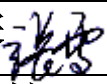





上海赛威认证有限公司

基于 ISO/IEC 29151 的个人身份信息保护 管理体系认证实施规则

文件状态	现行、受控		
文件编号	SW-TCR-1004-4	版本	1.2
发布日期	2023-10-28		
修订日期	2025-08-26		
实施日期	2025-08-26		
编制	技委会		
审核	张雯 		
批准	邓雪松 		



目录

- 1、适用范围与认证依据
- 2、规范性引用文件
- 3、术语和定义
- 4、认证基本原则
- 5、认证基本流程
- 6、认证人员要求
- 7、认证实施程序
 - 7.1、认证申请
 - 7.2、申请评审
 - 7.3、认证范围
 - 7.4、审核时间.
 - 7.5、审核时间计算方法
 - 7.6、建立审核方案
 - 7.7、审核启动
 - 7.8、初次认证审核
 - 7.9、认证决定
- 8、认证证书
- 9、监督审核
- 10、再认证
- 11、管理体系结合审核
- 12、特殊审核
- 13、暂停和恢复认证资格
- 14、撤销和注销认证资格
- 15、受理组织的申诉
- 16、认证记录的管理
- 17、其他



1、适用范围与认证依据

1.1 本文件适用于上海赛威认证有限公司（下称“SWCC”）对申请组织实施基于 ISO/IEC 29151 的个人身份信息安全管理体系（下称“PIIP”）的认证活动，以满足第三方认证制度要求以及作为提供认证服务的规范。

1.2 本文件规定了 PIIP 认证应遵循的原则、方法以及通报等内容。

1.3 本文件是对 SWCC 从事 PIIP 认证活动基本要求，并在认证双方签订合同时予以确认和采用。
说明：为简化文字描述，本文件中出现的“审核、评价、评估、检查”等活动均表述为“审核”。

注：根据认证过程的变化，本文件对申请认证单位可以使用不同的称呼，例如：申请组织/认证客户、受审核方、获证组织/客户。

1.4 认证依据

ISO/IEC 29151:2017《信息技术 安全技术 个人身份信息保护实施规范》

2、规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

◆ISO/IEC 29151:2017《信息技术 安全技术 个人身份信息保护实施规范》

◆GB/T 27021.1-2017《合格评定 管理体系审核认证机构要求 第 1 部分：要求》（ISO/IEC 17021-1:2015，IDT）（CNAS-CC01）

◆ISO/IEC 27006-1:2024《信息安全、网络安全和隐私保护 信息安全管理体系审核和认证机构要求 第 1 部分：通用》（CNAS-CC170）

◆ISO/IEC TS 27006-2:2021《信息安全管理体系审核和认证机构要求 第 2 部分：隐私信息管理体系》

◆ISO/IEC 27001:2022《信息安全、网络安全和隐私保护 信息安全管理体系 要求》

◆ISO/IEC 27002:2022《信息安全、网络安全和隐私保护 信息安全控制》

- ◆ISO/IEC 27005:2022 《信息安全、网络安全和隐私保护 信息安全风险管理指南》
- ◆ISO/IEC 27007:2020 《信息安全、网络安全和隐私保护 信息安全管理体系审核指南》
- ◆ISO/IEC 27013:2021 《信息安全、网络安全和隐私保护 关于 ISO/IEC 27001 和 ISO/IEC 20000-1 结合实施指南》
- ◆ISO/IEC 29100:2024 《信息技术 安全技术 隐私框架》
- ◆GB/T 19011-2021 《管理体系审核指南》（ISO 19011:2018, IDT）
- ◆CNAS-CC12 《已认可的管理体系认证的转换》（现行有效版本）
- ◆CNAS-CC14 《信息和通信技术（ICT）在审核中应用》（现行有效版本）

3、术语和定义

下列术语和定义适用于本文件。

3.1 个人信息 PII - personally identifiable information

是指（a）可用于在信息和与信息有关的自然人之间建立联系的信息，或（b）与自然人有或可能有直接或间接联系的信息。

注 1：定义中的“自然人”是 PII 主体。为了确定 PII 主体是否可识别，应考虑持有数据的隐私利益相关方或任何其他方可以合理使用的**所有**手段，以建立 PII 集合和自然人之间的联系。

注 2：**可直接关联的信息**：这类信息能够用于在信息和与信息有关的自然人之间建立直接的联系。简而言之，就是通过**这些**信息，可以明确地识别出特定的个人。例如：全名或姓名、身份证号码、联系方式（电话号码、电子邮件地址、邮寄地址、社交媒体账号、银行账户信息、生物识别信息、IP 地址、设备标识符、驾驶证信息、社保账号）。

注 3：**可能间接关联的信息**：除了直接可识别的信息外，PII 还包括那些虽然不直接包含个人身份标识，但通过与其他信息结合或经过一定分析后，仍然有可能识别出特定个人的信息。例如：出生日期、性别、职业、教育背景、居住区域、网络行为数据、位置数据、设备使用数据、健康数据、财务交易数据）。

3.2 个人敏感信息 sensitive PII

一类 PII，其性质敏感，如涉及 PII 主体最私密领域的信息，或对 PII 主体有重大影响的信息。

注：在某些司法管辖区或特定情况下，敏感 PII 是根据 PII 的性质来定义的，可能包括揭示种族血统、政治观点或宗教或其他信仰、健康状况、性生活或刑事定罪的个人数据，以及其他可被定义为敏感的个人信息。

3.3 PII 控制者 PII controller

确定处理个人身份信息（PII）的目的和方式的一个或多个隐私相关方，但不包括为个人目的而使用数据的自然人。

3.4 PII 主体 PII principal （数据主体 data subject）

与个人身份信息（PII）相关的自然人，即那些其信息被收集、处理、存储或传输的个人。

3.5 PII 处理者 PII processor

代表并按照 PII 控制者的指示处理 PII 的隐私利益相关方。

3.6 首席隐私官 Chief Privacy Officer (CPO)

负责保护组织内 PII 的高级管理员。

3.7 去(身份) 识别过程 de-identification process

使用去（身份）识别技术去除去一组（身份）识别数据和数据主体之间的关联的过程。

3.8 PII 的处理 processing of PII

对 PII 执行的操作或操作集。

注：PII 的处理操作的例子包括但不限于：收集、存储、更改、检索、咨询、披露、匿名化、假名化、传播或以其他方式提供、删除或销毁 PII。

4、认证基本原则

4.1 公正性：保持公正是提供第三方认证的必要条件。SWCC 通过申请评审、审核方案策划、现场审核与认证决定等过程控制，确保审核过程的公正、客观。

4.2 能力：能力是指经证实的应用知识和技能的本领。SWCC 通过审核人员管理机制，保障的人员能力是提供可建立信心的认证审核的必要条件。

4.3 责任：SWCC 基于获取的客观证据基础上进行审核和评价，并在此基础上做出认证决定。

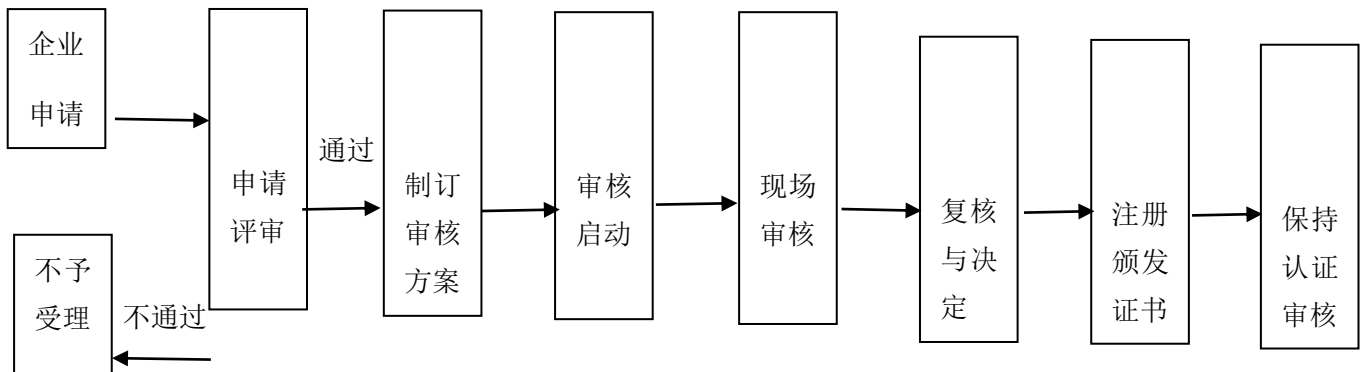
4.4 公开性：为确保诚信性与可信性，SWCC 采用透明运营的方式，公布有关认证审核过程和状态的适宜、及时的信息，或提供获取上述信息的公开渠道。

4.5 保密性：SWCC 采取措施对任何关于认证客户的专有信息予以保密（除书面授权或法律要求外），但 SWCC 享有获取充分评价认证审核符合性所需的信息的特别权利。

4.6 对投诉的回应：SWCC 确保依赖认证的各方相信，在投诉经查明有效时，SWCC 将对这些投诉进行适当的处理，并为解决这些投诉做出适当的努力。当投诉表明出现错误、疏忽或不合理行为时，对投诉做出有效回应是保护 SWCC 及客户和其他认证使用方的重要手段。

4.7 基于风险的方法：SWCC 考虑与提供有能力的、一致的和公正的认证相关的风险。基于风险的方法应对审核的策划、实施和报告具有实质性影响，以确保审核关注于对审核委托方重要的事项和对实现审核方案目标重要的事项。

5、认证基本流程



6、认证人员要求

6.1 总则

审核人员需取得 CCAA 信息安全管理体系（ISMS）注册审核员资质，并应具备信息安全管理体系审核及认证的能力。

6.2 认证人员能力要求

6.2.1 审核人员、复核审核报告和做出认证决定人员以及实施申请评审以确定所需的审核组能力、选择审核组成员并确定审核时间人员需具备表-1 的能力。

表-1 知识和技能表

知识	认证职能		
	实施申请评审以确定所需的审核组能力、选择审核组成员并确定审核时间	复核审核报告和做出认证决定	审核（包括组长）
业务管理实践知识			√
审核原则、实践和技巧的知识		√	√
特定管理体系标准和（或）规范性文件的知识	√	√	√
认证机构过程的知识	√	√	√
客户的业务领域的知识	√	√	√
客户的产品、过程和组织的知识	√		√
与客户组织中的各个层级相适应的语言技能			√
作记录和撰写报告的技能			√
表达技能			√
面谈技能			√
审核管理技能			√

6.2.2 PIIP 审核人员至少具备应用以下知识的技能：

- (1) 信息安全；
- (2) 与受审核的活动相关的技术；
- (3) 管理体系；
- (4) 审核原则；
- (5) PIIP 的监视、测量、分析和评价。

除（2）能在审核组成员之间共享外，以上（1）-（5）适用于审核组内的所有审核员。

审核组成员作为一个整体，应有与上述要求相适宜的技能。通过其应用经验能证实这些技能。



审核组成员作为一个整体，应有能力将客户 PIIP 中信息安全事件的迹象追溯到 PIIP 相应要素。

除上述要求以外，还应考虑以下内容。审核员应知晓和理解以下审核和 ISMS 方面的知识：

- 审核方案与策划；
- 审核类型和方法；
- 审核风险；
- 信息安全过程分析；
- 持续改进；
- 信息安全的内部审核。

审核员应知晓和理解以下方面的监管（法律法规）要求：

- 知识产权；
- 组织记录的内容、保护和保存；
- 数据保护和隐私；
- 密码控制规则；
- 电子商务；
- 电子签名和数字签名；
- 工作场所监控；
- 电信拦截（通信侦听）和监控数据（例如电子邮件）；
- 计算机滥用；
- 电子证据收集；
- 渗透试验；
- 国际的和国家的行业特定要求（例如，银行业）。

7、认证实施程序



7.1 认证申请

7.1.1 申请组织基本条件

(1) 具有明确的法律地位，申请方具有企业营业执照、事业单位法人证书、社会团体登记证书、非企业法人登记证书、党政机关设立文件等，可独立申请认证。其他类型的客户，应由具备资格的单位代为申请。如果申请方为组织的一部分（无独立的法人资格），应持有组织的授权证明等。

(2) 国家、地方或行业有要求时，申请方应具有规定的资质，并其申请认证范围应在法律地位文件和资质规定的范围内；申请的认证范围不能包括涉及国家安全和机密的内容和场所。

(3) 申请方在申请认证前一年内没有发生信息安全泄露事故或信息技术服务事故（包括已经或可能严重损害国家安全、社会秩序、公共利益或获证客户及其相关方的合法权益）或被执法监管部门责令停业整顿或在全国企业信用信息公示系统中被列入“严重违法企业名单”或违反国家相关法规，虚报、瞒报获证所需信息的情况。

(4) 申请方已经或正在按照相应的认证标准和其他规范的要求，建立了文件化的信息安全体系（含适用性声明），并初次认证现场审核前已至少持续稳定运行了 3 个月。申请方按规定实施了一次完整的内部审核和管理评审，没有发现重大的不足。

(5) 申请方委托认证范围涉及的产品、服务和信息安全体系等符合相关法律法规的要求；承诺始终遵守认证的有关规定，承担与认证有关的法律责任，并有义务协助认证监管部门的监督检查，对有关事项的询问和调查如实提供相关材料 and 信息。

(6) 申请方承诺获得 SWCC 认证后，按规定使用认证证书和认证标志和有关信息，不得擅自利用管理体系认证证书的文字、符号误导公众认为其产品或服务通过认证。按合同支付认证费用，并按规定接受监督。

(7) 申请方获得 SWCC 的认证后，需按照 SWCC 的规定，及时通报可能影响信息安全体系活动的能力和有效性的信息，例如：客户及相关方有重大投诉；产品或提供的服务被监管部门认定不合格；发生信息安全泄露事故或信息技术服务重大事故；相关情况发生变更（包括：法律地位、生产经营状况、组织状态或所有权变更、强制性认证或其他资质证书变更；法定代表人、最高管理者、生产经营或服务的工作场所变更；信息安全体系覆盖的活动范围变更；信息安全体系和重要过程的重大变更等）；出现影响信息安全体系运行的其他重要情况等。

(8) 认证审核期间，申请方能够提供与拟认证范围相关的产品/服务/活动现场

(9) 申请组织至少还需满足下列条件之一：

——获得了 SWCC 颁发的 ISMS 证书，且 ISMS 范围覆盖 PIIP 的范围；

——同时申请 ISMS 和 PIIP 的认证；

——组织已获得其他认证机构颁发的 ISMS 证书，并满足 ISMS 范围覆盖 PIIP 范围。

7.1.2 申请组织提供的基本信息

(1) 法律地位证明文件的复印件，包括：企业营业执照、组织机构代码证（如有）、事业单位法人证书、社会团体法人登记证、非企业法人登记证等；

注 1：若覆盖多场所活动，应附每个场所的法律地位证明文件以及中心职能机构与各分场所之间的法律或合作联系证明文件。

注 2：若申请方与受审核方不是同一组织，应提供双方相互关系的证明文件及受审核方接受审核的书面承诺。

(2) 与认证范围相关的法律法规许可证明文件的复印件。

(3) SWCC 为了确保认证的有效性，规避认证风险，暂不接受由其他认证机构颁发的现行有效的 PIIP 认证证书转为 SWCC 的认证证书，所有认证申请均按初次认证程序要求执行。

(4) 现行有效的文件化 PIIP 管理体系信息或管理制度（准则/标准/规范），例如：管理手册、程序文件或管理文件、适用性声明（SoA）、工艺/服务流程、PII 风险评估资料、认证范围与组织边界以及其他证实 PIIP 管理体系的资料。

注：提供的文件化信息必须为经批准的、已实施的、现行的有效版本。

(5) 与认证范围有关的过程和活动方面的重要信息：

a) 如实填报多场所信息，包括固定多场所、临时多场所、虚拟场所的数量和灾难恢复（DR）场所数量。

b) 外包方信息，包括外包从事的活动信息与控制程度。

c) 申请方总人员数以及与拟认证审核的体系控制下工作人数的差异性证明或说明资料, 包括在控制下工作的兼职人数、在认证范围内有较大比例从事某些相同的活动工作人数等。

d) 生产/服务提供方式, 如: 连续或季节性或其他方式; 生产经营活动的作息时间, 如: 全部类别工作人员常日班时间、轮班时间与信息等。

e) 拟审核审核场所限制信息, 并及时更新该限制信息, 如: ISMS 范围内的哪些信息资产不允许 SWCC 接触, 或者 SWCC 在接触相关信息资产时应满足哪些要求, 包括法律要求、相关方的要求和客户自身的要求。

注: 如果 SWCC 因为没有获得客户的允许或无法满足适用的要求而不能接触相关信息资产, 那么 SWCC 应对审核和认证所受到的影响进行评估并采取相应的措施 (例如终止审核、缩小审核和认证的范围等)。

f) 申请方如需认证人员身份背景以及相关保守秘密承诺时, 应予以说明, 以便 SWCC 判断其是否具备对该申请方实施认证活动的资格或条件。

g) 其他所需的资料与信息。

7.2 申请评审

7.2.1 应根据 SWCC 相关文件规定的等要求, 对申请组织提交的认证申请书及其相关资料进行评审并保存评审记录, 做出评审结论, 以确定:

- (1) 所需要的基本信息都得到提供;
- (2) SWCC 与申请组织之间任何已知的理解差异得到消除;
- (3) SWCC 有能力并能够实施认证活动;
- (4) 申请的认证范围、运作场所、完成审核需要的时间和任何其他影响认证活动的因素。

7.2.2 评审结果处理

(1) 提交的申请材料齐全并符合有关要求的、或经补充和完善申请资料并符合有关要求的, SWCC 将予以受理认证申请。

(2) 出现包括但不限于下列情况时，SWCC 将不予以受理组织认证客户的认证申请，并以书面的形式通知认证客户不予受理的理由：

- a) 组织提供的申请材料齐全或补充后仍未能符合有关要求的；
- b) 组织不具有明确的法律地位、或不满足相关法律法规要求、或为未取得相应行政许可文件；
- c) 组织被执法监督部门责令停业整顿或在全国企业信用信息系统中列入“严重违法企业名单”；
- d) 发生了信息安全泄露事故或隐私违规事件，反映出组织的信息安全体系建立及运行存在重大缺陷；

7.2.3 申请评审结论为受理后，SWCC 将与组织订立具有法律效力的书面认证合同，以明确双方的责任和义务。

7.3 认证范围

7.3.1 申请组织需明确 PIIP 管理体系的边界和适用性，以确定其范围。

注：认证证明文件（如证书）的范围与认证客户申请的拟认证范围可能有偏差，但最终遵循认证证明文件描述的范围和边界。

7.3.2 SWCC 应确保组织的 PII 安全风险评估和风险处置准确地体现其认证范围所界定的活动，并延伸到其活动的边界。SWCC 应确认这在组织的 PIIP 范围和适用性声明中得到了体现以及验证认证范围有适用性声明。

7.4 审核时间

7.4.1 SWCC 在本章节规定有关确定审核时间的最低要求和指南，以便在对客户涉及广泛的活动且具有不同规模和复杂度的 PIIP 范围实施认证时确定所需的时间，给予审核员足够的时间来开展与初次审核、监督审核或再认证审核相关的所有活动。总审核时间的计算，应包括报告审核情况所需的充足时间。

7.4.2 SWCC 针对每个客户及其被认证 PIIP，识别初始认证、监督审核和再认证审核所花费的审核时间。在审核策划阶段，按本章节要求使用一致的方法来确定适当的审核时间。此外，可以根据审核过程（尤其是第一阶段）的发现（例如，PIIP 范围的复杂度的不同评估结果，或范围内增加的场所）来调整审核时间。



7.4.3 PIIP 审核时间包括在客户场所的审核持续时间以及在现场以外实施策划、文件审查、与客户人员之间的相互活动和编写报告等活动的时间。

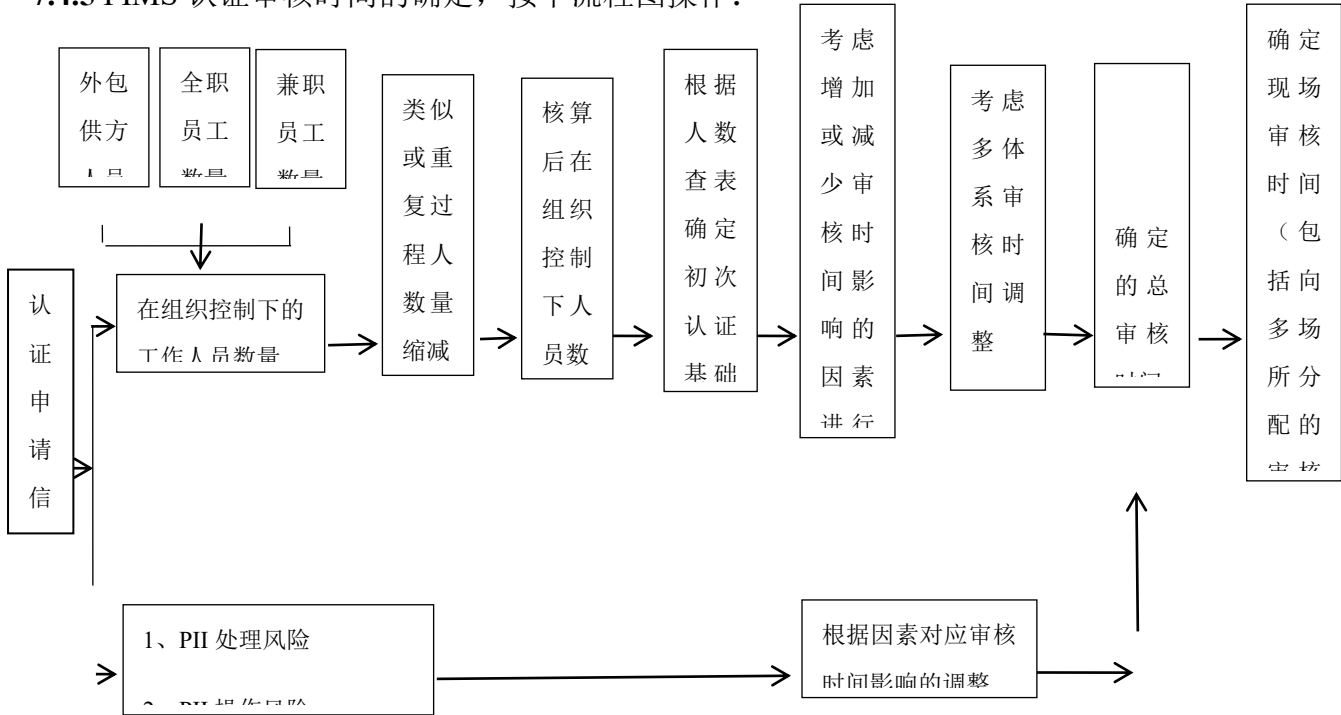
7.4.4 本章节与表-2 中所引用的“审核时间”，是根据审核中所花的“审核人天”来表示。审核人天的计算基于 8 小时工作日。

表-2 个人身份信息保护管理体系审核时间表（第一阶段+第二阶段）

有效人数	PIIP 初审审核天数	结合 ISMS 初次审核天数	结合 PIMS 初次审核天数	ISMS 认证后结合审核扩 展 PIIP +另加天数
1-10	3.5	5+1.5	6.5	2
11-15	3.5	6+1.5	6.5	2
16-25	4	7+2	6.5	2
26-45	4	8.5+2	7	2
46-65	4.5	10+2	8	2
66-85	4.5	11+2.5	9	2
86-125	5	12+2.5	10	2
126-175	5	13+2.5	11	2
176-275	5.5	14+3	12	3
276-425	6	15+3	12	3
426-625	6	16.5+3	14	3
626-875	7	17.5+3.5	15	3
876-1175	7	18.5+3.5	16	3
1176-1550	8	19.5+4	17	4
1551-2025	8	21+4	19	4
2026-2675	9	22+4.5	20	4
2676-3450	9	23+4.5	21	4
3451-4350	10	24+5	22	4
4351-5450	10	25+5	22	5

5451-6800	10	26+5	23	5
6801-8500	11	27+5.5	24	5
8501-10700	11	28+5.5	25	5
>10700	沿用以上规律	沿用以上规律	沿用以上规律	沿用以上规律

7.4.5 PIMS 认证审核时间的确定，按下流程图操作：



注：任何审核时间的减少，应在现场审核时间与总审核时间的比较之前进行。

7.4.6 在组织控制下的工作人员数量

在认证范围内，处于组织控制下工作的、所有班次工作的人员总数是确定审核时间的起点。

7.4.6.1 兼职人员：根据实际工作的小时数，兼职人员的数量可以减少或增加，并换算成等效的全职人员数量，可按照此公式进行核算：等效的全职人员数量=工作小时数/8 小时×兼职人员数量。

例如：30 名每天工作 4 小时的兼职人员，相当于 15 名全职人员。

7.4.6.2 倒班人员：如果组织运作的重要部分采用轮班制，且不同班次间活动的类型、环境影响和工作强度没有显著区别，则倒班的有效人数可用此方法折算：轮班的员工数量/（班数-1）



示例：某过程活动连续进行，共设置 3 班组，每个班组共有 12 人，按照早、中、晚进行轮班，则轮班的有效人员： $(12*3)/(3-1)=18$ 人。

7.4.7 审核时间调整的因素

表-2 审核时间表不得单独使用。分配的时间还应考虑与 PIIP 复杂性相关的因素，以及 PIIP 审核所需的工作的因素。这些可以包括但不限于：

- (1) PII 处理活动的复杂性；
- (2) PII 处理的控制措施数量；
- (3) PII 处理活动的数量；
- (4) 正在处理的 PII 的分类/类别；
- (5) 组织运营的地点/地理区域/司法管辖区的数量；
- (6) PII 的转移程度；
- (7) 处理/有关访问 PII 的人数；
- (8) PII 数据量（体量）；
- (9) 处理 PII 主要数据的平台数量。

注：下列 7.5 条款中提供了在计算审核时间时如何考虑这些不同因素的示例。

7.4.8 对审核时间偏离的限制

为了确保能够实施有效的审核并确保可靠和可比较的结果，对表-2 中审核时间的减少，不应超过 30%。

7.4.9 现场审核时间

策划和编制报告一起所用的时间，通常不宜使现场（物理/远程）审核时间减少到根据计算时间的规定要求计算的“总审核时间”70%以下。当策划和/或编制报告需要增加时间时，这不应成为减少现场审核时间的理由。

审核员旅途时间未计在内，这应在表-2 中所给出的审核时间的基础上另外增加。

7.4.10 监督审核时间

在初次认证审核周期，对一个组织的监督时间宜与初次审核时间成比例，每年用于监督审核的时间总量大约是初次审核时间的 1/3。宜时常评审所策划的监督审核时间，以考虑影响审核时间的变更。为审核 PIIP 的变更(例如，审核新的或变更的隐私控制、过程和服务)，应增加监督审核的时间。

7.4.11 再认证审核时间

用于再认证审核总的时间，应取决于 PIIP 审核特别要素和任何以往审核的结果。

再认证审核所需的时间，宜与同一组织的初次认证审核所用的时间成比例，宜至少是同一组织初次认证审核时间的 2/3。

7.4.12 多场所审核时间

通常，总的现场审核时间应考虑在组织控制下工作的人员总数，而不考虑人员所在的位置。

或者，基于形成文件的合理理由，允许每个场所单独计算审核时间进行汇总，只要总审核时间大于按人员总数计算的审核时间。

适用时，若某些审核内容与总部办公室或本地场所无关，则可以减少审核时间，则应记录此类减少的理由。

根据上述的规定要求为认证范围计算出总的现场审核人日；SWCC 可根据场所与因素安全管理体系的相关性、场所所展开的活动和所识别的风险，将总的现场审核人日分配到不同的场所，则应记录分配的理由。

SWCC 针对多场所的审核时间分配一般遵循以下要求：

——分配到多场所的审核人日不超过总的现场审核人日的 50%

——若另行需要增加多场所抽验以证实 PIMS 认证范围的有效性时，增加的每个场所的审核人日一般不超过 0.5 人天。

7.4.13 扩大范围的审核时间

扩大 PIMS 范围所需的审核时间应考虑到以下因素：

- (1) 扩大的类型；
- (2) 当前认证的活动；
- (3) 展开活动的地点的数量；
- (4) 与活动相关的隐私风险；
- (5) 与所扩范围相关的控制数量；
- (6) 所扩范围内，在组织控制下工作的人数；
- (7) 审查将所扩范围整合到 PIIP 时所需时间。

SWCC 为扩大范围的审核时间计算遵循下述要求：

- (1) 扩大 PIMS 范围所需的审核时间，应增加到审查客户获证 PIMS 所需的审核时间中。
- (2) 对于所扩范围的初次审核，审核时间应根据当前认证范围内增加的人员和场地的数量，使用上述规定的方法来计算。
- (3) 当扩大范围审核是结合监督审核或再认证审核进行时，应至少增加为 0.5 天（审核人日）；
- (4) 当扩大范围审核是单独进行时，相应的时间应至少为 1.0 天（审核人日）。

7.5 审核时间计算方法

本章节为推导出审核时间计算公式提供了进一步的指南。

下述 7.5.1 条款给出了一个对因数进行分类的示例，它可用作审核时间计算的基础。

下述 7.5.2 条款提供了一个审核时间计算的示例。

7.5.1 审核时间计算因素的分类

上述“7.4.7 审核时间调整的因素”条款中（1）-（9）所列举的，以及下表-1 给出对主要的审核时间计算因数进行分类的示例，SWCC 将使用该分类来计算审核时间。

表-3 计算审核时间的因素分类

因素（7.4.7）	高	中	低
PII 的分类	——PII 被认为是高度敏感	——PII 包括银行账户和财务信息、国家标识符（国民	PII 具有普遍性：



	性的； ——需要数据保护影响评估（DPIA）或类似流程； ——大量敏感/特殊类 PII	识别号）、弱势群体； ——大量的信息，包括一些特殊类别的数据，如人力资源数据； ——假名数据（能够反转为原始数据）	——公司一般 PII，包括一些与人力资源相关的 PII； ——PII 加密数据； ——去识别数据（无法以合理的方法反转原始数据）
PII 的转移	——将 PII 转移到不同的司法管辖区和地理区域	——PII 的转移通过约束性企业规则或其他机制进行控制	——在同一或管辖范围内/地区运行的相互关系规则中转移 PII ——用加密对 PII 转移
处理的复杂性	——商业用途的 PII 分析； ——数据挖掘 ——大量的法律和法规	——PII 分析用于自身目的； ——一些特定行业的法规	——一般处理
PII 处理数量	——多个处理需要使用不同平台	——多个处理使用相同平台	——1-2 简单处理使用相同平台
处理/能够访问 PII 的人数	——100%与认证范围内的组织相关人员	——50%-75%与认证范围内的组织相关人员	——<25%与认证范围内的组织相关人员
实施标准控制措施的数量	——实施所有控制措施	——实施 70%控制措施	——实施<30%控制措施
场所/地理位置/管辖区的数量	——多个地理位置/司法管辖区运营	——同一司法管辖区的多个场所运营	——单一场所
PII 主要数据量（记录）	——高数据量>10 亿	——中数据量>1 百万	——低数据量<1 万
其他因素	高	中	低
数据泄露的影响	——诉讼，高额罚款，损害声誉	——重大影响，包括赔偿、罚款、损害声誉	——影响较小，包括赔偿、罚款、损害声誉
在认证范围内处理 PII 的平台数量	——>100 ——PII 在许多平台上进行处理	——>50 ——PII 在几个平台上进行处理	——<50 ——PII 使用平均 1-5 平台进行处理

7.5.2 审核时间计算的示例

SWCC 按 7.4 中提供的因素来计算审计时间，并根据下列示例方法进行：

步骤 1：确定表-4 中与 PII 处理风险相关的因素，得出分值；

步骤 2：确定表-5 中与 PII 运营风险的相关因素，得出分值；

步骤 3：根据步骤 1 和步骤 2 的结果，在表-6 中选择适当条目，确定各因素对审核时间的影响；

步骤 4：最终计算：由表-2 确认的基础人日×步骤 3 中得出的系数。

当利用多场所抽样时，要根据执行多场所抽样计划所需的工作量增加所计算出的审核人天。

这个计算的结果为最终审核人天数。

表-4：PII 处理风险

PII 处理风险	审核时间计算分类		
	高/分值 3（任一项）	中/分值 2（任一项）	低/分值 1（任一项）
PII 的分类	<ul style="list-style-type: none"> —PII 被认为是高度敏感性的； —需要数据保护影响评估（DPIA）或类似流程； —大量敏感/特殊类 PII 	<ul style="list-style-type: none"> —PII 包括银行账户和财务信息、国家标识符（NI 号）、弱势群体； —大量的信息，包括一些特殊类别的数据，如人力资源数据； —假名数据（能够反转为原始数据） 	PII 具有普遍性： <ul style="list-style-type: none"> —公司一般 PII，包括一些与人力资源相关的 PII； —PII 加密数据； —去识别数据（无法以合理的方法反转原始数据）
PII 的转移	<ul style="list-style-type: none"> —将 PII 转移到不同的司法管辖区和地理区域 	<ul style="list-style-type: none"> —PII 的转移通过约束性企业规则或其他机制进行控制 	<ul style="list-style-type: none"> —在同一或管辖范围内/地区运行的相互关系规则中转移 PII —用加密对 PII 的转移
处理的复杂性	<ul style="list-style-type: none"> —商业用途的 PII 分析； —数据挖掘 —大量的法律和法规 —多个地理位置/司法管辖区运营 —多个处理需要使用不同平台 —自动化决策 	<ul style="list-style-type: none"> —PII 分析用于自身目的； —一些特定行业的法规 —同一司法管辖区的多个场所运营 —多个处理使用相同平台 	<ul style="list-style-type: none"> —一般处理 —单一场所 —1-2 简单处理使用相同平台

表-5：PII 运营风险

PII 运营风险	审核时间计算分类		
	高/分值 3（任一项）	中/分值 2（任一项）	低/分值 1（任一项）
处理/能够访问 PII 的人数	<ul style="list-style-type: none"> —100%与认证范围内的组织相关人员 	<ul style="list-style-type: none"> —50%-75%与认证范围内的组织相关人员 	<ul style="list-style-type: none"> —<25%与认证范围内的组织相关人员
实施标准附录 A 控制措施的数量	<ul style="list-style-type: none"> —实施所有控制措施 	<ul style="list-style-type: none"> —实施 70%控制措施 	<ul style="list-style-type: none"> —实施<30%控制措施

PII 主要数据量 (记录)	——高数据量>10 亿	——中数据量>1 百万	——低数据量<1 万
	——多个数据集	——一些数据集	——1-2 个数据集

表-6 因素对审核时间的影响

		PII 处理风险		
		低 (3-4)	中 (5-6)	高 (7-9)
PII 运营风险	高 (7-9)	+ 5%~20%	+ 10%~50%	+ 20%~100%
	中 (5-6)	- 5%~10%	0%	+ 10%~50%
	低 (3-4)	- 10%~30%	- 5%~10%	+ 5%~20%

示例：受审核的组织有 100 人，因此根据表-2 其初次认证审核时间需要 5 人天。该组织 PII 处理风险为中、PII 运营风险也为中，利用表-6 可以得出该审核时间无需调整（0%），最终审核时间为 5 人天。

7.6 建立审核方案

7.6.1 方案的策划

在认证审核之前，SWCC 要求受审核方为调阅内部审核报告和信息安全独立评审报告做出所有的必要安排，并要求受审核方报告是否存在因包含保密信息或敏感信息而导致不能提供给审核组审查的 PIIP 相关信息（例如，PIIP 记录或关于控制的设计与有效性的信息）。

SWCC 将确定是否能在缺少这些信息的情况下对 PIIP 进行充分审核，如果结论是若不审查已识别的保密信息或敏感信息就不能对 PIIP 进行充分地审核，那么则告知受审核方只有在适当的访问安排获得许可后才能进行认证审核。

审核方案包括两个阶段的初次审核、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。认证周期的审核方案覆盖全部的管理体系要求。保持审核方案策划的文件化信息。

7.6.2 审核周期与方式

(1) 受审核方只有有充分的证据证实覆盖认证范围的管理评审和 PIIP 内部审核的安排已经实施、是有效的并将得到保持，SWCC 才能其的 PIIP 实施认证。



(2) SWCC 与受审核方商定一个能够最佳地证实其 PIIP 全部范围的审核时间。适当时，考虑因素包括季度、月份、日期和班次。

(3) SWCC 针对受审核方的审核一般采用现场审核的方式，在特定的情况下可采用“远程审核”。

(4) SWCC 针对受审核方实施远程审核遵循相关文件的要求。

注 1：如果利用交互式网络协作、网络会议、电话会议和/或组织流程的电子验证等远程审核方法与组织进行交互，则应在审核计划中确定这些活动的安排，并可将其视为总的“现场审核时间”的一部分。

注 2：现场审核时间是指为各个场所分配的现场审核时间。远程场所的电子审核被认为是远程审核，即使电子审核是在组织的场所进行的。

7.6.3 确定审核时间

(1) SWCC 相关人员根据上述 7.4 条款的要求确定现场审核的时间，对场所的审核时间根据其业务与 PII 的复杂性，合理安排审核时间，并应记录管理体系审核的时间及其合理性。没有被指派为审核的审核组成员（即技术专家、翻译人员、观察员和实习审核员）所花费的时间不应计入上面所确定的审核时间。

注：使用翻译人员可能需要额外增加审核时间。

(2) PIIP 审核时间包括在客户场所的审核持续时间以及在现场以外实施策划、文件审查、与客户人员之间的相互活动和编写报告等活动的时间。

(3) 审核报告、审核计划或与客户沟通等的时间不应超过审核时间的 30%。

7.6.4 多场所抽样

当受审核方拥有满足以下(1)至(3)的多个场所时，SWCC 可以考虑使用基于抽样的方法进行多场所认证审核：

(1) 所有的场所在同一个 PIIP 下运行且该 PIIP 实行集中统一的管理、审核和管理评审；

(2) 所有的场所都包含在受审核方的 PIIP 内部审核方案中；



(3) 所有的场所都包含在受审核方的 PIIP 管理评审方案中。

SWCC 在使用基于抽样的方法时应确保：

(1) 在初次的合同评审时，最大程度地识别场所之间的差异，以便确定适当的抽样水平；

(2) 结合以下因素，抽取具有代表性的场所：

- 总部（适宜时）及各场所的内部审核结果；
- 管理评审的结果；
- 场所规模的差异；
- 场所业务范围的差异；
- 不同场所信息系统的复杂程度；
- 工作实践的差异；
- 所开展活动的差异；
- 控制的设计与运行的差异；
- 与关键信息系统或处理敏感信息的信息系统之间的潜在交互；
- 任何不同的法律要求；
- 地域因素和文化因素；
- 场所的风险状况；
- 特定场所发生的隐私信息事件。

(3) 从受审核方 PIIP 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 (2) 中所列因素的判定，同时也考虑随机因素；

(4) 在授予认证之前，SWCC 审核了 PIIP 中每个具有重大风险的场所；

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

(6) 在单个场所发现不符合时，纠正措施程序的实施适用于证书所覆盖的所有场所。



SWCC 的审核人员应关注受审核方为确保单一的 PIIP 适用于所有场所并在运行层面实施统一管理所进行的活动，并应关注上述所有事项。

SWCC 保持关于初次、监督和再认证审核中抽样现场的选择的理由和方法的文件化信息。

7.6.5 选择审核组成员

方案管理人员选择审核组应考虑在规定的范围内实现每次审核目标所需的能力。如果只有一名审核员，该审核员应履行审核组长的所有适用职责。审核组成员具有实际的隐私工作经验和 ISMS 审核能力的审核员。在确定具体审核的审核组规模和组成时，应考虑以下事项：

- 考虑到审核范围和准则，实现审核目标所需的审核组整体能力；
- 审核的复杂程度；
- 审核是否是多体系审核或联合审核；
- 所选择的审核方法；
- 避免审核过程中的任何利益冲突，确保客观性和公正性；
- 审核组成员工作能力以及与受审核方代表和有关相关方互动的能力；
- 相关的外部/内部因素，如审核语言，以及受审核方的社会和文化特性，这些因素可以通过审核员自身的技能或通过技术专家的支持予以解决，同时考虑到对翻译的需求；
- 拟审核的过程的类型和复杂程度。

注：如果审核组中的审核员没有具备必要的能力，应使用具有相关能力的技术专家来支持审核组。审核组可以包括实习审核员，但实习审核员应在审核员的指导和帮助下参与审核。

(2) 方案管理人员应委派具有能力的审核员担任审核组长，并负责领导审核组实施审核工作，包括制定审核计划、召开会议、实施审核及编制报告等。委派的一阶段审核组长与二阶段审核组长宜为同一人。

审核组长与审核组协商后，应将审核具体过程、活动、职能或地点的职责，分配给每个成员，

适当时分配决策权。此项分配应兼顾公正性、客观性和审核员能力以及资源的有效利用，以及审核员、实习审核员和技术专家的不同角色和职责。审核组长应召开审核组会议，以分配工作任务并决定可能的变更。在审核进程中，为确保实现审核目的，可以改变工作分配。

(3) 在审核期间，可能需要改变审核组的组成，例如，如果出现利益冲突或能力问题。当出现这种情况，应在做出任何改变前，与适当的各方（审核组长、方案管理人员、受审核方、认证机构）解决该问题。

(4) 审核组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。

(5) 实习审核员可以参与审核，此时要指派一名审核员作为评价人员。审核组成员中实习审核员数量不宜超过审核员数量并不超过 2 名。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。

注：结合审核或一体化审核的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。

7.7 审核启动

7.7.1 与受审核方建立联系

(1) 方案管理人员根据策划的要求，将确定的审核日期以及相关的信息的审核任务告知受审核方和审核组。征求受审核方及审核组成员的意见，以避免利益冲突。如果受审核方反对审核组或审核组成员，声明有利益冲突，应立即调整审核组成员。

(2) 实施审核的责任应该由指定的审核组长承担，直到审核完成。实施审核前审核组长应与受审核方进行联系，确定审核的可行性，为审核目标的实现提供合理的信心：

- 确认受审核方代表的沟通渠道；
- 确认进行审核的权限；
- 提供有关审核目标、范围、准则、方法和审核组组成的相关信息；

- 请求获得用于策划的目的的相关信息，包括关于受审核方已确定的风险和机遇以及如何应对这些风险和机遇的信息；
- 确定适用的法律法规要求以及与受审核方的活动、过程、产品和服务有关的其他要求；
- 确认与受审核方关于保密信息披露的程度或处理的协议；
- 确认对审核进行安排的计划，包括日程表；
- 确定任何特定地点的访问、健康和安全、防护、保密等安排；
- 确认同意观察员的出席及审核组对向导或翻译人员的需求；
- 确定与具体审核有关的受审核方利益、关注或风险的任何领域；
- 解决审核组与受审核方或审核委托方的组成问题。

当审核不可行时，审核组长应向方案管理人员提出替代方案并与受审核方协商一致。

7.7.2 审核活动的准备

7.7.2.1 实施文件评审

(1) 审核组长组应对申请组织提交的文件和资料实施文件评审，并形成文件评审报告。

——收集信息了解受审核方运行情况，准备审核活动和适用的审核工作文件，例如过程、职能；

——建立成文信息的范围的概览，以确定是否符合审核准则，并发现可能存在的问题，如缺陷、遗漏或冲突。

(2) 成文信息应包括但不限于：管理体系文件和记录，以及以前的审核报告。评审应考虑受审核方组织的范围，包括其规模、性质和复杂性，以及相关风险和机遇。它还应考虑审核范围、准则和目标。

(3) 当文件评审不满足要求时，审核组长需通知申请组织补充提供相关信息和文件资料。

(4) 文件评审通过后，可安排现场审核；文件评审的结果应予以保持并提交申请组织。

7.7.2.2 审核计划

(1) 审核组长应在现场审核之前，与受审核方就审核计划的事宜进行充分沟通，确保双方在理

解上没有歧义，并应考虑所确定的信息安全控制。审核组应结合文件评审的结果、审核覆盖的范围等信息，对现场审核做出具体安排，包括但不限于具体的时间安排、审核组成员对受审核方按岗位和活动以何种方式进行评价的安排、高层沟通的安排和会议的安排。

(2) 审核计划应具有充分的灵活性，以允许随着审核活动的进展而进行必要的调整。审核计划应包括或涉及以下内容：

——审核目标；

——审核范围，包括组织及其职能的识别，以及受审核的过程；

——审核准则和引用的成文信息；

——拟实施审核活动的位置、日期、预期时间和持续时间，包括与受审核方管理者的会议；

——审核组对熟悉受审核方的设施和需求的需求，例如，通过实地考察或评审信息和通信技术（ICT），并需描述用于协助远程审核的工具；

——拟采用的审核方法，包括为了获得足够的审核证据需要进行审核抽样的程度；

——审核组成员以及向导和观察员或翻译人员的角色和职责；

——在考虑与拟审核的活动有关的风险和机遇的基础上配置适当的资源。

适当时，审核计划还应考虑：

——明确受审核方本次审核的代表；

——审核工作和审核报告所用的语言；

——审核报告的主题；

——后勤和沟通安排，包括对受审核地点的具体安排；

——为应对实现审核目标的风险和产生的机遇而采取的任何具体行动；

——与保密和信息安全有关的事项；来自以往审核或其他来源的任何后续行动；

——对所策划的审核的任何后续活动；

——在联合审核的情况下，与其他审核活动的协调。

审核计划的任何问题应当在审核组长、受审核方和(如有必要)审核方案管理人员之间解决。

(3) 多场所审核时, 审核计划还应考虑:

——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;

——分派的具有能力的审核组。

7.8 初次认证审核

初次认证审核分两个阶段实施: 第一阶段和第二阶段。

7.8.1 第一阶段审核

(1) 方案管理人员根据拟认证组织的特点、规模和复杂程度, 合理策划和确定第一阶段审核时间, 通常情况下, 第一阶段现场审核所需的审核时间宜为 1-2 个审核人日; 对于 PIIP 控制下工作人员少、业务和 PII 复杂性低的受审核方, 可降低至 0.5 人日。

(2) 第一阶段审核目的是为了了解受审核方的 PIMS 建立和运行的情况, 并确认是否做好了认证审核阶段的准备。为实现此目的审核组应对受审核方开展一阶段现场审核, 审核内容应包括:

——审查客户的文件化的 PIIP 信息, 包括 ISO/IEC 27001 要求的 ISMS 文件等;

——客户 PIIP 认证范围和边界的确认, 包括 PIIP 和其所覆盖活动的一般信息;

——确认 PIIP 受审核方控制下的工作人员、业务与 PII 处理风险、PII 运营风险、轮班信息等, 以便评估和重新确定审核时间;

——评价客户组织的运作场所和现场的具体情况, 并与申请组织的人员进行讨论, 以确定第二阶段审核的准备情况;

——审查客户现场审核的资源保障情况, 并与其商定第二阶段的细节;

——评价客户是否策划和实施了内部审核与管理评审, 以及 PIIP 的实施程度能否证明客户已为

第二阶段做好准备；

——结合客户 PIIP 标准或其他规范性文件充分了解其的管理体系和现场运作，以便为策划第二阶段提供关注点。

(3) 审核组应将第一阶段审核发现形成报告，包括文件评审报告，识别任何引起关注的、在第二阶段审核中可能被判定为不符合的问题。

(4) 审核组应充分了解受审核方的 PIIP 的设计，包括风险评估与风险处置（包括所确定的控制）、隐私方针和目标等，特别是应充分了解受审核方的审核准备情况，以便将所了解的信息应用于策划第二阶段。

(5) 在确定第一阶段和第二阶段的间隔时间时，将考虑受审核方解决第一阶段识别的任何需关注问题所需的时间。SWCC 也可能需要调整第二阶段的安排。如果发生任何将影响 PIMS 的重要变更，SWCC 将考虑是否有必要重复整个或部分第一阶段。告知受审核方户第一阶段的结果有可能导致推迟或取消第二阶段。

注：如第一阶段中所发现的合规性问题，在其纠正措施得到确认后，方可进入二阶段审核。

(6) 第一阶段审核后的 6 个月内没有完成第二阶段的审核，将重新实施第一阶段审核。

(7) 在决定进行第二阶段之前，SWCC 将审查第一阶段的审核报告，以便为第二阶段选择具备所需能力的审核组成员。如果第一阶段的审核组长具备能力且适宜时，可由其来实施该审查。

注：由未参与审核的 SWCC 人员来审查报告、做出实施第二阶段的决定和确认实施第二阶段的审核组能力，能在一定程度上降低所涉及的风险。然而，其他降低风险的措施也能达到同样的目的。

(8) SWCC 让受审核方知晓在第二阶段可以要求对其他类型的信息和记录进行详细检查。

7.8.2 第二阶段审核

(1) 第二阶段现场评价的目的是在受审核方的现场全面收集审核证据，以判断其 PIIP 建立与实施是否符合 ISO/IEC 29151 的规定，并确定是否推荐认证注册。

(2) 第二阶段应在受审核方现场审核。方案管理人员应根据第一阶段审核发现调整或确定第二阶段方案，确保审核组长依据第一阶段的审核结果制订第二阶段的审核计划。

(3) 第二阶段现场审核除评价受审核方 PIMS 的有效实施外, 还包括确认其遵守自身的策略、目标和规程。为此, 审核应重点关注受审核方的以下方面:

——最高管理层对隐私目标的领导和承诺;

——隐私风险评估, 包括确保在重复实施风险评估时能产生一致的、有效的和可比较的结果;

——根据隐私风险评估和风险处置过程来确定控制;

——隐私绩效和 PIIIP 有效性, 包括根据隐私目标对其实施评价;

——所确定的控制、适用性声明、隐私风险评估结果、风险处置过程与隐私方针和目标之间的对应关系;

——控制的实现: 审核应考虑外部环境、内部环境、相关风险以及组织对隐私安全过程和控制的监视、测量与分析过程, 并确定待实现的控制是否已经实现且有效;

——方案、过程、规程、记录、内部审核和对 PIIIP 有效性的评审, 且这些都能追溯到最高管理层的决定、隐私方针和目标。

7.8.3 现场审核准备

(1) 现场审核组应做好准备工作, 明确审核任务重点、组内人员分工、审核范围和路线, 准备审核所需要的装备, 如现场核查清单、交通工具、通信器材、录音录像器材、现场采样器材等。

(2) 现场审核组根据文件评审结果、受审核方业务与 PII 复杂度、场所的数量和灾难恢复场所的数量、计划的抽样数量等因素, 策划现场审核的方案以及受审核方准备材料清单。

7.8.4 审核活动的实施

7.8.4.1 向导和观察员的作用和职责的分配

如有需要, 向导和观察员获得审核组长、审核委托方或受审核方的批准, 可陪同审核组。

向导和观察员不得影响或干扰审核工作的进行。如果不能保证这一点, 审核组组长应有权拒绝观察员出席某些审核活动。

对于观察员来说, 关于访问、健康和安、环境、防护和保密的任何安排应受审核委托方和受



审核方的管理。

由受审核方指定的向导应协助审核组，并应审核组长或被指派的审核员的要求采取行动。他们的责任应包括：

- 协助审核员识别参加面试的人员以及确认时间和地点；
- 安排访问受审核方的特定地点；
- 确保审核组成员和观察员了解和遵守关于访问、健康和安全、环境、防护、保密和其他问题的特定地点安排的规则，并处理任何风险；
- 在适当情况下，代表受审核方见证审核；
- 在需要时提供澄清或协助收集信息。

7.8.4.2 举行首次会议

审核组应与受审核方的管理层举行一次正式的首次会议，如有必要应包括负责拟审核部门或过程的人员，并记录与会人员。首次会议应由审核小组组长主持，其目的是简单说明审核活动将如何开展，并应包括下列信息：

- 介绍参与人员，包括简介其角色；
- 确认审核范围；
- 与受审核方确认审核计划，任何变化以及其他相关安排，如末次会议的日期和时间、审核小组和受审核方管理层之间的临时会议；
- 确认审核小组和受审核方之间的正式沟通渠道；
- 确认具备审核小组所需的资源和设施；
- 确认有关保密及信息安全的事宜；
- 审核组的关于访问、健康和安全、防护、紧急情况和其他的安排；
- 确认陪同人员和观察员，其角色和职责；
- 报告审核结果的方法，包括声明信息披露；

- 审核可能提前终止的情况；
- 审核组长及审核小组对审核负责，且应控制审核计划的执行，包括审核活动和审核线索；
- 如适用，确认前次审核发现的状态；能够影响审核工作进行的现场活动；
- 根据抽样进行审核所需使用的方法和过程；
- 确认审核中使用的语言；
- 确认在审核中，将会向受审核方及时通报审核进度及任何关注的问题；
- 受审核方提问的机会。

7.8.4.3 审核中的沟通

(1) 在审核期间，可能有必要对审核组内部以及审核组与受审核方、审核方案管理人员、可能的的外部相关方（如监管部门）之间的沟通作出正式安排，特别是法律法规要求强制性报告不符合项的情况。

(2) 审核组在审核期间应定期讨论，以交换信息，评估审核进度，以及需要时重新分配审核组成员的工作。在审核中，适当时，审核组长应定期向受审核方和审核方案管理人员沟通进度、重要审核发现和任何关注。如果收集的证据表明存在紧急和重大的风险，应当立即报告给受审核方，适当时报告给审核方案管理人员。

(3) 对于超出审核范围之外的引起关注的问题，应予以记录并向审核组长报告，以便与审核方案管理人员和受审核方进行可能的沟通。

(4) 当获得的审核证据表明无法实现审核目标时，或显示存在紧急和重大的事件、事故，例如安全风险、突发的生产过程事故。审核组长应与审核方案管理人员取得联系,并同受审核方商量确定补救措施或终止审核。补救措施可以考虑以下方式：

- 重新安排；
- 修改审核计划，对存在重大不符合项的相关区域另外安排时间跟踪审核；
- 改变审核目的及审核范围。



(5) 当现场审核时, 出现人数、名称、地址等或/及审核范围(包括场所边界)变更, 审核组长负责与审核方案管理人员取得联系并填写变更专用表单, 由受审核方签字确认后传回给 SWCC 进行评审。审核方案管理人员负责变更的评审, 对于认证业务范围等的变更应确定下述事宜后决定应采取的措施:

——认证范围的变更: 审核组成员专业能力、审核的业务范围、征求受审核方的意见。

——场所边界等的变更: 审核人日的变更、审核计划的调整、征求受审核方的意见。

(6) 审核组内沟通在确定构成不符合项时, 应经审核组长确认同意后; 当就不符合项产生争议时, 审核员现场应服从审核组长安排。事后可将该争议提报 SWCC 裁定。

(7) 当与受审核方就不符合项发生分歧时, 审核组应首先虚心听取其的解释, 不可武断或以自己以往的经验要求客户, 应努力以适当的、富有建设性、专业的方式解决与客户之间的分歧; 如受审核方的解释合理, 应取消发生争议的不符合项。如争议无法解决, 应向受审核方解释 SWCC 有关的处理途径或方法。

(8) 若审核组内部或与受审核方之间发生无法处理或协调的异常/突发事件, 审核组长应立即上报 SWCC。

7.8.4.4 收集和验证信息

(1) 现场审核应通过现场观察、询问及内外部相关资料的查阅、数据的收集分析等方式实施。审核组成员应在其承担的审核工作内, 根据审核计划使用抽样的方式进行信息的收集, 信息的来源, 包括但不限于:

——与员工和其他人员的交谈;

——对活动、周围工作环境和条件的观察;

——文件, 如方针、目标指标、程序、标准、指导书/规范、图样、合同、营业执照、许可证等;

——抽样方案的信息、抽样和测量过程的信息

——其他方面的报告, 如: 相关方的反馈等;

——数据库和网站;



——记录。

(2) 所有审核记录包括从申请、合同评审、任务书、审核计划、两个阶段的审核报告等所有与审核相关的记录和文件，均应规定的要求予以保留（原件或电子文档）。

(3) 现场审核记录使用的文字为中文，特殊情况下，经批准可使用外文。审核记录应体现审核证据（如人/物证、记录、具有可追溯的抽样、面谈人员姓名等）。需记录具体的不符合和支持的审核证据；符合要求和支持的审核证据的记录应简明扼要，具有可追溯性。

7.8.4.5 审核发现和不符合项

(1) 审核组应对照审核准则评价审核证据以确定审核发现。具体的审核发现应包括不符合项和良好实践以及他们的支持证据、改进机会和对受审核方提出的任何建议。

(2) 对于审核中发现的不符合时，应出具书面不符合和支持不符合的审核证据以及不符合的分级（严重不符合、轻微或一般不符合），与受审核方一起评审不符合，以确认审核发现是否正确，并使受审核方理解不符合。应尽一切努力解决与审核证据或调查结果有关的任何分歧意见。未解决的问题应记录在审核报告中。

(3) 对于审核中发现的不符合，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。审核组将对受审核方所采取的纠正和纠正措施及其结果的有效性进行验证，记录所取得的为不符合的解决提供支持的证据，并将验证的结果告知受审核方。

(4) 如果为了验证纠正和纠正措施的有效性，将需要补充一次全面的或有限的审核（跟踪审核），或者需要文件化的证据（需要在未来的审核中确认），则应告知受审核方。

(5) 受审核方的不符合关闭未在上述期限内完成、或不符合的整改经验证不满足要求、或经后续的现场跟踪访问不符合仍不符合要求的，则审核将被视为无效。

7.8.4.6 确定审核结论

(1) 审核组应在末次会议之前举行组内会议，充分讨论和评审审核发现与审核期间收集的任何其他适当信息，就审核过程中固有的不确定因素对审核结论达成组内的一致性意见，提出相应的推荐建议，如：推荐注册/保持注册/再认证注册、不推荐注册等。

◆推荐注册/保持注册/再认证注册



当审核没有发现严重不符合或发现 2 个以下非合法性的不符合，或发现轻微不符合，或没有不符合时，均已采取了纠正措施并经验证符合要求后，初次认证和再认证时，推荐注册；监审时，推荐保持注册。

◆不推荐注册

当存在可能导致系统失效的 2 个以上严重不符合项，且在规定时间内无法完成有效的纠正措施时，或存在与隐私信息相关的严重违法违规行为时。

注 1：推荐证书暂停：年审时，严重不符合项未能在规定时间内关闭，则暂停证书。

注 2：推荐撤销证书：证书暂停后的规定时间内仍未对验证不符合项采取有效的纠正措施。

(2) 审核组达成一致的审核结论应陈述受审核方 PIIP 与审核准则的符合程度和其良好实践，PIIP 有效实施、保持与改进的能力，审核目标的实现情况、审核范围的覆盖情况和审核准则的履行情况等，以及提出改进的建议或今后审核活动的建议。

7.8.4.7 举行末次会议

(1) 审核组应召开正式的有受审核方的管理者出席的末次会议，并记录参加人员。末次会议由审核组长主持，会议目的是提出审核结论，包括关于认证的推荐性意见。不符合应以使受审核方“被理解”的方式提出，并应就回应的时间表达达成一致。

注：“被理解”不一定意味着客户已经接受了不符合。

(2) 末次会议还应向受审核方说明下列内容：

——告知所收集的审核证据是基于可获得的信息样本，并且不一定充分代表受审核方过程的总体有效性；

——进行报告的方法和时间表，包括审核发现的任何分级；

——以受审核方管理者理解和承认的方式提出审核发现和结论；

——受审核方对审核中识别的任何不符合项提出纠正和纠正措施的时间安排；

——受审核方未充分处置审核发现的可能后果；

——SWCC 处理不符合项的过程，包括任何与受审核方证书相关的结果；

- 任何相关的审核后续活动（例如：实施和评审纠正措施，处理审核投诉、申诉的程序）；
- 保密声明；
- 获证后，受审核方的证书和标识使用说明；
- 获证后，受审核方任何与管理体系有关变更的信息通过与履行认证协议实施监督审核；
- 获证后，受审核方配合行政监督检查的义务等。

（3）末次会议应给受审核方提问和澄清的机会。关于审核组和受审核方之间的审核发现或结论的任何分歧意见都应当讨论，如果可能的话应当予以解决。如果没有解决，应该被记录下来。

7.8.5 终止审核（发生时）

发生以下情况时，审核组应终止审核，并及时向 SWCC 报告。

- （1）组织对审核活动不予配合，导致审核活动已无法进行。
- （2）组织管理体系有重大缺陷，不符合 PIIP 标准的要求。
- （3）发现组织存在重大隐私安全问题或有其他严重违法违规行为。
- （4）其他导致审核程序无法完成的情况（如：体系运行不满 3 个月、经营活动不能正常运行、未获得相应许可等）。
- （5）发生不可抗力事件或其他相关原因，导致审核活动已无法进行。

7.8.6 跟踪/补充审核（需要时）

- （1）在认证周期的任何阶段（第二阶段、监督和再认证），如需要现场验证主要不符合项或多个次要不符合项的纠正措施结果，审核组长应告知受审核方需进行额外的跟踪审核。
- （2）如果投诉不能远程解决或投诉的重要程度要求在下一计划审核前解决，也可安排临时通知访问。临时通知访问也可在受审核方证书暂停后进行。这些审核的过程与任何一般审核相同，其范围将针对投诉调查或决定是否可以解除暂停。
- （3）如果进行跟踪审核，SWCC 将与受审核方安排日期，同时与审核组长商定一位最适合进行现场跟踪审核的审核员。



7.8.7 审核报告

(1) 在验证可接受的不符合整改证据后，审核组长应编制审核报告提交给受审核方。审核报告应提供完整、准确、简洁和明确的审核记录，并应包括或引用下列内容：

- a) 审核目标；
- b) 审核范围，特别是明确受审核的组织（受审核方）及其职能或过程；
- c) 明确审核委托方；
- d) 明确审核组和受审核方参与者；
- e) 进行审核活动的日期和地点；
- f) 审核准则；
- g) 审核发现和相关证据；
- h) 审核结论；
- i) 隐私风险分析的审核情况说明；受审核方所使用的任何隐私控制措施集；
- j) 审核组与受审核方之间未解决的分歧意见；
- k) 审核本质上是一种抽样活动；因此，存在被查验的审核证据不具代表性的风险。

适当时，审核报告还可包括或引用以下内容：

——包括日程安排的审核计划；如果使用了远程审核方法，应说明远程审核方法在审核中的使用程度及其实现审核目标的有效性。当受审核方的活动不是在明确的物理位置实施的，而是其所有活动都是远程实施的时，审核报告应说明组织所有活动都是远程实施的。

——审核过程综述，包括遇到可能降低审核结论可靠性的障碍；

——确认在审核范围内，已按审核计划达到审核目标；

——审核范围内未覆盖的领域，包括任何任何证据可获得性、资源或保密问题，并附有相关解释理由；

——审核结论综述和支持审核结论的主要审核发现，包含有关审核中所评价的样本的信息；



- 概述关于 PIIP 要求和隐私信息控制的实现与有效性的最重要评论意见（正面和负面的）；
- 对适用声明（SoA）版本引用，以及在适用的情况下，与之前认证审核结果任何有用比较；
- 受审核方采用的内部组织和规程的充分性，以增强对 PIIP 的信心；
- 商定的后续行动计划（如果有）；
- 关于内容保密性质的陈述；
- 对审核方案或后续审核的影响。

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

7.9 认证决定

(1) 经批准或授权的认证决定人员（小组）认证决定的流程和管理文件的规定对申请组织的认证实施复核和决定。

(2) 认证注册要求

认证决定人员实施认证决定时应根据认证过程中收集的信息和其他相关信息，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。在做出认证的決定前，将对下列方面进行有效的审查：

- 审核组提供的信息足以确定认证要求的满足情况和认证范围；
- 对于所有严重不符合，SWCC 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，SWCC 已审查和接受了客户对纠正和纠正措施的计划。

(3) 认证决定结论

- 同意认证注册，颁发认证证书；
- 补充认证决定所需的信息（包括但不限于申请材料、审核材料）再行决定；
- 不同意认证注册，并将理由通知申请组织。

注：最终注册的认证范围以现场审核和认证决定的意见为准。



8、认证证书

8.1 PIMS 初始认证证书有效期为 3 年。证书到期后如获证客户要求继续使用认证证书，应在证书有效期内接受再认证。

8.2 证证书应使用 SWCC 的标准证书模版，至少应包含下列内容：

(1) 证书名称：个人身份信息保护管理体系认证证书

(2) 获证客户的名称和地理位置（或多场所认证范围内总部和所有场所的地理位置）；

(3) 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认证决定的日期；

注：当证书失效一段时间时，本机构在满足下列条件时，可以在证书上保留原始的认证日期：

——清晰标示了当前认证周期的开始时间和截止时间；

——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。

(4) 认证有效期或与认证周期一致的应进行再认证的日期；

(5) 唯一的识别代码；

(6) 审核获证客户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）；

(7) 与活动、产品和服务类型等相关的认证范围，适用时，包括每个场所相应的认证范围，且没有误导或歧义；

注：如果认证范围内的组织在指定的物理地点没有任何活动，那么认证文件应声明该组织的所有活动都是远程进行的。

(8) 获证客户 PIIP 的适用性声明（SoA）版本；

注：适用性声明的变更，如果不对认证范围内的控制措施覆盖范围产生影响，则不需要更新认证文件。

(9) SWCC 的名称、地址和认证标志；可以使用其他标识（如认可标识、客户的徽标），但不能产生误导或含混不清；

- (10) 认证用标准和（或）其他规范性文件所要求的任何其他信息；
- (11) 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；
- (12) 其他为了说明证书有效性的其他信息，包括证书信息公开、查询途径等。

示例：监督审核的相关要求以及监督审核后证书必须与年度确认书一起使用方可有效；证书查询途径等。

8.3 多场所组织证书

- (1) 认证证书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）。
- (2) 认证证书应包含所有场所的名称和地址，反映出组织与认证证书相关。范围或认证证书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，认证证书应包括该场所的子范围。当在认证证书上展示临时场所时，应注明这些场所为临时场所。
- (3) 如果向一个场所颁发认证证书，其中应包括：
 - 管理体系针对被认证的整个组织；
 - 该认证所覆盖对特定场所、法律实体的活动；
 - 与主证书之间的可追溯性，如：编号/代码；
 - 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证书，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、活动符合标准和规范文件的声明。

- (4) 当任一场所不能满足保持认证的必要规定，认证证书将被整体撤销。

9、监督审核

监督审核的现场审核实施程序与初次认证现场审核实施程序基本相同。

9.1 监督审核频次

(1) SWCC 采用监测监督审核和日常监督【关注国家有关部门发布的信息公报、关注获证组织相关方的信息、审查获证组织对其运作的说明（如宣传材料、网页）、要求获证组织提供文件化信息（纸质或电子介质）、其他监视获证组织绩效的方法】相结合方式对获证组织实施监督活动。

(2) 在证书有效期内，获证组织必须接受监督审核，初次认证后的第一次监督审核应在认证决定之日起 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；第二次监督审核通常在第一次监督审核的审核开始日期起 12 个月内实施。特殊情况下（如：发生不可抗力的原因），经过 SWCC 批准后可适当延期，但两次监督审核的审核时间间隔不能超过 15 个月。

(3) 获证组织因未在规定的时间内实施监督审核而暂定证书的，监督审核恢复后，下次审核时间按照原来计划的时间计算。

(4) 若发生下列情况则应增加监督频次，或与获证组织商定提前监督审核：

- 获证组织 PIIP 发生重大变化或发生重大隐私信息安全事故时；
- 有足够信心表明获证组织发生了组织机构、生产条件、产品变更等影响其认证基础的更改；
- 获证组织其客户提出投诉未得到处理时；
- 其他需考虑的情况。

(5) 因获证组织业务运作的时间（季节）特点及其内部审核安排等原因，可以合理选取和安排监督周期及时机，在认证证书有效期内的监督审核必须覆盖认证范围内的所有业务活动与边界。

9.2 信息收集与评审

9.2.1 在进行监督审核之前，需要收集获证组织的管理体系相关信息，以确定获证组织的管理体系相关信息是否发生变化。需要获证组织体供的信息包括但不限于以下几个方面：

- (1) 法律地位、经营状况、组织状态或所有权（包括隶属关系）；
- (2) 组织和管理层（如关键的管理、决策或技术人员）；
- (3) 联系地址和场所；
- (4) 获证管理体系覆盖的运作范围；

(5) 管理体系和过程的重大变更（如活动与服务等）

9.2.2 审核方案策划人员应对获证组织的信息确认文件进行评审，以确定：

- (1) 获证组织的管理体系变化情况，尤其是管理体系范围的变化；
- (2) 是否需要修订审核方案；
- (3) 适用时，对现场审核做出安排。

由于监督审核并不要求覆盖体系的所有方面，因此在监督审核的策划过程中，如果获证组织的认证范围信息有变化，应对变化的方面进行关注，必要时重新确认认证范围。

9.3 确定监督审核人日与审核组

9.3.1 初始的三年认证周期中，对获证组织实施监督审核的审核时间，宜与初次认证审核（第一阶段+第二阶段）的时间成比例，即每年实施监督审核的总时间约为初次认证审核时间的 1/3。作为每次监督审核的组成部分，本机构应获得与获证组织管理体系有关的更新信息。所策划的监督审核时间应得到审查（至少在每次监督审核时），以便考虑客户的组织、体系成熟度等方面的变化、风险相关的隐私信息安全问题其对客户的影响。实施该审查（包括任何对管理体系审核时间的调整）的证据应得到记录。

注：监督审核时间通常情况下不会少于 1 个审核人日，否则可能影响审核有效性。

9.3.2 作为每次监督审核的组成部分，应获得与获证组织管理体系有关的更新信息。所策划的监督审核时间应得到审查（至少在每次监督审核和再认证时），以便考虑客户的组织、体系成熟度等方面的变化。实施该审查（包括任何对管理体系审核时间的调整）的证据应得到记录。

注：监督审核时间视情况在原有的审核持续时间上，适当增加审核人日。

9.3.3 审核方案管理人员应根据获证组织的相关信息确定审核组，指派审核组长，审核组确定原则本文件初次认证审核要求相同。

9.4 监督审核计划

9.4.1 审核组应结合获证组织的信息确认文件、审核方案对监督审核中现场评价的策划对现场评价做出具体安排，包括但不限于具体的时间安排、审核组成员对获证组织按岗位和活动以何种方式进行评价的安排、高层沟通的安排和会议的安排。

审核组长应至少在实施现场审核之前，与获证组织就审核计划进行充分沟通，确保双方在理解上没有歧义。

9.4.2 监督审核是现场审核，但不一定是对整个体系的审核，并应与其他监督活动一起策划，以使 SWCC 能对获证组织 PIIP 在认证周期内持续满足要求保持信任。监督审核采取抽样的方式进行，抽样准则为：

- (1) 两次监督审核涉及的条款之和必须覆盖标准所有条款或过程；
- (2) 标准中对能源管理过程有决定作用的条款每次监督审核都需要抽到；
- (3) 获证组织前一次审核问题较多的条款在本次监督审核中需要抽到；
- (4) 多场所的抽样遵循多场所组织审核的规定。

9.5 监督审核内容

9.5.1 监督的目的包括验证获证 PIIP 得到持续实施、考虑由客户运作实践变化所引起的管理体系变化的影响和确认与认证要求的持续符合。每次监督审核方案应至少包括：

- (1) PIIP 维护要素，如隐私风险评估与控制的维护、内部审核、管理评审和纠正措施；
- (2) 与外部各方的沟通（包括投诉的处理），以及认证所需的其他文件；
- (3) 对上次审核中确定的不符合采取的措施；
- (4) 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；
- (5) 为持续改进而策划的活动的进展；
- (6) 持续的运作控制；
- (7) 任何情况的变更以及变更对体系运行符合性和有效性的影响；
- (8) 标志的使用和（或）任何其他对认证资格的引用。



9.5.2 每一次监督审核应至少审查以下方面：

- (1) PIIP 在实现客户信息安全方针的目标方面的有效性；
- (2) 相关隐私法律法规合规性的定期评价和审查规程的运行情况；
- (3) 所确定的控制的变更，及其引起的适用性声明（SoA）变更；
- (4) 审核方案中所述控制的实现和有效性。

9.6 监督审核实施与结论

9.6.1 审核组应该对现场评价中收集的所有信息和证据进行汇总分析，评价审核发现并就审核结论达成一致。如果现场评价发现不符合项应开具不符合项报告，且获得获证组织认同。现场审核结束，审核组应形成是否推荐保持认证注册的结论或其他的推荐结论。

9.6.2 SWCC 应能够调整监督审核活动计划，以反映与客户风险和影响相关的隐私问题，并证明该控制计划的合理性。

9.6.3 当监督审核与其他管理体系审核相结合时，应清晰地指出与每个管理体系相关的方面。

9.6.4 在监督审核过程中，应检查客户提交给 SWCC 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，还应检查客户是否对其自身的 PIMS 和规程进行了调查并采取了适当的纠正措施。

9.6.5 在监督审核中发现的不符合项，获证组织需进行分析原因，在规定时限要求完成纠正和纠正措施并提供纠正和纠正措施有效性的证据。在验证和接受不符合整改措施后，审核组长应完成监督审核报告编制工作，并与受审核方进行沟通，确保双方对审核报告的理解没有歧义。

9.6.6 监督审核报告应包括有关消除以往发现的不符合、适用性声明（SoA）的版本和上次审核后发生的重大变更的信息。

9.7 监督审核认证决定

认证决定人员（小组）实施认证决定时应以认证过程中收集的信息和其他相关信息为基础，以充分的证据证实获证组织管理体系得到了建立、实施、运行、监视、评审、保持和改进。

对获证组织的认证申请实施认证决定，以决定：



- (1) 同意保持认证注册，颁发年度确认书；
- (2) 同意认证范围扩大或缩小，颁发年度确认书；
- (3) 补充认证决定所需的信息，包括但不限于申请材料、审核材料，再行决定；
- (4) 不同意保持认证注册，做出暂定或撤销的决定，并将理由通知获证组织；
- (5) 适用时，做出同意恢复认证资格的决定。

10、再认证

再认证的现场审核实施程序与初次认证现场审核实施程序基本相同。

10.1 再认证审核策划

(1) 再认证审核的目的是确认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。获证客户证书有效期届满前 3 个月时，将向获证客户发放《再认证审核通知书》，如获证客户要继续保持认证注册资格，须与 SWCC 联系再认证事宜，SWCC 将按认证程序与其签订认证合同，对其进行再认证审核，以评价获证组织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。再认证的策划和实施应及时进行，以便认证能在到期前及时更新。

(2) 再认证活动应考虑管理体系在最近一个认证周期内的绩效，包括调阅以前的监督审核报告。

(3) 当获证组织、隐私信息管理体系或管理体系的运作环境（如法律法规、政府政策、标准要求的变更）有重大变更时，再认证审核活动可能需要有第一阶段。

注：此类变更可能在认证周期中的任何时间发生，SWCC 可能要求实施特殊审核，以确保 PIIP 和认证范围的符合，并此类特殊审核可能需要或不需两阶段审核。

(4) 对于多场所认证进行的认证，再认证审核的策划应确保现场审核具有足够的覆盖范围，以提供对 PIIP 认证的信任。

10.2 再认证审核人日

(1) 再认证审核时间宜根据更新的客户信息计算，而不是简单按初次认证审核（第一阶段+第二阶段）时间的 2/3 计算。通常做法是：假设基于更新的信息对组织实施初次认证审核，再认证审



核时间约为该初次审核所需时间的 2/3。作为特例，如果再认证时组织的情况与初次认证审核时相同，则再认证审核时间大约为初次认证审核时间的 2/3。

(2) 再认证审核时间应考虑管理体系绩效评价的结果（见《企业再认证绩效评价表》）。对管理体系绩效评价本身并不作为再认证审核时间的一部分。

注：再认证审核时间通常情况下不会少于 1 个审核人日，否则可能影响审核有效性。并可视情况在原有的审核持续时间上，适当增加审核人日。

10.3 再认证审核

(1) 在认证证书到期后，如果 SWCC 能够在 6 个月内完成未尽的再认证活动，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（即按初次认证第二阶段的要求实施）。

(2) 如果在认证终止日期前，SWCC 未能完成再认证审核，则不应推荐再认证，也不应延长认证证书的有效期。

(3) 现场再认证审核应重点关注以下内容：

——结合内外部变化评价 PIIP 的有效性，以及认证范围的持续相关性和适宜性；

——经证实的对保持 PIIP 有效性并改进管理体系，以提高整体绩效的承诺；

——PIIP 在实现获证组织的目标和预期结果方面的有效性。

(4) 再认证现场审核活动参见本文件初始认证审核的相关要求。

10.4 再认证的决定

(1) 认证决定人员（小组）应根据再认证审核的结果，以及认证周期内的体系评价结果和认证使用方的投诉，作出是否更新认证的决定。

(2) 如果在认证证书终止日期前，因获证组织原因，审核组不能完成对严重不符合实施的纠正和纠正措施验证，则不应推荐再认证注册，也不应延长认证的效力，并告知申请组织和解释后果。

(3) 认证决定人员（或小组）按照本文件 7.9 条要求作出再认证决定。获证组织继续满足认证要求并履行认证合同义务的，向其换发认证证书

11、管理体系结合审核

11.1 当认证客户在运行 PIIP 的同时还运行了其他管理体系，若其他管理体系在 SWCC 的认证业务范围内，则 SWCC 可以根据认证客户的需求对管理体系进行单独的审核，或者对多个管理体系进行结合审核，但需确保在结合审核的情形下，对诸如审核范围的界定、审核时间的确定、审核方案的策划等进行有效的管理。

11.2 对于结合审核，必须以审核活动满足体系认证所有要求为前提，并且 PIIP 审核的完整性不应由于结合审核而受到负面影响。在审核报告中，应清晰体现所有与管理体系有关的重要要素的描述并易于识别。

(1) 初次审核：SWCC 将对组织的申请信息应包括与一体化程度有关的信息（包括文件、管理体系要素和职责整合信息）予以评审，并在第一阶段审核期间，审核组应就受审核方的管理体系一体化程度进行确认。必要时，应基于申请阶段所获取的信息而确定的审核时间进行评审和调整。

(2) 监督和再认证活动：SWCC 应确认受审核方的管理体系的一体化程度在整个认证周期里保持不变，以确保所确立的审核时间依然适用。

(3) 暂停、缩小、撤销：在受审核方一体化管理体系中，如果暂停、缩小或撤销其中一个或多个管理体系标准/规范认证时，SWCC 应调查由此产生的对于其他管理体系标准/规范认证的影响。

(4) 审核应覆盖受审核方一体化管理体系范围内所涉及的每一个管理体系标准的所有适用要求。

(5) 管理体系审核报告可以是综合的或分开的报告。在一份综合的报告中，对于每一项发现，应追溯至适用的管理体系标准/规范。

(6) SWCC 应考虑针对其中一个管理体系标准/规范所发现的每个不符合对于其他管理体系标准/规范的符合性的影响。

12、特殊审核

12.1 扩大认证范围

(1) 对于已授予的认证，应对获证组织扩大认证范围的申请进行评审，策划并实施必要的审核活动，并在该审核活动中验证获证组织的 PIIP 的适宜性和有效性，作出是否可予扩大认证范围的决定。扩大认证范围的审核活动可单独进行，也可和监督审核同时进行。

(2) 扩大认证范围的条件

——获证组织保持认证资格有效；

——获证组织申请扩大的认证范围在法律地位文件范围内。国家或行业有要求时，获证组织扩大的认证范围应具有有效的行政许可文件；

——国家或行业有要求时，获证组织申请扩大的认证范围内的组织单元、活动、服务及其过程和活动，已满足适用的法律法规的要求；

——获证组织的管理体系覆盖申请扩大的认证范围，并扩大的认证范围的管理体系运行符合认证标准/规范性文件要求；

——获证组织按照 SWCC 有关要求缴纳补充的认证费用。

(3) 扩大范围的申请与策划

——SWCC 向获证组织提供与扩大认证范围有关信息的公开文件，并使其知晓与理解。

——获证组织需提交正式的扩大范围的申请和相关附件，需要时，获证组织与 SWCC 双方签订补充认证协议或合同。

——方案管理人员对扩大范围审核进行策划，确认现场评价审核方式和委派审核组等相关事宜，扩大范围的审核认证参见本文件相关规定。

(4) 扩大范围的认证决定

——认证决定人员（小组）根据扩大审核的结果，认为获证组织申请的扩大认证范围满足批准认证资格的条件，同意批准扩大认证范围，换发新的认证证书。认证证书的注册号和有效性保持不变。SWCC 向获证组织送交新的认证证书，同时收回原证书。

——若认证决定人员（小组）根据扩大审核的结果，认为不满足认证资格的条件，则告知获证组织的不授于扩大范围的理由。

12.2 提前较短时间通知的审核

为了调查投诉、对变更做出回应、对被暂停认证资格的获证组织进行追踪，或配合国家有关部门的监督检查，SWCC 可能需要指派审核组在提前较短时间通知获证组织后或不通知获证组织就对其进行特殊审核。

- (1) 应向获证组织说明并使其提前了解将在何种条件下进行此类审核；
- (2) 审核组应制订审核计划，形成审核结论；
- (3) SWCC 应根据审核结论作出认证决定。

注：若获证组织不配合或不接受安排的特殊审核，认证证书将会被暂停。

12.3 缩小认证范围和变更认证信息

12.3.1 缩小认证范围

(1) 缩小认证范围的条件

- 获证组织认证范围内部分过程或活动、区域等不符合认证标准/规范性文件和其他要求；
- 获证组织不愿再继续保持认证范围内的部分过程、区域等的认证资格；
- 获证组织缩小认证范围不应包括缩小认证风险的情况。

(2) 缩小认证范围的处理程序

- 根据受审核方的现场审核证据或认证决定人员根据审核结果，认为需要缩小认证范围的，需告知受审核方并得到其确认；
- 获证组织提交正式的缩小范围申请，经 SWCC 与获证组织沟通后达成一致意见的，可缩小原认证范围。需要时，修订认证协议或合同；
- 经 SWCC 审定认为获证组织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，换发新的认证证书或附件，认证证书注册号和有效期保持不变；
- 获证组织缩小认证范围后，其证书和标志的使用需遵循 SWCC 的公开文件《GK-06 认证证书和认证标志使用管理规定》的相关要求。

12.3.2 变更认证信息

(1) 变更认证信息的条件

在认证证书有效内，获证组织因信息变更，导致与认证证书信息不一致时，应予以更新。

(2) 变更认证信息的要求

a) 获证组织名称、住所（注册地址）、行政区域地址的变更

——获证组织提出书面的变更申请，并提供行政主管部门的变更核准证明或新的营业执照、或行政部门相关文件的复印件；

——对于因改制、重组而引起的名称变更，获证组织不能提供名称变更核准证明时，应提交原名称现名称的变更申请、行政主管部门的批文或原名称注销的证明；并因变更引起 PIMS 重大变化的，需接受 SWCC 的一次特殊审核或结合监督/再认证时的审核和审核决定。

——行政区域地址的变更（物理位置没有变化），可行时，需提供当地政府的相关证明。

——有行政许可、资质等要求的获证组织，还需提供变更后的有关文件。

b) 认证/审核地址、证书覆盖的多场所地址变更

获证组织提出书面的变更申请；有行政许可、资质等要求的，还需提供变更后的有关文件。需接受 SWCC 的一次特殊审核或结合监督/再认证时的审核和审核决定。

c) 证书范围中质量管理过程、活动的变更

获证组织提出书面的变更申请；有行政许可、资质等要求的认证范围，还需提供变更后的有关文件。需接受 SWCC 的一次特殊审核或结合监督/再认证时的审核和审核决定。

d) 认证标准/规范性文件的版本变更

获证组织提出书面的变更申请，需接受 SWCC 的一次特殊审核或结合监督/再认证时的审核和审核决定。

e) 体系覆盖的人数变更

获证组织提出书面的变更申请，SWCC 按新的体系覆盖人数策划各类型的审核人日。

(3) 变更信息的处理流程

获证组织根据上述的要求提交满足要求的书面变更申请和相关文件资料。

——经 SWCC 审定，认为满足认证信息变更条件，并无需实施一次监督审核或特殊审核的，同意批准认证信息变更，将换发证书或附件，认证证书有效期保持不变，需要时，收回原认证证书。

——经 SWCC 审定，需实施一次监督审核或特殊审核的，根据审核结果同意批准认证信息变更，将换发认证证书或附件，认证证书的有效期保持不变，需要时，收回原认证证书。

13、暂停和恢复认证资格

13.1 暂停认证资格

13.1.1 符合下列条件之一的获证组织，SWCC 将暂停其认证证书：

(1) 管理体系持续或严重不满足认证要求，包括对体系运行的有效性要求。

——获证组织管理体系发生重大变更，不能持续符合认证标准/规范性文件要求；

——获证组织监督审核期间发生严重影响体系运行的情况；

——获证组织在认证范围的组织单元、管理过程或活动不能满足适用的法律法规和标准的要求，并没有采取措施或措施无效；

——获证组织没有按照认证要求的变更作出相应的调整，或调整不满足变更要求。

(2) 组织不承担、履行认证合同约定的责任和义务。

——获证组织未能在规定的期间内接受监督或再认证审核；

——获证组织未履行与 SWCC 签署的认证合同中规定的责任和义务，并对保持认证资格产生重大影响；

——获证组织未按照认证合同缴纳认证费用；

——获证组织在获证期间发生误用认证证书和标志，并未能及时有效地采取纠正和纠正措施，以将产生的影响降至最小程度。

(3) 获证组织在证书有效期间受到相关执法监管部门处罚或责令停业整顿。

——获证组织未能按要求向 SWCC 进行相关信息通报；

——获证组织针对处罚没有没有采取措施或措施无效；

——获证组织在获证期间被列入“严重违法失信名单”。

(4) 获证组织被地方认证监管部门发现管理体系运行存在问题。

获证组织在获证期间认证范围内发生国家抽验不合格，并没有查明原因和采取补救措施。

(5) 获证组织持有的与管理体系认证范围有关的行政许可证明、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。

——获证组织的法律地位、资质等不在符合国家的最新要求；

——获证组织的认证范围已不在现行有效的法律地位文件和资质规定的范围内。

(6) 组织发生了与管理体系有关的重大事故，反映出组织的体系建立及运行存在重大缺陷。

——获证组织在获证期间因管理引起的重大事故，未能按要求向 SWCC 进行相关信息通报，并没有查明原因和采取纠正措施；

——获证组织在获证期间认证范围内存在严重负面影响舆情，没有查明原因和采取补救措施。

(7) 获证组织主动请求暂停。

(8) 其他原因需要暂停证书，包括但不限于：

——不能按照规定或约定的时间间隔接受监督的；

——未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的；

——拒绝配合认证监管部门或其他行政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；

——获证组织在获证期间多次被其客户投诉；

——法律主体的变更（或法律地位、经营状况、组织状态或所有权的变更）影响管理体系正常运行的；关键的管理、决策或技术人员的变更影响管理体系正常运行的。

13.1.2 暂停资格处理程序

(1) 经 SWCC 核实暂停条件后，与获证组织沟通提出暂停其全部或部分认证范围内的认证资格，提供相应的理由和证据，确定暂停期限，向获证组织发送暂停通知；

(2) 经 SWCC 审核和评定，认为获证组织在认证范围内全部或部分不能持续满足认证要求，但在短期内不能采取纠正措施的，将批准同意暂停全部或部分认证范围的认证资格，并确定暂停期限，向获证组织发送暂停通知。

(3) 获证组织应按 SWCC 的公开文件要求，停止使用认证证书和标志；暂停期间获证组织的管理体系认证暂时无效。暂停将不超过 6 个月。在暂停期间，获证客户的管理体系认证暂时无效。

13.2 恢复认证资格

13.2.1 恢复认证资格的条件

获证客户在规定的期限内，已经针对暂停认证资格的原因采取了有效的措施，造成暂停的问题已得到解决，重新符合认证的相关要求，则其认证资格可以恢复，并同时已经证实在暂停期间没有使用、引用认证资格（如广告宣传）和使用认证标志。

13.2.2 恢复认证资格的处理流程

获证组织已消除产生暂停认证资格的原因，或提交的相关纠正措施和有效性验证资料，经 SWCC 审定符合相关的认证要求，办理恢复手续，同意批准恢复其认证资格，向获证组织发送恢复通知。

14、撤销和注销认证资格

14.1 撤销认证资格

14.1.1 符合下列条件之一的获证组织，SWCC 将撤销其认证证书：

- (1) 组织的审核没有通过。
- (2) 组织被注销或撤销法律地位证明文件的（或法律地位、资质不符合国家最新要求）。
- (3) 组织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。
- (4) 出现重大的隐私信息安全或其他事故，经执法监管部门确认是获证组织违规造成的。

(5) 组织在证书有效期内有其他严重违法法律法规行为，受到执法监管部门处罚的。

(6) 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）。

(7) 没有运行管理体系或者已不具备运行条件的：

——组织认证范围内 PIMS 发生重大变更，未向 SWCC 通报，并在短期内无法满足认证要求；

——组织体制变更后，原管理体系已不再适宜；

——组织不再生产体系覆盖内的产品或提供服务的；

——组织停业或关闭的；

——组织在认证范围内的组织单元、管理过程或活动严重不能满足适用新的法律法规和标准的要求，并在短期内无法采取措施或采取的措施无效。

(8) 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 SWCC 已要求其纠正但超过 6 个月仍未纠正的。

(9) 组织发生了与隐私有关的重大事故，反映出组织的 PIIP 建立及运行存在重大缺陷的。

(10) 组织不承担、履行认证合同约定的责任和义务。

(11) 其他原因需要撤销证书，包括但不限于：

——针对不符合项的整改和关闭超过规定的期限，或整改不符合要求的；

——对相关方重大投诉（含媒体负面曝光），不能采取有效处理措施的；

——被执法监管认定存在严重违法失信行为，经行政复议后尚未移出“严重违法失信名单”的；

——获证组织伪造、涂改、转让和非法买卖 SWCC 的认证证书和标志的。

14.1.2 撤销认证资格的处理流程

经 SWCC 审定，确认获证组织在认证范围内的管理体系不再满足认证要求，作出撤销认证资格的结论，发送撤销通知并将相关信息上报和公示，认证组织不得再使用 SWCC 的认证证书和标识，

并要求认证组织返还所有与 SWCC 认证相关的证书和标识。

14.2 注销认证资格

14.2.1 注销认证资格的条件

符合下列条件之一的获证组织，其认证证书可以注销：

- (1) 获证组织申请注销认证证书。
- (2) 认证证书有效期届满，未申请延续使用。
- (3) 因换发新证书而注销旧证书。
- (4) 其他原因需要注销认证证书。

14.2.2 注销认证资格的处理流程

经 SWCC 审定，确认满足注销条件的（因换发新证书而注销旧证书除外），将作出注销认证资格的结论，并将相关信息上报和公示，认证组织不得再宣称通过 SWCC 的管理体系认证，及不得再使用 SWCC 的认证证书和标识。获证组织在证书有效期内予以注销的，应返还所有与 SWCC 认证相关的证书和标识。

15、受理组织的申诉

15.1 申请组织或获证组织对认证决定有异议时，SWCC 应接受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送交申诉人。

15.2 书面通知应当告知申诉人，若认为 SWCC 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认监委投诉，也可向相关认可机构投诉。

16、认证记录的管理

16.1 SWCC 建立认证记录保持制度，记录认证活动全过程并妥善保存。

16.2 记录应当真实准确以证实认证活动得到有效实施。记录资料应当使用中文，保存时间至少应当与认证证书有效期一致。

16.3 以电子文档方式保存记录的，应采用不可编辑的电子文档格式。



17、其他

17.1 本文件内容提及 ISO/IEC 29151 标准时均指认证活动时该标准的有效版本。认证活动及认证证书中描述该标准号时，应采用当时有效版本的完整标准号。

17.2 本文件未尽事宜，按照国家有关法律、法规的规定执行；本文件如与国家日后颁布的法律、法规或经合法程序修改后的章程相抵触的，按照国家有关法律、法规的规定执行，并立即修订。

17.3 本文件自发布之日起实施，修订亦同。
