。

6.4.2 任用中

6.4.2.1 管理责任

适用 ISO/IEC 27002:2013,7.2.1 中规定的控制，实施指南和其他信息适。

6.4.2.2 信息安全意识，教育和培训

适宜采取措施，包括对事故报告的认识，以确保相关工作人员了解对组织可能造成的后果（例如法律后果，业务损失和品牌或声誉受损），对工作人员的后果（例如纪律处分的后果）以及对违反隐私或安全规则和流程（尤其是那些涉及 PII 处理的规则和流程）的 PII 主体的后果（例如物理，物质和情感的后果）。

注 这些措施可包括对有权访问 PII 的人员进行适当的定期培训。

6.4.2.3 违规处理过程

适用 ISO/IEC 27002:2013,7.2.3 中规定的控制，实施指南和其他信息。

6.4.3 任用终止和变更

6.4.3.1 任用终止或变更的责任

适用 ISO/IEC 27002:2013,7.3.1 中规定的控制，实施指南和其他信息。

6.5 资产管理

6.5.1 资产责任

6.5.1.1 资产清单

适用 ISO/IEC 27002:2013,8.1.1 中规定的控制，实施指南和其他信息。

6.5.1.2 资产的所属关系

适用 ISO/IEC 27002:2013,8.1.2 中规定的控制，实施指南和其他信息。

6.5.1.3 资产的可接受使用

适用 ISO/IEC 27002:2013,8.1.3 中规定的控制，实施指南和其他信息。

6.5.1.4 资产归还

适用 ISO/IEC 27002:2013,8.1.4 中规定的控制，实施指南和其他信息。

6.5.2 信息分类

6.5.2.1 信息分类

适用 ISO/IEC 27002:2013,8.2.1 中规定的控制，实施指南和其他信息以及以下补充指南
ISO/IEC 27002:2013，8.2.1，信息分类的补充实施指南是：

组织的信息分类系统宜明确将 PII 视为其实施方案的一部分。在整个分类系统中考虑 PII 对于理解组织什么处理 PII（例如种类，特殊类别），以及存储此类 PII 的位置以及它可以在哪些系统内流通是不可或缺的。

6.5.2.2 信息标记

适用 ISO/IEC 27002:2013,8.2.2 中规定的控制，实施指南和其他信息以及以下附加补充指南。

ISO/IEC 27002:2013,8.2.2，信息的标记的补充实施指南是：

组织宜确保其控制下的人员了解 PII 的定义以及如何识别 PII 信息。

6.5.2.3 资产的处理

适用 ISO/IEC 27002:2013,8.2.3 中规定的控制，实施指南和其他信息。

6.5.3 介质处理

6.5.3.1 可移动介质的管理

适用 ISO/IEC 27002:2013,8.3.1 中规定的控制，实施指南和其他信息以及以下补充指南

ISO/IEC 27002:2013,8.3.1 移动介质的管理的补充实施指南是：

组织应记录用于存储 PII 的移动介质和/或设备的任何使用情况。在可行的情况下，组织宜在存储 PII 时，对可移动物理介质和/或设备使用加密方法。未加密的介质仅宜在不可避免的情况下使用，并且在使用未加密的介质和/或设备的情况，组织宜实施相应规程或补偿控制（例如防篡改包装）以降低 PII 的风险。

ISO/IEC 27002:2013,8.3.1，移动介质管理的其他信息是：

被带出组织的物理范围之外的移动介质容易丢失，损坏，被不当访问。加密移动介质可为 PII 增加一定程度的保护，从而降低移动介质在安全性和隐私方面受到侵害的风险。

6.5.3.2 介质的处置

适用 ISO/IEC 27002:2013,8.3.2 中规定的控制，实施指南和其他信息以及以下补充指南。

ISO/IEC 27002:2013,8.3.2，介质的处置的补充实施指南是：

在处置存储 PII 的移动介质的情况下，安全处理规程应包括在存档文件中，并实施以确保先前存储的 PII 信息不能被访问。

6.5.3.3 物理介质的转移

适用 ISO/IEC 27002:2013,8.3.3 中规定的控制，实施指南和其他信息以及以下补充指南。

ISO/IEC 27002:2013，8.3.3 物理介质的转移的补充实施指南是：

如果使用物理介质进行信息传输，则宜建立一个系统来记录包含 PII 的传入和传出物理介质的信息，包括物理介质的类型，授权的发件人/收件人，日期和时间以及物理介质的数量。在可能的情况下，宜实施其他措施（如加密），以确保数据只能在目的地而非传输途中被访问。

组织宜在物理介质离开所在场所之前对包含 PII 的物理介质实施授权的规程，并确保除授权人员之外的任何人都无法访问 PII。

注 确保离开组织场所的物理介质上的 PII 安全的一种可能的措施是加密 PII 使其不可访问，并且将解密的能力限定在被授权人员身上。

6.6 访问控制

6.6.1 访问控制的业务要求

6.6.1.1 访问控制策略

适用 ISO/IEC 27002:2013,9.1.1 中规定的控制，实施指南和其他信息。

6.6.1.2 网络和网络服务的访问

适用 ISO/IEC 27002:2013,9.1.2 中规定的控制，实施指南和其他信息。

6.6.2 用户访问管理

6.6.2.1 用户注册和注销

适用 ISO/IEC 27002:2013,9.2.1 中规定的控制,实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013,9.2.1，用户注册和注销的补充实施指南是：

管理或操作处理PII的系统和服务的用户的注册和注销流程宜解决用户对其的访问控制受到危害的情况，例如密码或其他用户注册数据的损坏或危害（例如，无意泄露的情况）。

对于处理 PII 的系统和服务，组织不宜向用户重新发布任何已失效或已过期的用户 ID。

在组织将 PII 处理作为服务提供的情况下，客户可以负责一些或所有方面的用户 ID 管理。此类情况宜包括在文件化信息中。

某些司法管辖区对与处理PII的系统相关的未使用的身份验证凭据的检查频率提出了特定要求。在这些司法管辖区运营的组织应考虑到这些要求。

6.6.2.2 用户访问供给

适用 ISO/IEC 27002:2013,9.2.2 中规定的控制,实施指南和其他信息以及以下补充指南。

ISO/IEC 27002:2013 的 9.2.2，用户访问配置的补充实施指南是：

组织宜保持为已授权访问信息系统（其中包含 PII）创建的用户信息的记录准确，且保持最新。该记录包括关于该用户的一系列数据，包括用户 ID，以及用于实现提供授权访问的所识别的技术控制。

通过设置用户访问的唯一 ID，实施适当配置以使得系统能够识别访问 PII 的用户、以及用户所做的添加、删除或更改。这样的配置在保护了组织的同时也保护了用户，系统可以识别用户已处理、未处理的内容。

在组织将 PII 处理作为服务提供的情况下，客户可以承担访问管理的部分或全部职责。在适当的情况下，组织宜向客户提供执行访问管理的方法，例如通过提供管理权限来管理或终止访问。此类情况宜包括在文件化信息中。

6.6.2.3 特定访问权管理

适用 ISO/IEC 27002:2013,9.3.3 中规定的控制，实施指南和其他信息。

6.6.2.4 用户的秘密鉴别信息管理

适用 ISO/IEC 27002:2013,9.2.4 中规定的控制，实施指南和其他信息。

6.6.2.5 用户访问权的评审

适用 ISO/IEC 27002:2013,9.2.5 中规定的控制，实施指南和其他信息。

6.6.2.6 访问权的移除或调整

适用 ISO/IEC 27002:2013,9.2.6 中规定的控制，实施指南和其他信息。

6.6.3 用户责任

6.6.3.1 秘密鉴别信息的使用

适用 ISO/IEC 27002:2013,9.3.1 中规定的控制，实施指南和其他信息。

6.6.4 系统和应用程序访问控制

6.6.4.1 信息访问限制

适用 ISO/IEC 27002:2013,9.4.1 中规定的控制，实施指南和其他信息。

6.6.4.2 安全登录规程

适用 ISO/IEC 27002:2013,9.4.2 中规定的控制, 实施指南和其他信息以及以下补充指南。

ISO/IEC 27002:2013,9.4.2，安全登录规程的补充实施指南是:

如果客户要求，组织宜具备为客户控制下的任何帐户提供安全登录规程的能力。

6.6.4.3 口令管理体系

适用 ISO/IEC 27002:2013,9.4.3 中规定的控制，实施指南和其他信息。

6.6.4.4 特权实用程序的使用

适用 ISO/IEC 27002:2013,9.4.4 中规定的控制，实施指南和其他信息。

6.6.4.5 程序源代码的访问控制

适用 ISO/IEC 27002:2013,9.4.5 中规定的控制，实施指南和其他信息。

6.7 密码

6.7.1 密码控制

6.7.1.1 密码控制的使用策略

适用 ISO/IEC 27002:2013,10.1.1 中规定的控制，实施指南和其他信息以及以下补充指南。

ISO/IEC 27002:2013,10.1.1，密码控制的使用策略的补充实施指南是：

某些司法管辖区可能要求使用加密技术来保护特定类型的 PII，例如健康数据，居民登记号码，护照号码和驾驶执照号码。

组织宜向客户提供有关其使用什么样的加密技术来保护其处理的 PII 的信息。组织还宜向客户提供相应的功能信息，以帮助客户应用自己的加密技术保护自身的 PII 信息。

6.7.1.2 密钥管理

适用 ISO/IEC 27002:2013,10.1.2 中规定的控制，实施指南和其他信息。

6.8 物理和环境安全

6.8.1 安全区域

6.8.1.1 物理安全边界

适用 ISO/IEC 27002:2013,11.1.1 中规定的控制，实施指南和其他信息。

6.8.1.2 物理入口控制

适用 ISO/IEC 27002:2013,11.1.2 中规定的控制，实施指南和其他信息。

6.8.1.3 办公室，房间和设施的安全保护

适用 ISO/IEC 27002:2013,11.1.3 中规定的控制，实施指南和其他信息。

6.8.1.4 外部和环境威胁的安全防护

适用 ISO/IEC 27002:2013,11.1.4 中规定的控制，实施指南和其他信息。

6.8.1.5 在安全区域工作

适用 ISO/IEC 27002:2013,11.1.5 中规定的控制，实施指南和其他信息。

6.8.1.6 交接区

适用 ISO/IEC 27002:2013,11.1.6 中规定的控制，实施指南和其他信息。

6.8.2 设备

6.8.2.1 设备安置和保护

适用 ISO/IEC 27002:2013,11.2.1 中规定的控制，实施指南和其他信息。

6.8.2.2 支持性设施

适用 ISO/IEC 27002:2013,11.2.2 中规定的控制，实施指南和其他信息。

6.8.2.3 布缆安全

适用 ISO/IEC 27002:2013,11.2.3 中规定的控制，实施指南和其他信息。

6.8.2.4 设备维护

适用 ISO/IEC 27002:2013,11.2.4 中规定的控制，实施指南和其他信息。

6.8.2.5 资产的移动

适用 ISO/IEC 27002:2013,11.2.5 中规定的控制，实施指南和其他信息。

6.8.2.6 组织场所外的设备与资产安全

适用 ISO/IEC 27002:2013,11.2.6 中规定的控制，实施指南和其他信息。

6.8.2.7 设备的安全处置或再利用

适用 ISO/IEC 27002:2013,11.2.7 中规定的控制，实施指南和其他信息以及以下补充指南。

ISO/IEC 27002:2013 的 11.2.7，设备的安全处置或再利用的补充实施指南是：

组织宜确保每次重新分配存储空间时，以前驻留在该存储空间中的任何 PII 都不可访问。

在删除信息系统中保留的 PII 时，受设备性能因素制约，彻底删除该 PII 是可能是不切实际的。这会产生另一个用户可以访问 PII 的风险。宜通过具体的技术措施避免这种风险。

为了安全处置或再利用，可能包含 PII 的存储介质的设备宜被视为包含 PII。

6.8.2.8 无人值守的用户设备

适用 ISO/IEC 27002:2013,11.2.8 中规定的控制，实施指南和其他信息。

6.8.2.9 清理桌面和屏幕策略

适用 ISO/IEC 27002:2013,11.2.9 中规定的控制，实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013 的 11.2.9，清理桌面和屏幕策略的补充实施指南是：

组织宜将包含 PII 的硬拷贝材料的创建数量，限定在满足已知处理目的最低值。

6.9 运行安全

6.9.1 运行规程和责任

6.9.1.1 文件化的操作规程

适用 ISO/IEC 27002:2013,12.1.1 中规定的控制，实施指南和其他信息。

6.9.1.2 变更管理

适用 ISO/IEC 27002:2013,12.1.2 中规定的控制，实施指南和其他信息。

6.9.1.3 容量管理

适用 ISO/IEC 27002:2013,12.1.3 中规定的控制，实施指南和其他信息。

6.9.1.4 开发，测试和运行环境的分离

适用 ISO/IEC 27002:2013,12.1.4 中规定的控制，实施指南和其他信息。

6.9.2 恶意软件防范

6.9.2.1 恶意软件的控制

适用 ISO/IEC 27002:2013,12.2.1 中规定的控制，实施指南和其他信息。

6.9.3 备份

6.9.3.1 信息备份

适用 ISO/IEC 27002:2013,12.3.1 中规定的控制，实施指南和其他信息以及以下补充指南。

ISO/IEC 27002:2013,12.3.1，信息备份的补充实施指南是：

组织宜制定策略，以满足 PII 的备份，恢复和恢复要求（可以是整体信息备份策略的一部分），进而满足删除备份数据中包含的 PII 信息的要求（例如合同和/或法律要求）。

在这方面，PII 的具体职责可能取决于客户。组织宜确保已通知客户有关备份的服务限制。

如果组织明确向客户提供备份和还原服务，组织宜向他们提供有关其备份和恢复 PII 功能的明确信息。

某些司法管辖区对 PII 的备份频率，备份的审查频率，测试和恢复频率或者相应的恢复规程提出了具体要求。在这些司法管辖区运营的组织宜证明符合这些要求。

可能存在需要恢复 PII 的情况，可能是由于系统故障，攻击或灾难。当 PII 恢复时（通常来自备份介质），需要建立确保 PII 恢复到可以确保 PII 完整性的状态，和/或识别 PII 不准确和/或不完整的状态以及解决这些问题的流程（可能涉及 PII 主体）。

组织宜有 PII 恢复工作的流程和日志。至少，PII 恢复的日志宜包含：

— 负责恢复的人的姓名;

— 已恢复的 PII 的说明。

一些司法管辖区规定了 PII 恢复工作日志的内容。组织宜能够记录恢复日志的适当内容以符合辖区特定要求。此类审议的结论宜包括在文档化信息中。

在本标准中记述的关于分包商处理 PII 信息的控制（请参阅 6.5.3.3, 6.12.1.2）中，规定了使用分包商来存储 PII 处理的复制或备份的要求。本标准中的控制（6.10.2.1）也包含了与备份和恢复相关的物理介质传输的情况。

6.9.4 日志和监视

6.9.4.1 事态日志

适用 ISO/IEC 27002:2013,12.4.1 中规定的控制，实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013,12.4.1 事态日志的补充实施指南是：

宜建立一个流程并使用连续的，手动或自动化的监控和警报流程来审查事件日志。手动审查宜以明确的、文档化规定的周期实施，以识别违规行为并提出补救措施。

在可能的情况下，事件日志应记录对 PII 的访问，包括由谁，何时，访问哪个 PII 主体的 PII，以及由于事件而进行的任何更改（添加，修改或删除）。

如果多个服务提供者参与提供服务，则在实施本指南时可能会有不同或共享角色。宜明确定义这些角色并将其包含在文档化信息中，并宜就供应者实施的任何日志访问达成协议。

PII 处理者的实施指南：

组织宜定义关于客户是否，何时以及如何确保日志信息可用的标准。这些标准宜提供给客户。

如果组织允许其客户访问组织控制的日志记录，组织宜实施适当的控制以确保客户只能访问与该客户的活动相关的记录，不能访问与其他客户的活动相关的任何日志记录，并且不能以任何方式修改日志。

6.9.4.2 日志信息的保护

适用 ISO/IEC 27002:2013,12.4.2 中规定的控制，实施指南和其他信息以及以下补充指南:

ISO/IEC 27002:2013，12.4.2，日志信息的保护的补充实施指南是:

记录的日志信息例如安全，监视和操作诊断可以包含 PII。宜采取措施如控制访问（参见 ISO/IEC 27002:2013, 9.2.3），以确保记录的信息仅按预期使用。

宜建立一个规程，最好是自动规程，以确保按照保留计划删除或去标志记录信息（参见 7.4.7）。

6.9.4.3 管理员和操作员日志

适用 ISO/IEC 27002:2013,12.4.3 中规定的控制，实施指南和其他信息。

6.9.4.4 时钟同步

适用 ISO/IEC 27002:2013,12.4.4 中规定的控制，实施指南和其他信息。

6.9.5 运行软件的控制

6.9.5.1 在运行系统上安装软件

适用 ISO/IEC 27002:2013,12.5.1 中规定的控制，实施指南和其他信息。

6.9.6 技术脆弱性管理

6.9.6.1 技术脆弱性的管理

适用 ISO/IEC 27002:2013,12.6.1 中规定的控制，实施指南和其他信息。

6.9.6.2 软件安装限制

适用 ISO/IEC 27002:2013,12.6.2 中规定的控制，实施指南和其他信息。

6.9.7 信息系统审计的考虑

6.9.7.1 信息系统审计控制

适用 ISO/IEC 27002:2013,12.7.1 中规定的控制，实施指南和其他信息。

6.10 通信安全

6.10.1 网络安全管理

6.10.1.1 网络控制

适用 ISO/IEC 27002:2013,13.1.1 中规定的控制，实施指南和其他信息。

6.10.1.2 网络服务的安全

适用 ISO/IEC 27002:2013,13.1.2 中规定的控制，实施指南和其他信息。

6.10.1.3 网络隔离

适用 ISO/IEC 27002:2013,13.1.3 中规定的控制，实施指南和其他信息。

6.10.2 信息传输

6.10.2.1 信息传输策略和规程

适用 ISO/IEC 27002:2013,13.2.1 中规定的控制，实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013 的 13.2.1，信息传输策略和规程的补充实施指南是：

组织宜考虑确保在适用的情况下，在系统内外强制执行与 PII 处理相关的规则程。

6.10.2.2 信息传输协议

适用 ISO/IEC 27002:2013,13.2.2 中规定的控制，实施指南和其他信息。

6.10.2.3 电子消息发送

适用 ISO/IEC 27002:2013,13.2.3 中规定的控制，实施指南和其他信息。

6.10.2.4 保密或不泄漏协议

适用 ISO/IEC 27002:2013,13.2.4 中规定的控制，实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013,13.2.4，保密或不泄漏协议的补充实施指南是：

组织宜确保在其控制下，访问 PII 的操作的个人承担保密义务。无论是合同的一部分还是单独的保密协议，都应规定履行义务的时效。

当组织是 PII 处理者时，组织、员工及其代理之间的任何形式的保密协议宜确保员工遵守有关数据处理和保护的策略、规程。

6.11 系统获取，开发和维护

6.11.1 信息系统的安全要求

6.11.1.1 信息安全要求分析和说明

适用 ISO/IEC 27002:2013,14.1.1 中规定的控制，实施指南和其他信息。

6.11.1.2 公共网络上的应用服务的安全保护

适用 ISO/IEC 27002:2013,14.1.2 中规定的控制，实施指南和其他信息及以下补充指南：

ISO/IEC 27002:2013,14.1.2,公共网络上的应用服务的安全保护的补充实施指南是：

组织宜确保在不受信任的数据传输网络上传输的 PII 被加密后方可进行传输。

不受信任的网络包括：公共互联网和组织运营控制之外的其他设施。

注意 在某些情况下（例如，电子邮件的交换），不可信数据传输网络系统的固有特性可能要求暴露一些报头或流量数据，方可进行有效传输。

6.11.1.3 应用服务事务的保护

适用 ISO/IEC 27002:2013,14.1.3 中规定的控制，实施指南和其他信息。

6.11.2 开发和支持过程中的安全

6.11.2.1 安全的开发策略

适用 ISO/IEC 27002:2013,14.2.1 中规定的控制，实施指南和其他信息以及以下补充指南。

ISO/IEC 27002:2013,14.2.1 安全的开发策略的补充指南是：

基于对 PII 原则和/或任何适用法律和/或法规的义务以及组织执行的处理类型，系统开发以及设计的策略宜包含组织对处理 PII 需求的指南，第 7 章和第 8 章提供处理 PII 的控制考虑因素可用于制定系统设计中的隐私策略。

对隐私有贡献的设计的策略和默认的策略宜考虑以下几个方面：

a） 关于 PII 保护的指南以及软件开发生命周期中隐私原则的实施（参见 ISO/IEC 29100）；

b） 设计阶段的隐私和 PII 的保护要求，可以从隐私风险评估和/或隐私影响评估得到输出（参见 7.2.5）；

c） 项目里程碑内的 PII 保护检查点；

d） 必要的隐私和 PII 保护知识；

e） 默认情况下，最小化 PII 的处理。

6.11.2.2 系统变更控制规程

适用 ISO/IEC 27002:2013,14.2.2 中规定的控制，实施指南和其他信息。

6.11.2.3 运行平台变更后对应用的技术评审

适用 ISO/IEC 27002:2013,14.2.3 中规定的控制，实施指南和其他信息。

6.11.2.4 软件包变更的限制

适用 ISO/IEC 27002:2013,14.2.4 中规定的控制，实施指南和其他信息。

6.11.2.5 系统安全工程原则

适用 ISO/IEC 27002:2013,14.2.5 中规定的控制，实施指南和其他信息以及以下附加补充指南：

ISO/IEC 27002:2013,14.2.5，安全系统工程原则的补充实施指南是：

与 PII 处理相关的系统和/或组件宜按照设计的隐私原则和默认的隐私原则来设计，并预测和促进相关控制的实施（如第 7 章和第 8 章 ，分别对于 PII 控制者和 PII 处理者的描述），特别是在这些系统中 PII 的收集和处理仅限于所识别到的必须的 PII 处理目的（见 7.2）。

例如，在相关管辖区内，组织宜确保在指定期限内处置 PII，处理该 PII 的系统宜设计相应功能以便能实施删除操作，来满足该要求。

6.11.2.6 安全的开发环境

适用 ISO/IEC 27002:2013,14.2.6 中规定的控制，实施指南和其他信息。

6.11.2.7 外包开发

适用 ISO/IEC 27002:2013,14.2.7 中规定的控制，实施指南和其他信息以及以下补充指南。

ISO/IEC 27002:2013,14.2.7 外包开发的补充指南是：

设计的隐私原则和默认的隐私原则（见 6.11.2.5）如果适用，也同样适用于外包信息系统。

6.11.2.8 系统安全测试

适用 ISO/IEC 27002:2013,14.2.8 中规定的控制，实施指南和其他信息。

6.11.2.9 系统验收测试

适用 ISO/IEC 27002:2013,14.2.9 中规定的控制，实施指南和其他信息。

6.11.3 测试数据

6.11.3.1 测试数据的保护

适用 ISO/IEC 27002:2013,14.3.1 中规定的控制，实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013 的 14.3.1，测试数据保护的补充实施指南是：

PII 不宜用于测试目的；宜使用假的或合成的 PII。如果无法避免将 PII 用于测试目的，则宜实施与生产环境中使用的等效的技术和组织措施，以最大限度地降低风险。如果这种等效措施不可行，则宜进行风险评估，并用于选择适当的减缓风险的控制措施。

6.12 供应商关系

6.12.1 供应商关系中的信息安全

6.12.1.1 供应商关系的信息安全策略

适用 ISO/IEC 27002:2013,15.1.1 中规定的控制，实施指南和其他信息。

6.12.1.2 在供应商协议中强调安全

适用 ISO/IEC 27002:2013,15.1.2 中规定的控制，实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013，5.1.2 在供应商协议中强调安全的补充实施指南是：

组织宜在与供应商的协议中规定是否处理 PII，以及供应商为满足其信息安全和 PII 保护义务而需要满足的最低技术和组织措施（参见 7.2.6 和 8.2.1）.

供应商协议宜在考虑处理的 PII 种类的情况下，明确地在组织，合作伙伴，供应商和适当的第三方（客户，供应商等）之间分配职责。

组织与其供应商之间的协议宜提供一种机制，以确保组织支持和管理对所有适用法律和/或法规的遵守情况。协议宜要求客户接受独立审核以验证其合规性。

注 出于此类审核目的，可以考虑遵守相关和适用的安全和隐私标准，如 ISO/IEC 27001 或本标准。

PII 处理者的实施指南：

组织宜在与任何供应商的合同中指明 PII 仅允许在其指导下进行处理。

6.12.1.3 信息与通信技术供应链

适用 ISO/IEC 27002:2013,15.1.3 中规定的控制，实施指南和其他信息。

6.12.2 供应商服务交付管理

6.12.2.1 供应商服务的监视和审查

适用 ISO/IEC 27002:2013,15.2.1 中规定的控制，实施指南和其他信息。

6.12.2.2 供应商服务的变更管理

适用 ISO/IEC 27002:2013,15.2.2 中规定的控制，实施指南和其他信息。

6.13 信息安全事件管理

6.13.1 信息安全事件的管理和改进

6.13.1.1 责任和规程

适用 ISO/IEC 27002:2013,16.1.1 中规定的控制，实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013,16.1.1，责任和规程中的补充指南是：

作为整个信息安全事件管理过程的一部分，组织宜建立识别、记录违反 PII 的责任和处置规程。此外，组织应考虑适用的法律和/或法规，规定报告 PII 违规行为的通知方（包括此类通知的时间安排）和向执法当局披露的责任和规程。

一些司法管辖区对违规响应做出了具体规定，包括通知义务。在这些司法管辖区内运营的组织宜确保他们能够证明遵守这些法规。

6.13.1.2 报告信息安全事态

适用 ISO/IEC 27002:2013,16.1.2 中规定的控制，实施指南和其他信息。

6.13.1.3 报告信息安全弱点

适用 ISO/IEC 27002:2013,16.1.3 中规定的控制，实施指南和其他信息。

6.13.1.4 信息安全事态的评估和决策

适用 ISO/IEC 27002:2013,16.1.4 中规定的控制，实施指南和其他信息。

6.13.1.5 信息安全事件的响应

适用 ISO/IEC 27002:2013,16.1.5 中规定的控制，实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013 的 16.1.5，信息安全事件的响应的补充实施指南是：

PII 控制者的实施指南

作为其信息安全事件管理流程的一部分，涉及 PII 的事件宜引发组织的评审，以确定是否触发了 PII 违规行为响应流程。

事件不一定会触发此类评审。

注 1 导致未经授权访问 PII、访问存储 PII 的设备或设施，不一定以高频信息安全事件的形式展现。这些事件可以包括但不限于：对防火墙或边缘服务器的 ping 攻击(用來测试数据包能否利用 IP 协议访问特定主机) 和其他广播攻击，端口扫描攻击，不成功的登录尝试攻击，拒绝服务攻击和数据包嗅探攻击。

当违反 PII 发生时，响应规程宜包括相关通知和记录。

某些司法管辖区定义了宜将违反行为通知监管机构的情况，以及何时宜通知 PII 主体的情况。

通知宜明确的且是被要求的。

注 2 通知可以包含以下详细信息：

— 可以获得更多信息的联络点;

— 违规的可能后果;

— 对违规行为的描述，包括设计有关人员的数量以及有关的记录数量;

— 已采取或计划采取的措施。

注 3 有关安全事件管理的信息可在 ISO/IEC 27035 系列中找到。

如果发生涉及 PII 的违规行为，宜保留一份记录，并提供足够的信息，以便为监管和/或司法目的提供报告，例如：

— 对事件的描述;

— 时间段;

— 事件的后果;

— 报告者的名字;

— 事件报告给了谁;

— 为解决事件所采取的步骤（包括负责人和恢复的数据）;

— 事件导致 PII 无法获得，丢失，披露或更改的情况。

如果发生涉及 PII 的违规行为，该记录还宜包括已泄露的 PII 描述（如果已知）;如果需要实施通知，宜采取措施通知 PII 主体，监管机构或客户。

PII 处理者的实施指南

涉及 PII 违约通知的规定宜是组织与客户之间合同的一部分。合同应规定组织如何提供客户必需的信息，以保证顾客履行他们向相关机构通知的义务。此通知义务不会延伸到由客户或 PII 主体触发的由其承担负责的系统组件的违规。合同还宜定义与外部沟通时，双方必须遵守的响应时间。

在某些司法管辖区，PII 处理者应该在没有不当延迟的情况下（即尽快）通知 PII 控制者存在违规行为，期望事件一旦被发现，PII 控制者就可以采取适当的行动。

如果发生 PII 的违规行为，宜保留一份记录，并提供足够的信息，以便为监管和/或司法目的提供报告，例如：

— 对事件的描述;

— 时间段;

— 事件的后果;

— 报告着的名字;

— 事件报告给了谁;

— 为解决事件所采取的步骤（包括负责人和恢复的数据）;

— 事件导致 PII 无法获得，丢失，披露或更改的情况。

如果发生涉及 PII 的违规行为，该记录还宜包括已泄露的 PII 描述（如果已知）;如果执行了通知，则宜采取措施通知客户和/或监管机构。

在某些司法管辖区，适用的法律和/或法规可要求组织直接通知适当的监管机构（例如 PII 保护机构）涉及 PII 的违规行为。

6.13.1.6 从信息安全事件中学习

适用 ISO/IEC 27002:2013,16.1.6 中规定的控制，实施指南和其他信息。

6.13.1.7 证据的收集

适用 ISO/IEC 27002:2013,16.1.7 中规定的控制，实施指南和其他信息：

6.14 业务连续性管理的信息安全方面

6.14.1 信息安全连续性

6.14.1.1 规划信息安全连续性

适用 ISO/IEC 27002:2013,17.1.1 中规定的控制，实施指南和其他信息。

6.14.1.2 实现信息安全连续性

适用 ISO/IEC 27002:2013,17.1.2 中规定的控制，实施指南和其他信息。

6.14.1.3 验证，评审和评价信息安全连续性

适用 ISO/IEC 27002:2013,17.1.3 中规定的控制，实施指南和其他信息。

6.14.2 冗余

6.14.2.1 信息处理设施的可用性

适用 ISO/IEC 27002:2013,17.2.1 中规定的控制，实施指南和其他信息。

6.15 符合性

6.15.1 遵守法律和合同要求

6.15.1.1 确定适用的法律和合同要求

适用 ISO/IEC 27002:2013,18.1.1 中规定的控制，实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013，18.1.1，适用的法律和合同要求的识别的补充指南是：

组织应确定与处理与 PII 有关的任何法律制裁 (可能由于某些义务被遗漏而导致) 风险，包括直接来自当地监管机构的巨额罚款。在某些司法管辖区，本标准等国际标准可用于构成组织与客户之间合同的基础，为各自的安全性、隐私和 PII 保护责任提供框架。如果违反这些责任，合同条款可以成为制裁的依据。

6.15.1.2 知识产权

适用 ISO/IEC 27002:2013,18.1.2 中规定的控制，实施指南和其他信息。

6.15.1.3 记录的保护

ISO/ EC 27002:2013,18.1.3，中规定的控制，实施指南和其他信息于以下补充指南：

ISO/IEC 27002:2013 的 18.1.3，保护的记录的补充实施指南是：

可能需要审查当前和历史的策略和规程（例如，当客户争议解决和监管机构调查时）。

组织宜在其规定的保留期限内保留其隐私策略和相关规程的副本（请参阅 7.4.7）。这包括更新这些文档的先前版本。

6.15.1.4 隐私和个人身份信息保护

适用 ISO/IEC 27002:2013,18.1.4 中规定的控制，实施指南和其他信息。

6.15.1.5 密码控制规则

适用 ISO/IEC 27002:2013,18.1.5 中规定的控制，实施指南和其他信息。

6.15.2 信息安全评审

6.15.2.1 信息安全的独立评审

适用 ISO/IEC 27002:2013,18.2.1 中规定的控制，实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013,18.2.1，信息安全的独立评审的补充实施指南是：

如果组织为 PII 处理者，当单个的客户审核不切实际、可能增加安全风险时，组织宜在订立合同之前，以及在合同期存续期间，向客户提供客观公正的证据以证明安全性是根据组织的策略和规程实施和运作的。如果独立审核能涵盖预期用户的需求，并且结果能以足够透明的方式提供，那么组织实施的独立审核通常被认为满足客户对关注焦点的审核。

6.15.2.2 符合安全政策和标准

适用 ISO/IEC 27002:2013,18.2.2 中规定的控制，实施指南和其他信息。

6.15.2.3 技术符合性评审

适用 ISO/IEC 27002:2013,18.2.3 中规定的控制，实施指南和其他信息以及以下补充指南：

ISO/IEC 27002:2013,18.2.3，技术符合性评审的补充指南是：

技术评审作为遵守安全策略和标准的一部分，组织宜定义并实施针对 PII 处理工具和组件的评审。这可以包括：

— 持续监控以确认只允许的技术评审被实施;和/或

— 特定的渗透或漏洞测试（例如，去标识化的数据集可以应对有动机的入侵测试，以验证去标识化方法是否符合组织要求的）。

7 针对 PII 控制者的附加 ISO/IEC 27002 指南

7.1 总则

指南第 6 章 以及本章的补充内容为 PII 控制者创建了 PIMS 的特定指南。本章中记述的关于控制的实施指南在附录 A 中都有列出。

7.2 收集和处理的条件

目标：确定并记录该处理是合法的，具有适用司法管辖区的法律基础以及明确定义的合法目的。

7.2.1 识别并记录目的

控制

组织宜识别并记录 PII 处理的特定目的。

实施指南

组织宜确保 PII 主体了解组织处理 PII 的目的。组织有责任明确形成文件并与 PII 主体沟通。如果没有明确说明处理目的，就不能充分给予同意和选择。

处理 PII 目的的文档宜足够清晰和详细，以便用于向 PII 主体提供所需信息（见 7.3.2）。这包括获得同意所必需的信息（见 7.2.3），以及策略和规程的记录（见 7.2.8）。

其他信息

在云计算服务的部署中，ISO/IEC 19944 中的分类和定义有助于提供用于描述 PII 处理目的的术语。

7.2.2 确定合法的依据

控制

组织宜确定，记录并遵守为确定目的而处理 PII 的相关合法依据。

实施指南

某些司法管辖区要求组织能够在处理之前证明其处理的合法性。

处理 PII 的法律依据可以包括:

— PII 主体的同意;

— 履行合同;

— 遵守法律义务;

— 保护 PII 主体的切身利益;

— 实施为公共利益而执行的活动;

— PII 控制者的合法利益。

组织宜以此基础记录每个 PII 处理活动（参见 7.2.8）.

组织的合法利益可以包括，例如，信息安全目标，这些目标宜与 PII 主体在隐私保护方面的义务相平衡。

无论何时宜根据 PII 的属性（例如健康信息）或有关 PII 主体（例如与儿童有关的 PII）定义特殊类别的 PII，且组织宜在其分类方案中包括这些类别的 PII。

PII 的分类准则可能因司法管辖区而异，并且可能因适用于不同类型业务的不同监管制度而有所不同，因此组织需要了解适用于 PII 处理类别的内容并予以执行。

使用特殊类别的 PII 也可能受到更严格的控制。

更改或扩展处理 PII 的目的可能需要更新和/或修订法律依据。它还可能需要从 PII 主体那里获得额外的同意。

7.2.3 确定何时以及如何获得同意

控制

组织宜确定并记录一个过程，通过该过程，可以证明是否，何时以及如何从 PII 主体获得 PII 处理的同意。

实施指南

除非有其他适用的合法理由，否则处理 PII 需要主体同意。组织宜明确记录何时需要获得同意以及获得同意的要求。将处理目的、是否以及如何获得同意的信息相关联，可能是有用的。

某些司法管辖区对如何收集和记录同意具有特定要求（例如，不能与其他协议捆绑在一起）。此外，某些类型的数据收集（例如用于科学研究）和某些类型的 PII 主体（例如儿童）可能需要额外的要求。组织宜考虑此类要求并记录同意机制是如何满足这些要求。

7.2.4 获取并记录同意

控制

组织宜根据文件化的流程获得并记录 PII 主体的同意。

实施指南

组织宜根据请求提供所需同意的详细信息，以便获得 PII 主体的同意（例如，提供同意的时间、PII 主体的身份要求、同意书）。

在同意过程之前提交给 PII 主体的信息宜遵循在 7.3.3 的指导。

同意宜是：

— 完全出于自愿;

— 根据处理的目的而异;和

— 清楚无误。

7.2.5 隐私影响评估

控制

每当计划对 PII 进行新的处理或改变现有的 PII 处理时，组织宜判别实施隐私影响评估的必要性，适当时予以实施。

实施指南

PII 处理为 PII 主体带来风险。宜通过隐私影响评估来评估这些风险。某些司法管辖区定义了要求进行隐私影响评估的情况。触发 PIA 的情形包括：对 PII 主体产生法律效力的自动决策，特殊类别 PII 的大规模处理（例如健康相关信息，种族或民族信息，政治观点，宗

教或哲学信仰，工会会员资格，遗传数据或生物识别数据），或大规模公共可访问区域的系统性监测数据。

组织宜确定完成隐私影响评估所必需的因素。这些因素可以包括：已处理的 PII 类型列表，存储 PII 的位置，以及可以传输到的位置。在这种情况下，数据流程图和数据地图也很有用（参见 7.2.8 可获得记录以及处理 PII 的详细信息，这些信息可以帮助隐私影响或其他风险评估）。

其他信息

有关 PII 处理的隐私影响评估指南可在 ISO/IEC 29134 中找到。

7.2.6 与 PII 处理者的合同

控制

组织宜与 PII 处理者签订书面合同，合同宜确保在附录 B 中规定的适当控制措施得以实施。

实施指南

代表组织处理 PII 的 PII 处理者和组织之间签订的合同，宜要求实施附录 B 中适当控制，这需要建立在信息安全风险评估过程（见 5.4.1.2）和 PII 处理者执行范围（见 6.12）的基础上进行考虑。默认情况下，附录 B 中所有相关的控制都宜被考虑。如果组织决定不要求 PII 处理者实施附录 B 中的某些控制，宜明确不实施的理由。（见 5.4.1.3）。

合同可以分别定义各自的责任，但为了与本标准保持一致，宜考虑所有控制并将其包含在文档化信息中。

7.2.7PII 联合控制者

控制

组织宜确定与任何 PII 联合控制者处理 PII（包括 PII 保护和安全要求）的各自角色和职责。

实施指南

处理 PII 的角色和责任宜以透明的方式确定。

这些角色和责任宜记录在合同或各种类似的有约束力的文件中，其中宜包含 PII 被联合处置的条款和条件。在某些司法管辖区，此类协议称为数据共享协议。

PII 联合控制者协议可以包括（此列表既不是最终的也不是详尽的）：

— PII 共享/PII 联合控制者关系的目的;

— 识别 PII 联合控制者关系中的组织（PII 控制者）身份;

— 根据协议分享和/或传输和处理的 PII 类别;

— 处理操作概述（例如传输，使用）;

— 各自的角色和责任的描述;

— 负责实施 PII 保护的技术和组织安全措施;

— 在 PII 违约的情况下责任的定义（例如，谁将通知，何时，相互信息）;

— PII 的保留和/或处置条款;

— 不遵守协议的责任;

— 如何履行对 PII 主体的义务;

— 如何向 PII 主体提供有关 PII 联合控制者之间安排的本质信息;

— PII 主体如何获得他们有权获得的其他信息;和

— 给 PII 主体的联络点。

7.2.8 与处理 PII 有关的记录

控制

组织应确定并安全地保存必要的记录，以支持其处理 PII 的义务。

实施指南

维护 PII 处理记录的一种方法是拥有组织 PII 处理活动的清单或列表。这样的清单可以包括:

— 处理类型;

— 处理目的;

— PII 和 PII 主体类别的描述（例如儿童）;

— PII 曾经或将要披露 PII 的接收受者类别，包括第三国或国际组织的接收受者;

— 技术和组织安全措施的通用描述;和

— 隐私影响评估报告。

这样的清单应该由拥有者负责其准确性和完整性。

7.3 对 PII 主体的主要义务

目标：确保为 PII 主体提供有关其 PII 处理的适当信息，并履行与 PII 处理相关的任何其他适用义务。

7.3.1 确定并履行对 PII 主体的义务

控制

对于 PII 主体，组织宜确定并记录其应承担的与其处理 PII 相对应的法律、法规和业务义务，并提供履行这些义务的方式。

实施指南

对 PII 主体承担的义务及其支持他们的方式因司法管辖区而异。

组织宜确保他们提供适当的方式，以便及时，可行地履行对 PII 主体的义务。宜向 PII 主体提供明确的文件，说明对他们履行义务的程度，并提供最新的联系点以便 PII 主体提出他们的要求。

联系点宜以与收集和准许 PII 相似的方式提供（例如，如果收集 PII 是通过电子邮件或网站，联系点也应通过电子邮件或网站，而不是电话或传真等替代方案）。

7.3.2 确定 PII 主体的信息

控制

组织宜确定并记录需要向 PII 主体提供的信息，这些信息宜与他们的 PII 处理和提供时间相关联。

实施指南

组织宜确定法律，法规和/或业务要求以明确向 PII 主体提供信息的时间（例如，在处理之前，在请求之后的某个时间内回应等）以及所能提供的信息类型。

根据要求，信息可以采用通知的形式。可以提供给 PII 主体的信息类型的示例如下：

— 有关处理目的的信息;

— PII 控制者或其代表的联系方式;

— 有关处理的合法依据的信息;

— 如果不是直接从 PII 主体那里获得的话，获取 PII 地点的信息;

— 提供 PII 是否是法定或合同要求的信息，以及在适当情况下，未提供 PII 的可能后果;

— 有关对 PII 主体义务的信息，具体见 7.3.1 以及 PII 主体如何从中受益，特别是在访问，修改，纠正，请求删除，接收其 PII 副本和反对处理方面;

— 关于 PII 主体如何撤回同意的信息;

— 关于 PII 传输的信息;

— 有关 PII 接收人或接收人类别的信息;

— 有关 PII 保留期限的信息;

— 有关基于 PII 自动化处理的自动决策使用的信息;

— 有关提出投诉的权利以及如何提出投诉的信息;

— 关于提供信息的频率的信息（例如“及时”通知），组织如果更改或扩展 PII 处理的目的，组织宜提供最新信息。

7.3.3 向 PII 主体提供信息

控制

组织宜向 PII 主体提供清晰且易于访问的信息，以识别 PII 主体并描述如何处理其 PII。

实施指南

组织宜根据目标受众，使用清晰明了的语言，以及时，简洁，完整，透明，可理解和易于访问的形式向 PII 主体提供 7.3.2 中详细介绍的信息。

在适当的情况下，宜在收集 PII 时提供信息。它也宜是永久可访问的。

注 以图标和图像的形式向 PII 主体提供预定处理的概要是有帮助的。

7.3.4 提供修改或撤销同意的机制

控制

组织宜为 PII 主体提供修改或撤销其同意的机制。

实施指南

组织宜告知 PII 主体其可在任何时间撤销同意（可能因司法管辖区而异）的权利，并提供相应的机制。用于撤销的机制因系统而异;它应该与获得同意的机制保持一致。例如，如果通过电子邮件或网站收集同意，则撤销它的机制应该与其相同，而不是电话或传真等替代解决方案。

修改同意可以包括对 PII 的处理施加限制，这可以包括在某些情况下限制 PII 控制者删除 PII。

某些司法管辖区对 PII 主体何时以及如何修改或撤销其同意施加了限制

组织宜以与记录同意相类似的方式记录撤回或更改同意的任何请求

任何同意的变更宜传达到适当的系统，授权用户和相关第三方。

组织宜定义响应时间，并且宜根据它来处理请求。

附加信息

当撤销对特定 PII 处理的同意时，通常认为在撤回同意之前进行的所有 PII 处理都是适当的，但这种处理的结果不宜用于新处理。例如，如果 PII 主体撤回其对摘要信息的同意，则不宜进一步使用或咨询其摘要信息。

7.3.5 提供反对 PII 处理的机制

控制

组织宜为 PII 主体提供一种机制，以反对其 PII 的处理。

实施指南

某些司法管辖区为 PII 主体提供反对处理其 PII 的权利。受这些管辖区立法和/或法规约束的组织宜确保他们采取适当措施使 PII 主体能够行使这一权利。

组织宜记录与 PII 主体反对处理相关的法律和法规要求（例如，反对以有关直接营销为目的的 PII 处理）。组织宜向主体提供有关在这些情况下反对能力的信息。反对的机制可能有所不同，但宜与所提供的服务类型一致（例如，在线服务宜在线提供此功能）。

7.3.6 访问，更正和/或删除

控制

组织宜实施策略，规程和/或机制，以履行其对 PII 主体的义务，以访问，纠正和/或擦除其 PII。

实施指南

组织宜实施策略，规程和/或机制，以使 PII 主体能够在没有不当延迟的情况下获取，纠正和擦除其 PII。

组织宜定义请求响应时间，并且根据它来处理请求。

任何更正或擦除都宜通过系统和/或授权用户传达，并传递给接收 PII 数据的第三方。

注 由 7.5.3 相关规定产生的控制措施，在这方面提供帮助。

当 PII 主体对数据的准确性或更正存在争议时，组织宜实施策略，规程和/或机制予以解决。这些策略，规程和/或机制宜包括告知 PII 主体所做的更改，以及无法进行更正的原因（在特定情况下）。

某些司法管辖区对 PII 主体何时以及如何要求更正或擦除其 PII 施加限制。组织宜确定适用的这些限制，并使其保持最新状态。

7.3.7 PII 控制者告知第三方的义务

控制

组织宜通知共享 PII 的第三方针对共享 PII 数据的修改，撤回或异议，并实施适当的策略，流程和/或机制予以实现。

实施指南

组织宜用适当技术，采取适当措施，通知第三方任何与共享 PII 有关的修改，撤销准许，或异议。某些司法管辖区强制要求向这些第三方通报这些行为。

组织宜确定并维持与第三方的积极沟通渠道。相关责任可以分配给负责其运营和维护的个人。在通知第三方时，组织宜监控第三方的信息反馈。

注：对 PII 主体义务的变更可包括：修改、撤销同意、纠正请求、删除、处置限制，或对 PII 主体要求而产生的异议。

7.3.8 提供 PII 处置的副本

控制

当 PII 主体要求时，组织应该能够提供 PII 处置的副本。

实施指南

组织宜提供 PII 的副本，该副本以 PII 主体可访问的、结构化的、常用格式呈现， 并确保 PII 主体能够访问。

某些司法管辖区定义了哪些组织宜提供 PII 副本的情况，这些情况要求：允许 PII 主体或接收 PII 信息的控制者，以可移植性的格式提供 (通常是结构化的、常规的、机器可读的)。

组织宜确保提供给 PII 主体的 PII 副本仅与该 PII 主体相关。

根据保留和处置策略（如 7.4.7 中所述），所请求的 PII 如果已被删除，PII 控制者应通知 PII 主体。

如果组织不再能够识别 PII 主体（例如，由于去标识化过程），组织不宜仅以此为理由寻求（重新）识别 PII 主体。但是，在某些司法管辖区，法律可能会要求从 PII 主体处获取其他信息，以便重新识别 PII 主体和随后的披露。

如果技术上可行，应 PII 主体的要求，可将 PII 的副本从一个组织直接传输到另一个组织。

7.3.9 处理请求

控制

组织宜定义和记录策略和规程，用于处理和响应来自 PII 主体的合法请求。

实施指南

合理请求可包括处理 PII 副本的请求或提出投诉的请求。

某些司法管辖区允许组织在某些情况下收取费用（例如，过多或重复的请求）。

请求宜在适当的定义响应时间内处理。

某些司法管辖区定义了响应时间，具体取决于请求的复杂程度和数量，以及向 PII 主体通知的延迟要求。宜在隐私策略中定义适当的响应时间。

7.3.10 自动决策

控制

组织宜识别并明确对于 PII 主体的义务（包括法律义务），这些义务是由组织做出的 PII 自动处理的决定。

实施指南

当 PII 自动处理的决策对 PII 主体产生重大影响时，某些司法管辖区定义了对 PII 主体应尽的义务，例如：通知 PII 主体自动决策机制的存在。允许 PII 主体反对此类自动决策机制，和/或使用人为干预。

注：在某些司法管辖区，某些 PII 处理无法完全自动化。

在这些司法管辖区运营的组织宜考虑到这些义务。

7.4 默认隐私和设计的隐私

目标：确保设计流程和系统，使收集和处理（包括使用，披露，保留，传输和处置）仅限于所识别目的所必需的。

7.4.1 限制收集

控制

组织宜将 PII 的收集限制在与所识别目的相关性，成比例和必要的最小数量。

实施指南

组织宜将 PII 的收集与所识别的使用目的匹配，限定在充分的、相关的、必要的范围内。这包括限制组织间接收集的 PII 数量（例如，通过网络日志，系统日志等）。

隐私默认原则意味着：如果存在收集和处理 PII 的若干选项，则默认情况下，应禁用每个选项，并且仅通过 PII 主体的明确选择来逐个启用。

7.4.2 限制处理

控制

组织宜将 PII 的处理与所识别的使用目的匹配，限定在充分的、相关的、必要的范围内。

实施指南

限制 PII 的处理宜通过信息安全和隐私策略进行管理（见 6.2），同时宜建立文件化的规程以满足其选择以及合规。

PII 的处理包括：

— 披露;

— PII 存储期;和

— 谁能够访问他们的 PII;

宜默认为相对于所识别的处理目的，所需处理的最小数量。

7.4.3 准确性和质量

控制

在 PII 的整个生命周期中，组织应确保并记录相关信息，这些信息表明针对其被收集的目的，PII 是准确的，完整的和最新的。

实施指南

组织应实施策略，规程和/或机制，以尽量减少其处理的 PII 中的不准确性。还宜有策略，规程和/或机制来响应不准确的 PII 实例。这些策略，规程和/或机制宜包含记录的要求（例如通过技术系统配置等），并宜适用于整个 PII 生命周期。

附加信息

有关 PII 处理生命周期的更多信息，请参见 ISO/IEC 29101:2018, 6.2。

7.4.4 PII 最小化目标

控制

组织宜定义和记录数据最小化目标，以及使用哪些机制（例如去标识化）来实现这些目标。

实施指南

组织宜确定收集和处理的 PII 类型、PII 数量，相对于所识别目的是如何受限的。这可以包括使用去标识化或其他数据最小化技术。

所识别的目的（见 7.2.1）可以要求处理 PII 的去标识化信息，在这种情况下，组织应该能够描述这种处理。

在某些情况下，识别出的目的是：不需要处理原始 PII，并且已经去标识化的 PII 处理足以满足所识别的目的。在这些情况下，组织应定义并记录 PII 需求与 PII 主体之间的关联程度，以及用于处理 PII 的机制和技术，实现去标识化和/或 PII 最小化的目标。

用于最小化 PII 的机制取决于处理类型和处理系统。组织宜记录用于实现数据最小化的任何机制（技术系统配置等）。

如果数据去标识化处理后足以达到目的，组织宜定时记录旨在满足去识别目标的实施机制（技术系统配置等）。例如，删除与 PII 主体相关联的属性可足以使组织实现去标识化目的。在某些情况下，可以使用其他去识别技术，例如泛化（例如四舍五入）或随机化技术（例如，噪声添加）来实现足够的去标识化水平。

注 1：有关去标识化技术的更多信息，请参阅 ISO/IEC 20889。

注 2：对于云计算，ISO/IEC 19944 提供了数据识别限定的定义，可用于 PII 主体、将 PII 主体与 PII 中的一组特征的关联程度进行分类识别。

7.4.5 PII 在处理结束时去标识化和删除

控制

一旦原始 PII 不再需要用于所识别的目的，组织宜删除 PII，以不允许识别或需要重新识别 PII 主体的形式呈现它。

实施指南

组织宜有机制在没有预期进一步处理时删除 PII。或者，可以使用一些去标识化技术以达到去标识化数据不能被利用，以重新识别 PII 主体。

7.4.6 临时文件

控制

组织宜确保在指定的记录期内，按照记录的规程处置（例如擦除或销毁），因处理 PII 而创建的临时文件。

实施指南

组织宜定期检查以确保在确定的时间内删除未使用的临时文件。

其他信息

信息系统可以在正常的操作过程中创建临时文件。此类文件区别于系统或应用程序，但可包括：与数据库更新和应用操作程序相关的文件系统回滚日志和临时文件。相关信息处理任务完成后不需要临时文件，但有些情况下无法删除它们。这些文件保持使用的时间长度并不都是确定的，但“垃圾文件收集”规程宜识别相关文件，并确定自上次使用以来已经保存了多长时间。

7.4.7 保留

控制

满足 PII 处理目的时间截止，组织不宜逾期保留 PII。

实施指南

组织宜制定并维护其保留 PII 信息的时间表，同时考虑到保留 PII 不超过必要的要求。此类时间表宜考虑法律，法规和业务要求，如果组织保留数据与此类要求发生冲突，则需要做出业务决策（基于风险评估），并在时间表中记录。

7.4.8 处置

控制

组织宜具有处置 PII 的文件化策略，规程和/或机制。

实施指南

PII 处理技术的选择取决于许多因素，因为处置技术的性质和结果不同（例如，物理介质的粒度，或在电子介质上恢复已删除信息的能力）。在选择适当的处置技术时要考虑的因素包括但不限于待处置的 PII 的性质和范围，是否存在与 PII 相关的元数据，以及存储 PII 介质的物理特征。

7.4.9 PII 传输控制

控制

组织宜对数据传输网络传输（例如发送到另一个组织）的 PII 予以适当的控制，以确保数据到达预定目的地。

实施指南

需要控制 PII 的传输，通常是通过确保只有经过授权的个人可以访问传输系统，并遵循适当的流程（包括保留审核日志）来确保 PII 的传输不会损害正确的接收者。

7.5 PII 共享，转移和披露

目标：确定是否并记录何时共享，传输 PII 到其他司法管辖区、承担披露义务的第三方。

7.5.1 识别司法管辖区之间 PII 传输的基础

控制

组织宜确定并记录管辖区之间 PII 传输的相关基础。

实施指南

PII 传输可能受到法律和/或法规的约束，具体取决于数据将被传输到的管辖区域或国际组织（以及从何处传输）。组织宜记录满足传输基础要求的遵守情况。

某些司法管辖区可能会指定监管机构审查信息转让协议。在这些司法管辖区运营的组织宜了解此类要求。

注 如果传输发生在特定的司法管辖区内，发件人和收件人则均要准守该管辖区内适用的法律和/或法规。

7.5.2 PII 可以传输至的国家和国际组织

控制

组织宜制定并记录 PII 可以传输的目的国、目的国际组织。

实施指南

在正常运营中，应该向顾客提供：PII 可能被传输至的国家和国际组织的身份，宜包括 PII 分包处理国的身份。所包含的国家身份应考虑 7.5.1 的要求。

在正常运营之外，传输可能会应执法机关要求或者被适用的司法管辖区禁止，对这些国家的身份不能提前指定，以保护执法调查的机密性（见 7.5.1, 8.5.4 和 8.5.5）。

7.5.3 PII 转移记录

控制

组织宜记录 PII 向第三方的传输，并确保与各方的合作。作为对 PII 主体应尽的义务，组织宜支持 PII 主体未来的请求。

实施指南

记录包括：传输 PII 的第三方、由于 PII 控制者履行管理义务而修改的 PII、转让给第三方以满足 PII 主体的合法请求、删除 PII 的请求（例如，在撤回同意后）。

组织宜有一个策略来定义这些记录的保留期间。

组织宜严格保留必要信息，将数据最小化原则应用于传输记录。

7.5.4 向第三方披露 PII 的记录

控制

组织宜记录向第三方的 PII 披露，包括披露的 PII 内容、向谁、何时披露。

实施指南

PII 可以在正常操作过程中披露。宜记录这些披露。还宜记录对第三方的任何其他披露，例如合法调查或外部审核所产生的披露。记录宜包括披露的来源和进行披露权力的来源。

8 针对 PII 处理者的附加 ISO/IEC 27002 指南

8.1 总则

第 6 条章中的指南以及本章的补充指南为 PII 处理者创建了特定于 PIMS 的指南。本章中记述的关于控制的实施指南在附录 B 中都有列出。

8.2 收集和处理的条件

目标：根据适用的司法管辖区的法律，以及明确界定的合法的目的，确定并记录处理是合法的。

8.2.1 客户协议

控制

组织宜确保相关的 PII 处理合同能够解决：组织协助客户履行 PII 义务方面的作用（应考虑处理的性质和组织可利用的信息）。

实施指南

组织与客户之间的合同宜包括以下相关内容，并取决于客户的角色（PII 控制者或 PII 处理者）（此列表既不是绝对的也不是详尽的）：

— 设计的隐私和默认的隐私（见 7.4, 8.4）；

— 实现处理安全;

— 向监管机构通报涉及 PII 的违规行为;

— 向客户和 PII 主体通报涉及 PII 的违规行为;

— 进行隐私影响评估（PIA）;和

— 如果需要事先与相关 PII 保护机构进行磋商，则由 PII 处理者保证提供协助。

某些司法管辖区要求合同包括处理的主要内容和持续时间，处理的性质和目的，PII 的类型和 PII 主体的类别。

8.2.2 组织的目的

控制

组织宜确保代表客户处理 PII 仅按照客户的书面说明中所述的目的进行处理。

实施指南

组织与客户之间的合同应包括但不限于服务要实现的目标和时间表。

为了满足客户目标，在没有客户的明确指示的前提下，组织需满足客户的通用指令，组织可以确定处理 PII 方法的最优技术方案。 例如，为了有效地利用网络或处理能力，可能需要根据 PII 主体的某些特性来分配特定的处理资源。

组织应允许客户验证其是否符合目的规范和限制原则。这也确保了组织或其分包商不会出于其他目的而处理 PII，除非客户有书面说明具备其他目的。

8.2.3 营销和广告使用

控制

没有事先获得相应 PII 主体的同意，组织不宜使用根据合同处理的 PII 时，进行营销和广告。组织不宜将提供此类同意作为接收服务的条件。

实施指南

宜记录 PII 处理者与客户合同的合规性要求，尤其是在计划营销和/或广告的情况下。

如果未经 PII 主体明确同意，组织不应坚持包含营销和/或广告用途。

注 此控制是对通用控制 8.2.2 的补充，而不是替换或者取代。

8.2.4 侵权指令

控制

如果组织认为，处理指令违反了适用的法律和/或法规，组织应通知客户。

实施指南

组织验证客户指令是否违反法律和/或法规的能力取决于技术背景、指令本身、以及组织与客户之间的合同。

8.2.5 客户义务

控制

组织宜向客户提供适当的信息，以便向客户证明其履行了义务。

实施指南

客户所需的信息可包括组织是否允许客户参与、由客户授权或以其他方式同意的审核员进行审核，并为此做出贡献。

8.2.6 与处理 PII 有关的记录

控制

组织宜确定并保持必要的记录，以证明其代表客户尽了 PII 处理的义务（如适用合同中的规定）。

实施指南

某些司法管辖区可要求组织记录以下信息：

— 代表每个客户进行处理的类别;

— 传输到第三国或国际组织;和

— 技术和安全措施的通用描述。

8.3 对 PII 主体的义务

目标：确保为 PII 主体提供相关 PII 处理的适当信息，并履行与 PII 处理相关的适用义务。

8.3.1 对 PII 主体的义务

控制

组织宜为客户提供履行与 PII 主体相关的义务的方法。

实施指南

PII 控制者的义务可以通过立法，法规和/或合同来定义。客户的这些义务可能通过使用组织服务来履行。例如，包括及时纠正或删除 PII。

如果客户依赖于组织的信息或技术措施来履行其对 PII 主体的义务，则宜在合同中规定相关信息或技术措施。

8.4 默认的隐私，设计的隐私

目标：确保流程和系统的设计能够使 PII 的收集和处理（包括使用，披露，保留，传输和处置）必需限于所识别目的用途。

8.4.1 临时文件

控制

组织宜确保在指定的记录期内按照文件化规程处理（例如擦除或销毁）由于处理 PII 而创建的临时文件。

实施指南

组织宜定期验证以确保在指定的时间内删除未使用的临时文件。

其他信息

信息系统可以在正常的操作过程中创建临时文件。此类文件区别于系统或应用程序，但可包括：与数据库更新和应用操作程序相关的文件系统回滚日志和临时文件。相关信息处理任务完成后不需要临时文件，但有些情况下无法删除它们。这些文件保持使用的时间长度并不都是确定的，但“垃圾文件收集”规程宜识别相关文件，并确定自上次使用以来已经保存了多长时间。

8.4.2 回退，传输或处置 PII

控制

组织宜提供以安全的方式回退，传输和/或处置 PII 的能力。它还宜向客户提供该策略。

实施指南

在某个时间点，PII 可能需要以某种方式处置。这可能涉及将 PII 回退给客户，将其传输给另一个组织或 PII 控制者（例如，由于合并的结果），删除或以其他方式销毁，去标识化或存档。宜以安全的方式管理回退，传输和/或处置 PII 的能力。

当 PII 被客户确定为不再是必需时，组织宜提供必要的保证使客户确信，根据合同要求处理的 PII（由组织及其任何分包商）已从存储的任何位置删除，包括为了满足备份和业务连续性的目标。

组织宜制定并实施有关 PII 处置的策略，并应在被要求时向客户提供此策略。

该策略应涵盖合同终止至处置 PII 的保留期，以保护客户不会因合同失效而失去 PII。

注 这种控制和指南也与保存原则相关（见 7.4.7）。

8.4.3 PII 传输控制

控制

组织宜对通过数据传输网络传输的 PII 进行适当的控制，以确保数据到达其预定目的地。

实施指南

需要控制 PII 的传输，通常是通过确保只有经过授权的个人才能访问传输系统，并遵循适当的流程（包括保留审核数据）来确保 PII 的传输不会损害正确的接收者。PII 传输控制的要求可以包含在与客户签署的合同中。如果没有与传输相关的合同要求，则在传输之前应听取客户的建议。

8.5 PII 共享，传输和披露

目标：确定是否共享 PII，何时将其转让给其他司法管辖区或第三方，和/或根据适用的义务披露，以及是否提供文件。

8.5.1 管辖区之间 PII 传输的基础

控制

组织宜及时告知客户各管辖区之间的 PII 传输依据、以及此方面的预期变更，以便客户能够反对此类更改或终止合同。

实施指南

各管辖区之间的 PII 传输可能受到法律和/或法规的约束，具体取决于 PII 要传输到的管辖区域或组织（及 PII 数据的来源方）。组织宜记录对于此类要求的遵守情况，以作为转移的基础。

组织宜告知客户任何 PII 传输，包括传输到：

— 供应商;

— 其他方;

— 其他国家或国际组织。

如果发生变更，组织宜根据约定的时间提前通知客户，以便客户能够反对此类变更或终止合同。

组织与客户之间的协议可以包含组织可以在不通知客户的情况下实施变更的条款。宜设置此类情况限制在一定的范围内（例如，组织可以在不通知客户的情况下更改供应商，但不能将 PII 传输到其他国家/地区）。

在国际间传输 PII，宜识别诸如示范合同条款，具有约束力的公司规则或跨境隐私规则，以及在相关国家间签署的适用类似情况的协议。

8.5.2 PII 可以传输至的国家和国际组织

控制

组织宜制定并记录 PII 可能会被传输的目的地国和目的国际组织。

实施指南

在正常运营中，应该向顾客提供：PII 可能被传输至的国家和国际组织的身份，宜包括 PII 分包处理国的身份。所包含的国家的考虑宜涉及 8.5.1。

在正常运营之外，传输可能会应执法机关要求或者被适用的司法管辖区禁止，对这些国家的身份不能提前指定，以保护执法调查的机密性（见 7.5.1, 8.5.4 和 8.5.5）。

8.5.3 向第三方披露 PII 的记录

控制

组织宜记录向第三方的 PII 披露，包括已披露的 PII，向谁和何时披露。

实施指南

PII 可以在正常操作过程中公开。宜记录这些披露。还宜记录对第三方的任何其他披露，例如合法调查或外部审核所产生的披露。记录宜包括披露的来源和进行披露的批准来源。

8.5.4 PII 披露请求的通知

控制

组织宜通知客户任何具有法律约束力的 PII 披露请求。

实施指南

组织可能收到具有法律约束力的 PII 披露的请求（例如来自执法机构）。在这些情况下，组织宜在约定的时间范围内并根据商定的规程（可包括在客户合同中）通知客户任何此类请求。

在某些情况下，具有法律约束力的请求包括要求组织不要将此事件通知给任何人（禁止通知披露的一个例子是：根据刑法禁止通知，以维护执法调查的机密性）。

8.5.5 具有法律约束力的 PII 披露

控制

组织宜拒绝任何不具有法律约束力的 PII 披露请求，在进行任何 PII 披露之前宜询问客户，并接受那些已经通过客户授权且记录在合同中的纰漏请求。

实施指南

与控制实施相关的细节可以包含在客户合同中。

此类请求可能有多个来源，包括法院，法庭和行政当局。它们可以来自任何司法管辖区。

8.5.6 处理 PII 分包商的披露

控制

在使用分包商之前，组织宜向客户告知会使用分包商处理 PII 的情况。

实施指南

使用分包商处理 PII 的相关约定宜包括在客户合同中。

合同中宜披露拟使用分包商以及相关分包商的名称。披露的信息还宜包括分包商可以将数据传输至的国家和国际组织（见 8.5.2），以及分包商有义务达到或超过组织应尽义务的方式（见 8.5.7）。

如果评估分包商信息的公开披露为不可接受风险，则宜根据保密协议和/或应客户要求进行披露。宜让客户知道他的要求是可获得的。

这与 PII 可以传输至的国家名单无关。在任何情况下，都应向客户披露该清单，以便客户通知相应的 PII 主体。

8.5.7 分包商参与处理 PII

控制

组织宜仅根据客户合同聘请分包商处理 PII。

实施指南

如果组织将 PII 的部分或全部处理分包给另一个组织，则在分包商处理 PII 之前，需要客户的书面授权。可以是客户合同中的某一条款，也可以是特定的“一次性”协议。

组织宜与代表其进行 PII 处理的任何分包商签订书面合同，并宜确保其与分包商的合同涉及附录 B 中相应控制措施的实施。

组织与代表其处理 PII 的任何分包商之间的合同宜要求分包商实施附录 B 中相应的控制措施。这些措施应考虑到信息安全风险评估过程（见 5.4.1.2）和 PII 处理者执行的 PII 处理范围（见 6.12）。默认情况下，附录 B 中指定的所有控制宜被认为是有价值的。如果组织决定不要求分包商实施附录 B 中的某个控制，宜证明它被排除在外的正确性。

合同可以对各方的责任做出不同的定义，但为了与本标准保持一致，宜考虑标准中的所有控制措施并将其记载在书面信息中。

8.5.8 处理 PII 分包商的变更

控制

在获得常规书面授权的情况下，组织宜将有关添加或更换处理 PII 分包商的任何预期变更通知客户，从而使客户有机会反对此类变更。

实施指南

如果组织更换处理 PII 的部分或全部的分包商，则在新分包商处理 PII 之前，需要对客户的书面授权进行变更。可以是客户合同中的某一条款，也可以是特定的“一次性”协议。

附录 A

(规范性附录)

针对 PII 控制者的 PIMS 特定的控制目标和控制措施

本附录提供作为 PII 控制者的组织使用，无论是否使用 PII 处理者。本附录作为 ISO/IEC 27001:2013，附录 A 的扩展。

表 A.1 中列出的补充或修改的控制目标和控制直接源自本文档中的定义并与之一致，并在 ISO/IEC 27001:2013，6.1.3 的优化内容 5.4.1.3 的情景下使用。

并非本附录中列出的所有控制目标和控制都必须包含在 PIMS 的实施中。排除任何控制目标的理由应包括在适用性声明中（见 5.4.1.3）。排除的理由可包括风险评估认为不需要控制的地方，以及适用法律和/或法规不要求（或不受其限制）的情况。

注：本附录中的条款编号与本标准中第 7 章相关子条款编号一致。

表 A.1 - 控制目标和控制

A.7.2 收集和处理条件 目的： 确定并记录该处理是合法的，具有适用司法管辖区的法律基础以及明确定义的合法目的。		
A.7.2.1	识别和记录目的	控制 组织宜识别并记录 PII 处理的特定目的。
A.7.2.2	确定合法的依据	控制 组织宜确定，记录并遵守为确定目的而处理 PII 的相关合法依据。
A.7.2.3	确定何时和如何获得同意	控制 组织宜确定并记录一个过程，通过该过程，可以证明是否，何时以及如何从 PII 主体获得 PII 处理的同意。
A.7.2.4	获取并记录同意	控制 组织宜根据文件化的流程获得并记录 PII 主体的同意。
A.7.2.5	隐私影响评估	控制 每当计划对 PII 进行新的处理或改变现有的 PII 处理时，组织宜判别实施隐私影响评估的必要性，适当时予以实施。
A.7.2.6	与 PII 处理者的合同	控制 组织宜与 PII 处理者签订书面合同，合同宜确保在附录 B 中规定的适当控制措施得以实施。
A.7.2.7	联合 PII 控制者	控制 组织宜确定与任何 PII 联合控制者处理 PII（包括 PII 保护和安全要求）的各自角色和职责。
A.7.2.8	与处理 PII 有关的记录	控制 组织应确定并安全地保存必要的记录，以支持其处理 PII 的义务。

A.7.3 对 PII 主体的义务 目的： 确保为 PII 主体提供有关其 PII 处理的适当信息 履行与处理其 PII 相关的 PII 主体的任何其他适用义务。		
A.7.3.1	确定并履行对 PII 主体的义务	控制 对于 PII 主体，组织宜确定并记录其应承担的与其处理 PII 相对应的法律、法规和业务义务，并提供履行这些义务的方式。
A.7.3.2	确定 PII 主体的信息	控制 组织应确定并记录需要向 PII 主体提供的信息，这些信息应与他们的 PII 处理和提供时间相关。
A.7.3.3	向 PII 主体提供信息	控制 组织宜向 PII 主体提供清晰且易于访问的信息，以识别 PII 主体并描述如何处理其 PII。
A.7.3.4	提供修改或撤销同意的机制	控制 组织宜为 PII 主体提供修改或撤销其同意的机制。
A.7.3.5	提供反对 PII 处理的机制	控制 组织应为 PII 主体提供一种机制，以反对其 PII 的处理。
A.7.3.6	访问，更正和/或删除	控制 组织宜实施政策，规程和/或机制，以履行其对 PII 主体的义务，以访问，更正和/或擦除其 PII。
A.7.3.7	PII 控制者告知第三方的义务	控制 组织宜通知共享 PII 的第三方针对共享 PII 数据的修改，撤回或异议，并实施适当的策略，流程和/或机制予以实现。
A.7.3.8	提供 PII 处置的副本	控制 当 PII 主体要求时，组织应该能够提供 PII 处置的副本。
A.7.3.9	处理请求	控制 组织宜定义和记录策略和规程，用于处理和响应来自 PII 主体的合法请求。
A.7.3.10	自动决策	控制 组织宜识别并明确对于 PII 主体的义务（包括法律义务），这些义务是由组织做出的 PII 自动处理的决定。
A.7.4 默认的隐私，设计的隐私 目的： 确保设计流程和系统，使收集和处理（包括使用，披露，保留，传输和处置）仅限于所识别目的所必需的。		
A.7.4.1	限制收集	控制 组织宜将 PII 的收集限制在与所识别目的相关性，成比例和必要的最小数量。
A.7.4.2	限制处理	控制 组织宜将 PII 的处理与所识别的使用目的匹配，限定在充分的、相关的、必要的范围内。
A.7.4.3	准确性和质量	控制

		在 PII 的整个生命周期中，组织应确保并记录相关信息，这些信息表明针对其被收集的目的，PII 是准确的，完整的和最新的。
A.7.4.4	PII 最小化目标	控制 组织宜定义和记录数据最小化目标，以及使用哪些机制（例如去标识化）来实现这些目标。
A.7.4.5	PII 在处理结束时去识别化和删除	控制 一旦原始 PII 不再需要用于所识别的目的，组织宜删除 PII，以不允许识别或需要重新识别 PII 主体的形式呈现它。
A.7.4.6	临时文件	控制 组织宜确保在指定的记录期内，按照记录的规程处置（例如擦除或销毁），因处理 PII 而创建的临时文件。
A.7.4.7	保留	控制 满足 PII 处理目的时间截止，组织不宜逾期保留 PII。
A.7.4.8	处置	控制 组织宜具有处置 PII 的文件化策略，规程和/或机制。
A.7.4.9	PII 传输控制	控制 组织宜对数据传输网络传输（例如发送到另一个组织）的 PII 予以适当的控制，以确保数据到达预定目的地。
A.7.5 PII 共享，转移和披露 目标：确定是否并记录何时共享，传输 PII 到其他司法管辖区、承担披露义务的第三方。		
A.7.5.1	识别司法管辖区之间 PII 传输的基础	控制 组织宜确定并记录管辖区之间 PII 传输的相关基础。
A.7.5.2	PII 可以传输至的国家和国际组织	控制 组织宜制定并记录 PII 可以传输的目的国、目的国际组织。
A.7.5.3	PII 转移的记录	控制 组织宜记录 PII 向第三方的传输，并确保与各方的合作。作为对 PII 主体应尽的义务，组织宜支持 PII 主体未来的请求。
A.7.5.4	向第三方披露 PII 的记录	控制 组织宜记录向第三方的 PII 披露，包括披露的 PII 内容、向谁、何时披露。

附录 B

(规范性附录)

针对 PII 处理者的 PIMS 特定的控制目标和控制措施

本附录供作为 PII 处理者的组织使用，无论是否使用 PII 分包商。本附录作为 ISO/IEC 27001:2013，附录 A 的扩展。

表 B.1 中列出的补充或修改的控制目标和控制直接源自本文档中的定义的并与之一致，并在 ISO/IEC 27001:2013,6.1.3 的优化内容 5.4.1.3 的情景下使用。

并非本附录中列出的所有控制目标和控制都必须包含在 PIMS 的实施中。排除任何控制目标的理由应包括在适用性声明中（见 5.4.1.3）。排除的理由可包括风险评估认为不需要控制的地方，以及适用法律和/或法规不要求（或不受其限制）的情况。

注：本附录中的条款编号与本标准中第 8 章相关子条款编号一致。

表 B.1 - 控制目标和控制

B.8.2 收集和处理的条件 目标：根据适用的司法管辖区的法律，以及明确界定的合法的目的，确定并记录处理是合法的。		
B.8.2.1	客户协议	控制 组织宜确保相关的 PII 处理合同能够解决：组织协助客户履行 PII 义务方面的作用（应考虑处理的性质和组织可利用的信息）。
B.8.2.2	组织的目的	控制 组织宜确保代表客户处理 PII 仅按照客户的书面说明中所述的目的进行处理。
B.8.2.3	营销和广告使用	控制 没有事先获得相应 PII 主体的同意，组织不宜使用根据合同处理的 PII 时，进行营销和广告。组织不宜将提供此类同意作为接收服务的条件。
B.8.2.4	侵权指令	控制 如果组织认为，处理指令违反了适用的法律和/或法规，组织应通知客户。
B.8.2.5	顾客义务	控制 组织宜向客户提供适当的信息，以便向客户证明其履行了义务。
B.8.2.6	与处理 PII 相关的记录	控制 组织宜确定并保持必要的记录，以证明其代表客户尽了 PII 处理的义务（如适用合同中的规定）。
B.8.3 对 PII 主体的义务 目标：确保为 PII 主体提供有关其 PII 处理的适当信息，并履行与 PII 处理相关的任何其他适用义务。		

B.8.3.1	对 PII 主体的义务	控制 组织宜为客户提供履行与 PII 主体相关的义务的方法。
B.8.4 默认的隐私，设计的隐私 目标：确保流程和系统的设计能够使 PII 的收集和处理（包括使用，披露，保留，传输和处置）必需限于所识别目的用途。		
B.8.4.1	临时文件	控制 组织宜确保在指定的记录期内按照文件化规程处理（例如擦除或销毁）由于处理 PII 而创建的临时文件。
B.8.4.2	回退，传输或处置 PII	控制 组织宜提供以安全的方式回退，传输和/或处置 PII 的能力。它还宜向客户提供该策略。
B.8.4.3	PII 传输控制	控制 组织宜对通过数据传输网络传输的 PII 进行适当的控制，以确保数据到达其预定目的地。
B.8.5 PII 共享，传输和披露 目标：根据适用的义务，确定是否共享 PII，何时将其转让给其他司法管辖区或第三方和/或披露，以及是否提供文件。		
B.8.5.1	管辖区之间 PII 传输的基础	控制 组织宜及时告知客户各管辖区之间的 PII 传输依据、以及此方面的预期变更，以便客户能够反对此类更改或终止合同。
B.8.5.2	PII 可以被传输至的国家和国际组织	控制 组织宜制定并记录 PII 可能会被传输的目的地国和目的国际组织。
B.8.5.3	向第三方披露 PII 的记录	控制 组织宜记录向第三方的 PII 披露，包括已披露的 PII，向谁和何时披露。
B.8.5.4	PII 披露请求的通知	控制 组织宜通知客户任何具有法律约束力的 PII 披露请求。
B.8.5.5	具有法律约束力的 PII 披露	控制 组织宜拒绝任何不具有法律约束力的 PII 披露请求，在进行任何 PII 披露之前宜询问客户，并接受那些已经通过客户授权且记录在合同中的纰漏请求。
B.8.5.6	处理 PII 的分包商的披露	控制 在使用分包商之前，组织宜向客户告知会使用分包商处理 PII 的情况。
B.8.5.7	分包商处理 PII 的参与	控制 组织宜仅根据客户合同聘请分包商处理 PII。
B.8.5.8	分包商处理 PII 的变更	控制 在获得常规书面授权的情况下，组织宜将有关添加或更换处理 PII 分包商的任何预期变更通知客户，从而使客户有机会反对此类变更。

附录 C

(资料)

与 ISO/IEC 29100 的映射

表 C.1 和 C.2 给出本标准条款与 ISO/IEC 29100 隐私原则之间的映射关系。本附录以简洁的指示性方式就本标准的要求和控制的符合性如何与 ISO/IEC 29100 中规定的一般隐私原则给出了映射关系。

表 C.1 - PII 控制者和 ISO/IEC 29100 控制的映射

ISO/IEC 29100 隐私原则	PII 控制者的相关控制
1. 同意和选择	A.7.2.1 识别并记录目的 A.7.2.2 确定合法的依据 A.7.2.3 确定何时以及如何获得准许 A.7.2.4 获得并记录同意 A.7.2.5 隐私影响评估 A.7.3.4 提供修改或撤销同意的机制 A.7.3.5 提供反对 PII 处理的机制 A.7.3.7 PII 控制者告知第三方的义务
2.目的合法性和规范	A.7.2.1 识别并记录目的 A.7.2.2 确定合法的依据 A.7.2.5 隐私影响评估 A 7.3.2 确定提供给 PII 主体的信息 A 7.3.3 向 PII 主体提供信息 A 7.3.10 自动决策的制定
3.收集限制	A.7.2.5 隐私影响评估 A 7.4.1 限制收集
4.数据最小化	A 7.4.2 限制处理 A 7.4.4 PII 最小化目标 A 7.4.5 PII 在处理结束时去识别化和删除
5.使用，保留和披露限制	A 7.4.4 PII 最小化目标 A 7.4.5 PII 在处理结束时去识别化和删除 A 7.4.6 临时文件 A 7.4.7 保留 A 7.4.8 处置 A 7.5.1 识别司法管辖区之间 PII 传输的基础 A 7.5.4 向第三方披露 PII 的记录
6.准确性和质量	A.7.4.3 准确性和质量
7.公开性，透明度和通知	A 7.3.2 确定提供给 PII 主体的信息 A 7.3.3 向 PII 主体提供信息
8.个人参与和访问	A 7.3.1 确定并履行对 PII 主体的义务 A 7.3.3 向 PII 主体提供信息

	A 7.3.6 访问，更正和/或擦除 A 7.3.8 提供 PII 处置的副本 A 7.3.9 处理请求
9.问责制	A 7.2.6 与 PII 处理者的合同 A 7.2.7 联合 PII 控制者 A 7.2.8 与处理 PII 控制有关的记录 A 7.3.9 处理请求 A 7.5.1 识别司法管辖区之间 PII 传输的基础 A 7.5.2 PII 可以传输至的国家和国际组织 A 7.5.3 PII 转移的记录
10.信息安全	A 7.2.6 与 PII 处理者的合同 A 7.4.9 PII 传输控制
11.隐私合规	A.7.2.5 隐私影响评估

表 C.2 - PII 处理者和 ISO/IEC 29100 控制的映射

ISO/IEC29100 隐私原则	PII 处理者的相关控制
1.准许和选择	B.8.2.5 客户义务
2.目的合法性和规范	B.8.2.1 客户协议 B.8.2.2 组织的目的 B.8.2.3 营销和广告使用 B.8.2.4 侵权指令 B.8.3.1 对于 PII 主体的义务
3.收集限制	N / A
4.数据最小化	B.8.4.1 临时文件
5.使用，保留和披露限制	B.8.5.3 向第三方披露 PII 的记录 B.8.5.4 PII 披露请求的通知 B.8.5.5 具有法律约束力的 PII 披露
6.准确性和质量	N / A
7.公开性，透明度和通知	8.5.6 处理 PII 分包商的披露 8.5.7 分包商参与处理 PII 8.5.8 处理 PII 分包商的变更
8.个人参与和访问	B.8.3.1 对 PII 主体的义务
9.问责制	B.8.2.6 与处理 PII 有关的记录 B.8.4.2 回退，传输或处置 PII B.8.5.1 管辖区之间 PII 传输的基础 B.8.5.2 PII 可以传输至的国家和国际组织
10.信息安全	B.8.4.3 PII 传输控制
11.隐私合规	B.8.2.5 客户义务

附录 D

(资料)

与通用数据保护条例的映射

本附录给出了本标准条款与欧盟通用数据保护条例中第 5 章至第 49 条之间(43 条除外)的映射关系。它显示了如果遵守了本标准的要求和控制措施与其履行 GDPR 的相关性。

但是，这纯粹是指示性的，根据本标准，组织有责任评估其法律义务并决定如何遵守这些义务。

表 D.1- ISO/IEC 27701 与 GDPR 的映射

ISO/IEC 27701 条款	GDPR 条款
5.2.1	(24) (3) , (25) (3) , (28) (5) , (28) (6) , (28) (10) , (32) (3) , (40) (1) , (40) (2) (a) , (40) (2) (b) , (40) (2) (c) , (40) (2) (d) , (40) (2) (e) , (40) (2) (f) , (40) (2) (g) , (40) (2) (h), (40) (2) (i) , (40) (2) (j) , (40) (2) (k) , (40) (3) , (40) (4) , (40) (5) , (40) (6) , (40) (7) , (40) (8) , (40) (9) , (40) (10) , (40) (11) , (41) (1) , (41) (2) (a) , (41) (2) (b) , (41) (2) (c) , (41) (2) (d) , (41) (3) , (41) (4) , (41) (5) , (41) (6) , (42) (1) , (42) (2) , (42) (3) , (42) (4) , (42) (5) , (42) (6) , (42) (7) , (42) (8)
5.2.2	(31) , (35) (9) , (36) (1) , (36) (2) , (36) (3) (a) , (36) (3) (b) , (36) (3)) (c) , (36) (3) (d), (36) (3) (e) , (36) (3) (f) , (36) (5)
5.2.3	(32) (2)
5.2.4	(32) (2)
5.4.1.2	(32) (1) (b) , (32) (2)
5.4.1.3	(32) (1) (b) , (32) (2)
6.2.1.1	(24) (2)
6.3.1.1	(27) (1) , (27) (2) (a) , (27) (2) (b) , (27) (3), (27) (4) , (27) (5) , (37) (1) (a) , (37) (1) (b), (37) (1) (c) , (37) (2) , (37) (3) , (37) (4) , (37) (5) , (37) (6) , (37) (7) , (38) (1) , (38) (2) , (38) (3) , (38) (4) , (38) (5) , (38) (6) , (39) (1) (a) , (39) (1) (b) , (39) (1) (c) , (39) (1) (d) , (39) (1) (e) , (39) (2)
6.3.2.1	(5) (1) (F)
6.4.2.2	(39) (1) (b)
6.5.2.1	(5) (1) (f) , (32) (2)
6.5.2.2	(5) (1) (F)

6.5.3.1	(5) (1) (f) , (32) (1) (a)
6.5.3.2	(5) (1) (F)
6.5.3.3	(5) (1) (f) , (32) (1) (a)
6.6.2.1	(5) (1) (F)
6.6.2.2	(5) (1) (F)
6.6.4.2	(5) (1) (F)
6.7.1.1	(32) (1) (a)
6.8.2.7	(5) (1) (F)
6.8.2.9	(5) (1) (F)
6.9.3.1	(5) (1) (f) , (32) (1) (c)
6.9.4.1	(5) (1) (F)
6.9.4.2	(5) (1) (F)
6.10.2.1	(5) (1) (F)
6.10.2.4	(5) (1) (f) , (28) (3) (b) , (38) (5)
6.11.1.2	(5) (1) (f) , (32) (1) (a)
6.11.2.1	(25) (1)
6.11.2.5	(25) (1)
6.11.3.1	(5) (1) (F)
6.12.1.2	(5) (1) (f) , (28) (1) , (28) (3) (a) , (28) (3) (b) , (28) (3) (c) , (28) (3) (d) , (28) (3) (e), (28) (3) (f) , (28) (3) (g) , (28) (3) (h) , (30) (2) (d) , (32) (1) (b)
6.13.1.1	(5) (1) (f) , (33) (1) , (33) (3) (a) , (33) (3) (b) , (33) (3) (c) , (33) (3) (d) , (33) (4) , (33) (5) , (34) (1) , (34) (2) , (34) (3) (a) , (34) (3) (b) , (34) (3) (c) , (34) (4)
6.13.1.5	(33) (1) , (33) (2) , (33) (3) (a) , (33) (3) (b), (33) (3) (c) , (33) (3) (d) , (33) (4) , (33) (5), (34) (1) , (34) (2)
6.15.1.1	(5) (1) (f) , (28) (1) , (28) (3) (a) , (28) (3) (b) , (28) (3) (c) , (28) (3) (d) , (28) (3) (e), (28) (3) (f) , (28) (3) (g) , (28) (3) (h) , (30) (2) (d) , (32) (1) (b)
6.15.1.3	(5) (2) , (24) (2)
6.15.2.1	(32) (1) (d) , (32) (2)
6.15.2.3	(32) (1) (d) , (32) (2)
7.2.1	(5) (1) (b) , (32) (4)
7.2.2	(10) , (5) (1) (a) , (6) (1) (a) , (6) (1) (b) , (6) (1) (c) , (6) (1) (d) , (6) (1) (e) , (6) (1) (f) , (6) (2) , (6) (3) , (6) (4) (a) , (6) (4) (b) , (6) (4) (c) , (6) (4) (d) , (6) (4) (e) , (8) (3) , (9) (1) , (9) (2) (b) , (9) (2) (c) , (9) (2) (d) , (9) (2) (e) , (9) (2) (f) , (9) (2)

	(g) , (9) (2) (h) , (9) (2) (i) , (9) (2) (j) , (9) (3) , (9) (4) , (17) (3) (a) , (17) (3) (b) , (17) (3) (c) , (17) (3) (d) , (17) (3) (e) , (18) (2) , (22) (2) (a) , (22) (2) (b) , (22) (2) (c), (22) (4)
7.2.3	(8) (1) , (8) (2)
7.2.4	(7) (1) , (7) (2) , (9) (2) (a)
7.2.5	(35) (1) , (35) (2) , (35) (3) (a) , (35) (3) (b), (35) (3) (c) , (35) (4) , (35) (5) , (35) (7) (a), (35) (7) (b) , (35) (7) (c) , (35) (7) (d) , (35) (8) , (35) (9) , (35) (10) , (35) (11) , (36) (1), (36) (3) (a) , (36) (3) (b) , (36) (3) (c) , (36) (3) (d) , (36) (3) (e) , (36) (3) (f) , (36) (5)
7.2.6	(5) (2) , (28) (3) (e) , (28) (9)
7.2.7	(26) (1) , (26) (2) , (26) (3)
7.2.8	(5) (2) , (24) (1) , (30) (1) (a) , (30) (1) (b), (30) (1) (c) , (30) (1) (d) , (30) (1) (f) , (30) (1) (g) , (30) (3) , (30) (4) , (30) (5)
7.3.1	(12) (2)
7.3.2	(11) (2) , (13) (3) , (13) (1) (a) , (13) (1) (b), (13) (1) (c) , (13) (1) (d) , (13) (1) (e) , (13) (1) (f) , (13) (2) (c) , (13) (2) (d) , (13) (2) (e) , (13) (4) , (14) (1) (a) , (14) (1) (b) , (14) (1) (c) , (14) (1) (d) , (14) (1) (e) , (14) (1) (f) , (14) (2) (b) , (14) (2) (e) , (14) (2) (f) , (14) (3) (a) , (14) (3) (b) , (14) (3) (c) , (14) (4) , (14) (5) (a) , (14) (5) (b) , (14) (5) (c) , (14) (5) (d) , (15) (1) (a) , (15) (1) (b) , (15) (1) (c) , (15) (1) (d) , (15) (1) (e) , (15) (1) (f) , (15) (1) (g) , (15) (1) (h) , (15) (2) , (18) (3) , (21) (4)
7.3.3	(11) (2) , (12) (1) , (12) (7) , (13) (3) , (21) (4)
7.3.4	(7) (3) , (13) (2) (c) , (14) (2) (d) , (18) (1) (a) , (18) (1) (b) , (18) (1) (c) , (18) (1) (d)
7.3.5	(13) (2) (b) , (14) (2) (c) , (21) (1) , (21) (2), (21) (3) , (21) (5) , (21) (6)
7.3.6	(5) (1) (d) , (13) (2) (b) , (14) (2) (c) , (16), (17) (1) (a) , (17) (1) (b) , (17) (1) (c) , (17) (1) (d) , (17) (1) (e) , (17) (1) (f) , (17) (2)
7.3.7	(19)
7.3.8	(15) (3) , (15) (4) , (20) (1) , (20) (2) , (20) (3) , (20) (4)

7.3.9	(15) (1) (a) , (15) (1) (b) , (15) (1) (c) , (15) (1) (d) , (15) (1) (e) , (15) (1) (f) , (15) (1) (g) , (15) (1) (h) , (12) (3) , (12) (4) , (12) (5) , (12) (6)
7.3.10	(13) (2) (f) , (14) (2) (g) , (22) (1) , (22) (3)
7.4.1	(5) (1) (b) , (5) (1) (c)
7.4.2	(25) (2)
7.4.3	(5) (1) (d)
7.4.4	(5) (1) (c) , (5) (1) (e)
7.4.5	(5) (1) (c) , (5) (1) (e) , (6) (4) (e) , (11) (1), (32) (1) (a)
7.4.6	(5) (1) (c)
7.4.7	(13) (2) (a) , (14) (2) (a)
7.4.8	(5) (1) (F)
7.4.9	(5) (1) (F)
7.5.1	(15) (2) , (44) , (45) (1) , (45) (2) (a) , (45) (2) (b) , (45) (2) (c) , (45)) (3) , (45) (4) , (45) (5) , (45) (6) , (45) (7) , (45) (8) , (45) (9) , (46) (1) , (46) (2) (a) , (46) (2) (b) , (46)) (2) (c) , (46) (2) (d) , (46) (2) (e) , (46) (2) (f) , (46) (3) (a) , (46) (3) (b) , (46) (4) , (46) (5) , (47) (1) (a) , (47) (1) (b) , (47) (1) (c), (47) (2) (a) , (47) (2) (b) , (47) (2) (c) , (47) (2) (d) , (47) (2) (e) , (47) (2) (f) , (47) (2) (g) , (47) (2) (h) , (47) (2) (i) , (47) (2) (j) , (47) (2) (k) , (47) (2) (l) , (47) (2) (m) , (47) (2) (n) , (47) (3) , (49) (1) (a) , (49) (1) (b), (49) (1) (c) , (49) (1) (d) , (49) (1) (e) , (49) (1) (f) , (49) (1) (g) , (49) (2) , (49) (3) , (49) (4) , (49) (5) , (49) (6) , (30) (1) (e) , (48)
7.5.2	(15) (2) , (30) (1) (e)
7.5.3	(30) (1) (e)
7.5.4	(30) (1) (d)
8.2.1	(28) (3) (f) , (28) (3) (e) , (28) (9) , (35) (1)
8.2.2	(5) (1) (a) , (5) (1) (b) , (28) (3) (a) , (29) , (32) (4)
8.2.3	(7) (4)
8.2.4	(28) (3) (H)
8.2.5	(28) (3) (H)
8.2.6	(30) (3) , (30) (4) , (30) (5) , (30) (2) (a) , (30) (2) (b)
8.3.1	(15) (3) , (17) (2) , (28) (3) (e)
8.4.1	(5) (1) (c)

8.4.2	(28) (3) (g), (30) (1) (f)
8.4.3	(5) (1) (F)
8.5.1	(44), (46) (1), (46) (2) (a), (46) (2) (b), (46) (2) (c), (46) (2) (d), (46) (2) (e), (46) (2) (f), (46) (3) (a), (46) (3) (b), (48), (49) (1) (a), (49) (1) (b), (49) (1) (c), (49) (1) (d), (49) (1) (e), (49) (1) (f), (49) (1) (g), (49) (2), (49) (3), (49) (4), (49) (5), (49) (6)
8.5.2	(30) (2) (c)
8.5.3	(30) (1)
8.5.4	(28) (3) (a)
8.5.5	(48)
8.5.6	(28) (2), (28) (4)
8.5.7	(28) (2), (28) (3) (d)
8.5.8	(28) (2)

附录 E

(资料)

与 ISO/IEC 27018 和 ISO/IEC 29151 的映射

ISO/IEC 27018 为充当 PII 处理者并提供公共云服务的组织提供了进一步的信息。ISO/IEC 29151 为 PII 控制者处理 PII 提供了额外的控制和指导。

表 E.1 给出了本标准条款与 ISO/IEC 27018 和 ISO/IEC 29151 规定之间的指示性映射。它说明了本标准的要求和控制如何与 ISO/IEC 27018 和/或 ISO/IEC 29151 的规定保持一致。

本附录是指示性的，不宜假设具有映射关系的条款之间意味着等同。

表 E.1- ISO/IEC 27701 与 ISO/IEC 27018 和 ISO/IEC 29151 的映射

ISO/IEC 27701 条款	ISO/IEC 27018 子条款	ISO/IEC 29151 子条款
5.2	N/A	N/A
5.3	N/A	N/A
5.4	N/A	4.2
5.5	N/A	7.2.3
5.6	N/A	N/A
5.7	N/A	N/A
5.8	N/A	N/A
6.1	N/A	N/A
6.2	5.1.1	5
6.3	6.1.1	N/A
6.4	7.2.2	N/A
6.5.1	N/A	8.1
6.5.2	N/A	8.2
6.5.3	A.11.4,A11.5	8.3
6.6.1	N/A	N/A
6.6.2	9.2.1, A.11.8, A,11,9, A.11.10	9.2
6.6.3	N/A	9.3
6.6.4	7.2.2,9.4.2	9.4
6.7	10.1.1	N/A
6.8.1	N/A	11.1
6.8.2	11.2.7, A.11.2, A.11.13	N/A
6.9.1	N/A	12.1
6.9.2	N/A	12.2
6.9.3	N/A	12.3
6.9.4	12.4.1,12.4.2	12.4
6.9.5	N/A	N/A
6.9.6	N/A	N/A
6.9.7	N/A	N/A

6.10.1	N/A	13.1
6.10.2	13.2.1, A.11.1	13.2
6.11.1	A.11.6	N/A
6.11.2	N/A	N/A
6.11.3	12.1.4	N/A
6.12.1	A.11.11	N/A
6.12.2	N/A	N/A
6.13	16.1.1, A.10.1	N/A
6.14	N/A	N/A
6.15.1	A.10.2	N/A
6.15.2	18.2.1	18.2
7.2.1	N/A	A.4
7.2.2	N/A	A.4.1
7.2.3	N/A	N/A
7.2.4	N/A	A.3.1
7.2.5	N/A	A.11.2
7.2.6	N/A	A.11.3
7.2.7	N/A	N/A
7.2.8	N/A	N/A
7.3.1	N/A	A.10
7.3.2	N/A	N/A
7.3.3	N/A	A.9
7.3.4	N/A	N/A
7.3.5	N/A	N/A
7.3.6	N/A	A.10.1
7.3.7	N/A	N/A
7.3.8	N/A	N/A
7.3.9	N/A	N/A
7.3.10	N/A	N/A
7.4.1	N/A	A.5
7.4.2	N/A	N/A
7.4.3	N/A	A.8
7.4.4	N/A	N/A
7.4.5	N/A	A.7.1
7.4.6	N/A	A.7.2
7.4.7	N/A	A.7.1
7.4.8	N/A	N/A
7.4.9	N/A	N/A
7.5.1	N/A	A.13.2
7.5.2	N/A	A.13.2
7.5.3	N/A	A.13.2
7.5.4	N/A	A.7.4
8.2.1	N/A	N/A

8.2.2	A.3.1	N/A
8.2.3	A.3.2	N/A
8.2.4	N/A	N/A
8.2.5	N/A	N/A
8.2.6	N/A	N/A
8.3.1	A.2.1	N/A
8.4.1	A.5.1	N/A
8.4.2	A.10.3	N/A
8.4.3	A.12.2	N/A
8.5.1	N/A	N/A
8.5.2	A.12.1	N/A
8.5.3	A.6.2	N/A
8.5.4	A.6.1	N/A
8.5.5	A.6.1	N/A
8.5.6	A.8.1	A.7.5
8.5.7	A.8.1	N/A
8.5.8	A.8.1	N/A

附录 F

(资料)

如何在 ISO/IEC 27001 和 ISO/IEC 27002 的基础上实施 ISO/IEC 27701

F.1 如何应用本标准

本标准基于 ISO/IEC 27001:2013 和 ISO/IEC 27002:2013，并扩展了他们的要求和指南，除信息安全外，还考虑了可能受 PII 处理影响的 PII 主体的隐私保护。这意味着，在 ISO/IEC 27001 或 ISO/IEC 27002 中使用术语“信息安全”时，等同于使用“信息安全和隐私”。

表 F.1 给出了信息安全术语的扩展映射关系，以便将其应用于此文件。

表 F.1 - 对信息安全术语与追加隐私扩展后术语的映射关系

ISO/IEC 27001	ISO/IEC 27701
信息安全	信息安全和隐私
信息安全策略	信息安全和隐私策略
信息安全管理	信息安全和隐私信息管理
信息安全管理体系（ISMS）	隐私信息管理体系（PIMS）
信息安全目标	信息安全和隐私目标
信息安全绩效	信息安全和隐私绩效
信息安全要求	信息安全和隐私要求
信息安全风险	信息安全和隐私风险
信息安全风险评估	信息安全和隐私风险评估
信息安全风险处理	信息安全和隐私风险处理

基本上，在处理 PII 时，有三种情况本文适用于保护 PII 主体的隐私：

1) 安全标准的应用原则如下：参考的标准适用于上述各条款的术语扩展。因此，不再重复引用标准，而是仅在各个条款中提及。

2) 安全标准的增加：引用标准适用于其他特定于隐私的要求或实施指南。

3) 优化安全标准：引用标准通过隐私特定要求或实施指南进行完善。

F.2 安全标准的改进示例

本节描述了 5.4.1.2 如何适用于 ISO/IEC 27001:2013,6.1.2。

在处理 PII 时，考虑到保护 PII 主体的隐私，ISO IEC 27001:2013,6.1.2 将使用下面带下划线的文本进行修改：

6.1.2 信息安全风险评估

组织应定义并应用<u>信息安全和隐私风险评估过程</u>：

a）建立并维护信息安全和隐私风险标准，包括：

1）风险验收标准；和

2）进行信息安全和隐私风险评估的标准；

b）确保重复的信息安全和隐私风险评估产生一致，有效和可比较的结果；

c）识别信息安全和隐私风险：

1）应用信息安全和隐私风险评估过程，以识别与信息安全和隐私信息管理系统范围内的信息的机密性，完整性和可用性丧失相关的风险；和

2）识别风险所有者；

d）分析信息安全和隐私风险；

1）评估 6.1.2 c）中确定的风险实现后可能产生的后果；

2）评估 6.1.2 c）1）中确定的风险发生的实际可能性；和

3）确定风险等级；

e）评估信息安全和隐私风险：

1）将风险分析结果与 6.1.2 a）中确定的风险标准进行比较；和

2）优先分析风险处理的分析风险。

组织应保留有关信息安全和隐私风险评估过程的文档信息。

参考文献

[1] ISO/IEC 19944, *Information technology — Cloud computing — Cloud services and devices: Data flow, data categories and data use*

[2] ISO/IEC 20889, *Privacy enhancing data de-identification terminology and classification of techniques*

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

[4] ISO/IEC 27018, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

[5] ISO/IEC 27035-1, *Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management*

[6] ISO/IEC 29101, *Information technology — Security techniques — Privacy architecture framework*

[7] ISO/IEC 29134, *Information technology — Security techniques — Guidelines for privacy impact*

[8] ISO/IEC 29151, *Information technology — Security techniques — Code of practice for personally identifiable information protection*

[9] ISO/IEC/DIS 29184, *Information technology — Security techniques — Guidelines for online privacy notices and consent*