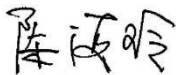
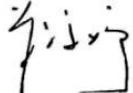


 深圳市深大国际认证有限公司 SHENDA INTERNATIONAL CERTIFICATION CO., LTD		版次	A/1
		文件编号	CTS SDIC-WI-TC121
文件名称	信息安全管理体系统认证实施规则	生效日期	2025 年 8 月 28 日

信息安全管理体系统认证实施规则

发行部门 Issuing Department:	技术部	日期 Date:	2025 年 8 月 28 日
编制 Preparation:	黄美秀、刘燕	日期 Date:	2025 年 8 月 28 日
审核 Audit:		日期 Date:	2025 年 8 月 28 日
批准 Approval:		日期 Date:	2025 年 8 月 28 日

 深圳市深大国际认证有限公司 SHENDA INTERNATIONAL CERTIFICATION CO., LTD		版次	A/1
		文件编号	CTS SDIC-WI-TC121
文件名称	信息安全管理体系认证实施规则	生效日期	2025年8月28日

目录

1 适用范围	4
2 认证依据用技术规范、技术规范强制性要求或者标准	4
2.1 认证依据	4
2.2 本文件适用的术语	4
3 认证实施程序	4
3.1 申请及受理	4
3.2 认证申请评审	5
3.3 认证合同	6
3.4 审核方案策划	7
3.5 审核实施	9
3.6 初次认证审核实施	9
3.7 监督审核	12
3.8 再认证程序	13
3.9 特殊审核	14
3.10 不符合项及验证	15
3.11 审核报告	15
3.12 技术审查及复核	17
3.13. 认证决定、认证证书颁发	19
4 认证证书、标志及认可标识的使用	20
4.1 认证证书的管理	20
4.2 认证证书和认证标志	20
4.3 认证证书	20
4.4 认证标志	21
5 认证证书的状态管理	22
5.1 证书状态管理的内容	22
5.2. 暂停认证证书的条件	22
5.3. 证书暂停	23
5.4 认证资格的撤销	23
5.5 认证资格的注销	23
5.6 认证资格的恢复	23
6 其它要求	24
6.1 受理组织的申诉和投诉	24
6.2 认证记录的管理	24
6.3 收费标准	25
6.4 对认证人员的条件和要求	25
7. 引用文件	25
7.1 相关规范/标准	25
7.2 引用程序	25
附件 ISMS/ITSMS 基础审核时间	27
附件 2 证书模板	29

 深圳市深大国际认证有限公司 SHENDA INTERNATIONAL CERTIFICATION CO., LTD		版次	A/1
		文件编号	CTS SDIC-WI-TC121
文件名称	信息安全管理体系认证实施规则	生效日期	2025年8月28日

1 适用范围

1.1 本规则适用于深圳市深大国际认证有限公司（以下简称深大认证）依据《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》标准对产品生产组织开展信息安全管理体系的认证活动。

1.2 本规则依据认证认可相关法律法规，结合相关技术标准，对组织实施信息安全管理体系认证过程作出具体规定，明确“深大认证”在认证过程中的认证程序、依据的认证准则，保证信息安全管理体系认证活动的规范有效。

1.3 本规则是信息安全管理体系认证活动中的基本要求，深大认证在该认证活动中将遵守本规则。

2 认证依据用技术规范、技术规范强制性要求或者标准

2.1 认证依据

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

2.2 本文件适用的术语

2.2.1 《GB/T 19000 质量管理体系 基础和术语》；

2.2.2 《GB/T 27000 合格评定 词汇和通用原则》的术语使用本文件

3 认证实施程序

3.1 申请及受理

3.1.1 按照《认证申请及受理程序》，市场拓展部业务人员指导认证申请组织如实填写《认证申请书》，按要求提供相关资料。《认证申请书》需经申请组织代表签字，并盖申请组织的公章。

3.1.2 申请方应提交的资料及具备的条件

3.1.2.1 申请组织应提交的资料

1) 营业执照（注册证明）复印件

 深圳市深大国际认证有限公司 SHENDA INTERNATIONAL CERTIFICATION CO., LTD		版次	A/1
		文件编号	CTS SDIC-WI-TC121
文件名称	信息安全管理体系认证实施规则	生效日期	2025年8月28日

- 2) 生产许可复印件（适用时）
- 3) 现行有效的信息安全文件及文件清单
- 4) 与经营过程有关的法律、法规及标准、技术规范（国际、国家、地方、行业）的清单
- 5) 主要生产/经营过程的描述
- 6) 组织架构图、信息安全服务流程及相关说明（适用时）；
- 7) 对信息安全管理体系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；
- 8) 涉及跨境数据传输的组织需额外提交《数据出境安全评估报告》
- 9) 适用性声明；

3.1.2.2 申请方应具备以下基本条件：

- 1) 依法成立，取得国家工商行政管理部门或有关机构注册登记的法人资格或其组成部分；
- 2) 遵守相关的法律法规要求；
- 3) 近三年无重大质量、安全、环保事故；
- 4) 承诺获证后发生重大事故及时向深大国际认证报告。
- 5) 体系运行3个月以上。

3.2 认证申请评审

3.2.1 认证申请评审人员对提交的申请书及相关资料见评审，并确定：

- 1) 提供的申请资料是否齐全，资料内容是否真实、准确、完整；
- 2) 申请组织从事的活动是否符合相关法律法规的规定；
- 3) 申请组织是否已了解认证的相关要求；
- 4) 申请组织所申请认证的领域及范围是否在认可的业务范围内。
- 5) 深大认证是否有能力并能够实施评价。
- 6) 是否被执法监管部门责令停业整顿或者在全国企业信用信息公示系统中被列

 深圳市深大国际认证有限公司 SHENDA INTERNATIONAL CERTIFICATION CO., LTD		版次	A/1
		文件编号	CTS SDIC-WI-TC121
文件名称	信息安全管理体系认证实施规则	生效日期	2025 年 8 月 28 日

入“严重违法企业名单”。

3.2.2 按照《管理体系/服务/产品业务范围管理程序》由业务初步确认认证审核的范围。认证范围的描述应明确到具体的产品或服务，采用专业化的术语且不会误导申请组织的顾客及其他相关方。

3.2.3 确定认证审核时间

业务人员、认证申请评审和认证客户沟通获取相关信息，确定审核时间。

3.2.4 认证申请回复

- 1) 深大认证市场拓展部应在收到申请表后 30 个工作日内通知申请方：
- 2) 如接受其申请，深大国际认证市场拓展部经理将在其申请表上签署意见后返回申请方一份，同时签订合同（一式二份），费用按深大国际认证现行收费标准收取。
- 3) 如不接受其申请，深大国际认证将通知其原因，并退回申请材料。该申请方在条件满足后可以再次提出申请。

3.3 认证合同

通过申请评审的，业务部应与认证客户签订具有法律效力的认证合同，以明确认证客户和深大认证的责任。

3.3.1 深大认证的责任至少包括：

- (1) 及时向符合认证要求并已缴纳认证费用的组织颁发认证证书，通过其网站或者其他形式向社会公布获证信息；
- (2) 对认证客户管理体系运行情况的有效监督，发现认证客户的管理体系不能持续符合认证要求的，应及时暂停或者撤销其认证书；
- (3) 因深大认证原因（如机构或其管理体系认证资质被注销或撤销）导致认证客户管理体系证书无法有效保持的，需及时告知认证客户并做出妥善处理，并承担由此导致的认证客户的经济损失。

3.3.2 认证客户的责任至少包括：

 深圳市深大国际认证有限公司 SHENDA INTERNATIONAL CERTIFICATION CO., LTD		版次	A/1
		文件编号	CTS SDIC-WI-TC121
文件名称	信息安全管理体系认证实施规则	生效日期	2025年8月28日

- (1) 遵守认证程序要求，认证过程如实提供相关材料和信息，通过管理体系认证后持续有效运行管理体系；
- (2) 配合认证监管部门的监督检查，配合深大认证对投诉的调查；
- (3) 应当在广告、宣传等活动中正确使用认证证书、认证标志和有关信息，认证证书注销或被暂停、撤销的，不得继续使用该证书和相关认证标志、信息；
- (4) 发生如下情况，应及时向深大认证通报：发生重大质量事故、受到市场监管部门行政处罚、被市场监管部门公布存在质量不符合、被媒体曝光存在质量问题、管理体系不能正常运行或发生重大变更，以及其他应通报的情况等；
- (5) 承担选择深大认证的风险，如：因深大认证资质被撤销而带来的认证证书无法使用的风险；
- 6) 按合同约定及时向深大认证缴纳认证费用，包括：在现场审核之前缴纳不低于80%的认证费用，余款应当在深大认证做出授予、保持认证资格的决定后支付。

3.4 审核方案策划

按照《审核策划操作规范》规定由审核方案策划人员进行审核方案的策划。策划的活动包括：

3.4.1 审核时间

3.4.1.1 深大认证根据申请组织的规模、特性、业务复杂程度、信息安全管理体系涵盖的范围、认证要求和其承担的风险等因素核算并确定审核人日，以确保审核的充分性和有效性。

3.4.1.2 审核时间见附表《ISMS/ITSMS 基础审核时间》。

3.4.2 审核组组长

审核组应具备实施信息安全管理体系认证审核的能力，并指定一名有能力的审核员担任审核组长在必要时还应配备相关行业的技术专家，以保证审核组的整体能力覆盖组织的信息安全管理体系认证的专业审核能力要求。

 深圳市深大国际认证有限公司 SHENDA INTERNATIONAL CERTIFICATION CO., LTD		版次	A/1
		文件编号	CTS SDIC-WI-TC121
文件名称	信息安全管理体系认证实施规则	生效日期	2025年8月28日

3.4.3 审核计划

审核组长接到《审核任务通知书》后，应结合审核组及受审核方情况编制《审核计划》。审计计划的内容及编制审核计划应注意的事项参见 SDIC-OP-AD-001 《审核过程管理程序》的 6.1.3.1 审核计划。

3.4.4 多场所抽样方案

3.4.4.1 深大认证建立并实施多场所组织认证抽样的规则并遵照执行，策划并保留多场所组织的抽样及确定审核时间的记录。

3.4.4.2 多场所抽样应基于与认证客户活动或过程性质相关的管理体系风险的评价，如果多个场所未涵盖相同的活动、过程及管理体系风险类型，则不应抽样，应当逐一到各场所进行审核。对多个相似场所可进行抽样审核，抽样数量应不少于按以下方法计算的结果：

初次审核：样本量为分场所数量的平方根（ $y=\sqrt{x}$ ），上入成整数。

监督审核：每年的样本量为分场所数量的平方根与系数 0.6 的乘积（ $y=0.6\sqrt{x}$ ），上入成整数。

再认证审核：样本量与初次审核相同，然而当其管理体系在三年中被证明有效时，样本量可乘以系数 0.8，即（ $y=0.8\sqrt{x}$ ），上入成整数。

以上抽样适用于少于 50 人且低、中风险影响的分场所。

注：其中 Y 为抽样的数量，结果向上取整；X 为相似场所的总体数量。

在新的一批场所申请纳入已获证的多场所网络时，每批新的场所宜被视为独立的一组以确定抽样量。在这批新的场所增加到证书后，宜将新的场所合计在以前的场所内，以确定在以后的监督审核或再认证时的样本量。

当对拟认证的管理体系覆盖的活动的风险分析显示出与下列因素有关的特殊情况时，宜增加样本量或抽样频次：

- a) 场所规模大与雇员数量多（例如，某场所雇员超过 50 人）；
- b) 活动和合规管理体系的复杂和风险水平高；
- c) 作业方法有差异（例如倒班工作）；

 深圳市深大国际认证有限公司 SHENDA INTERNATIONAL CERTIFICATION CO., LTD		版次	A/1
		文件编号	CTS SDIC-WI-TC121
文件名称	信息安全管理体系认证实施规则	生效日期	2025 年 8 月 28 日

- d) 所从事活动的差异大;
- e) 多次投诉及其纠正措施与预防措施的记录不完整;
- f) 有跨国情况;
- g) 内部审核结果可信度差。

3.4.4.3 分场所审核人日的计算方法参见 QMS 管理体系审核的相关要求且现场审核时间不得少于规定时间所现场审核时间的 50%。

3.5 审核实施

3.5.1 审核组应按照审核计划实施审核，并采用中文记录审核过程，可使用图片、音像等作为补充材料。

3.5.2 审核组应会同认证客户召开首、末次会议，认证客户的最高管理者（因特殊原因不能参加的，应授权高级管理层其他成员）、管理体系相关职能部门负责人应参加会议，缺席应记录理由。审核组应保留首、末次会议签到记录。审核组应按国家认监委的要求完成首、末次会议现场审核的网络签到。

3.5.3 发生下列情况时，审核组应向深大认证报告，经同意后终止审核：

- (1) 认证客户对审核活动不予配合，审核活动无法进行；
- (2) 认证客户实际情况与申请材料有重大不一致；
- (3) 其他导致审核程序无法完成的情况。

3.6 初次认证审核实施

由审核部按照《审核过程管理过程》对认证客户的信息安全管理体系进行审核，包括

3.6.1 信息安全管理体系认证审核分为两个阶段进行，分为第一阶段审核和第二阶段审核。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

3.6.2 第一阶段评价审核：文件审核，审核目的为判断是否具备充足的条件开展二阶段的评价审核。

 深圳市深大国际认证有限公司 SHENDA INTERNATIONAL CERTIFICATION CO., LTD		版次	A/1
		文件编号	CTS SDIC-WI-TC121
文件名称	信息安全管理体系认证实施规则	生效日期	2025 年 8 月 28 日

3.6.2.1 第一阶段评价审核的内容：

审核申请组织的信息安全管理体系文件；

(1) 评价申请组织的运作场所和现场的具体情况，覆盖的活动内容和范围、覆盖范围内有效人数、过程和场所，遵守适用的法律法规及强制性标准的情况。

(2) 审查申请组织理解和实施信息安全管理体系标准要求的情况；

(3) 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、生产或服务过程等是否与申请组织的实际情况相一致。

(4) 审查第二阶段审核所需资源的配置情况，并与申请组织商定第二阶段审核的细节；

(5) 结合申请组织信息安全管理体系方针和目标，了解其审核准备状态，为策划第二阶段的审核提供重点；

(6) 评价申请组织是否策划和实施了内部审核与管理评审，确认管理体系是否已运行并且超过 3 个月。以及信息安全管理体系的实施程度能否证明其已为第二阶段审核做好准备。

(7) 认证机构应将第一阶段审核发现形成文件并告知申请组织，包括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。对管理体系成文信息不符合现场实际、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，以及其他不具备二阶段审核条件的，不应实施二阶段审核。

3.6.2.2 第一阶段审核可以不在申请组织的现场进行，但应记录未在现场进行的原因。

3.6.2.3 非现场审核的条件

为达到第一阶段审核的目的和要求，除下列情况外，第一阶段审核活动应在认证客户现场实施：

(1) 认证客户已获本认证机构颁发的其他领域的有效认证证书，认证机构已对认证客户信息安全管理体系有充分了解；

(2) 认证机构有充足的理由证明认证客户的生产经营或服务的技术特征明显、

 深圳市深大国际认证有限公司 SHENDA INTERNATIONAL CERTIFICATION CO., LTD		版次	A/1
		文件编号	CTS SDIC-WI-TC121
文件名称	信息安全管理体系认证实施规则	生效日期	2025年8月28日

过程简单，通过对其提交文件和资料的审核可以达到第一阶段审核的目的和要求；

(3) 认证客户获得了经认可机构认可的其他认证机构颁发的有效的信息安全管理体系认证证书，通过对其文件和资料的审核可以达到第一阶段审核的目的和要求。

(4) 应记录未在现场进行一阶段审核的理由。

3.6.2.4 将认证客户是否具备二阶段审核条件的结论书面告知认证客户，包括所识别的需引起关注的、在二阶段可能被判定为不符合项的问题。

3.6.3 第二阶段评价审核：

第二阶段为现场审核，审核目的是评价客户满管理体系的实施情况，包括有效性。

3.6.3.1 第二阶段评价审核的内容：

3.6.3.1.1 第二阶段审核应在具备实施认证审核的条件下在申请组织的场所进行。确认其是否按照认证标准的要求建立、实施、保持和持续改进管理体系。如果第一阶段审核提出影响实施第二阶段审核的问题，这些问题应在第二阶段审核前得到解决。

3.6.3.1.2 第二阶段审核的目的是通过在申请组织的现场进行系统、完整地审核，评价申请组织的信息安全管理体系是否满足所有适用的认证依据的要求，并判断是否推荐认证注册。应重点关注申请组织是否充分识别了信息技术服务管理过程的重要性，并证实与申请组织的信息全安活动是相适应的。

审核目的为评价受审核方的管理体系实施的有效性；评价其是否遵守自身方针、策略和规程。

第二阶段审核应重点关注以下内容：

认证机构应要求申请组织证实其对信息安全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：

 深圳市深大国际认证有限公司 SHENDA INTERNATIONAL CERTIFICATION CO., LTD		版次	A/1
		文件编号	CTS SDIC-WI-TC121
文件名称	信息安全管理体系认证实施规则	生效日期	2025 年 8 月 28 日

- (1) 要求认证客户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) 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)；
- (3) 关系过程(业务关系管理，供方管理)；
- (4) 发布过程(发布管理)。
- (5) 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；
- (6) 认证依据所列的文件要求；
- (7) 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；
- (8) 基于风险评估和风险处置过程，确定控制目标和控制；
- (9) 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；
- (10) 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；
- (11) 控制的实施，是否考虑了外部环境、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、配置管理，变更管理，以确定控制是否得以实施、有效并达到其所规定的目标；
- (12) 方案、过程、规程、记录、内部审核、管理评审是否有效和对 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。
- (13) 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。

3.7 监督审核

3.7.1 按照《SDIC-OP-AD-001 审核过程管理程序》要求审核部策划组织对认证客户的信息安全管理体系实施监督审核。作为最低要求，初次认证后的第一次监督审核应在认证证书签发日起 12 个月内进行。此后，监督审核应至少每个日历年进行一次，且两次监督审核的时间间隔不得超过 15 个月。

 深圳市深大国际认证有限公司 SHENDA INTERNATIONAL CERTIFICATION CO., LTD		版次	A/1
		文件编号	CTS SDIC-WI-TC121
文件名称	信息安全管理体系认证实施规则	生效日期	2025年8月28日

3.7.2 审核部组织对认证客户进行有效跟踪，包括依据审核方案对认证客户开展的监督审核，以确认认证客户管理体系符合《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》持续符合性和运行的有效性。

3.7.3 每次监督审核应尽可能覆盖认证范围内的有代表性的过程、行业类别的典型产品/服务；并确保在认证证书有效期内的监督审核覆盖认证范围内的所有代表性的生产/服务过程、行业类别的典型产品/服务。

3.7.4 监督审核应重点关注认证客户的变更以及管理体系绩效的持续改进，监督审核的内容至少包括：

(1) 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是否规范和有效；

(2) 在实现信息安全管理体系认证客户目标和预期结果方面的有效性；

(3) 为持续改进而策划的活动的进展；

(4) 持续的运作控制；

(5) 任何的变更及变更的区域；

(6) 认证证书、认证标志的使用和（或）任何其他对认证信息的引用；

(7) 相关投诉的处理。

(8) 适宜时，其他所选择的区域

(9) 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。

3.7.5 监督审核的时间应根据认证客户当前情况（有效人数和管理体系风险类型）确定。审核时间为初次认证的 1/3。

3.8 再认证程序

3.8.1 按照《SDIC-OP-AD-001 审核过程管理程序》要求实施对认证客户进行再认证审核。

 深圳市深大国际认证有限公司 SHENDA INTERNATIONAL CERTIFICATION CO., LTD		版次	A/1
		文件编号	CTS SDIC-WI-TC121
文件名称	信息安全管理体系认证实施规则	生效日期	2025年8月28日

3.8.2 认证客户拟继续持有认证证书的，应至少在认证证书到期前 3 个月向深大认证提出再认证申请，逾期则按初次认证申请处理。

3.8.3 深大认证应依据审核方案实施再认证审核，以判断认证客户的管理体系作为一个整体与《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》持续符合性和运行的有效性。

3.8.4 再认证审核应在认证客户现场进行，并至少应在认证证书到期前 1 个月完成。再认证审核的内容至少应包括：

(1) 结合其内部环境和外部环境的变化情况，确认认证客户管理体系有效性及认证范围的持续相关性和适宜性；

(2) 认证客户《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》绩效持续改进的证实；

(3) 信息安全管理体系在实现认证客户目标和信息安全管理体系预期结果方面的有效性。

(4) 应与认证客户 ISMS 的初次认证审核的要求和指南保持一致。

3.8.5 再认证审核策划时应考虑认证客户最近一个认证周期内的信息安全管理体系绩效，包括调阅以往的监督审核报告。

再认证审核的审核时间应根据认证客户当前情况（有效人数和信息安全管理体系风险类型）来确定，不少于确定的初次认证审核时间的 2/3。

3.9 特殊审核

如果已经通过 ISMS 认证的客户对其管理体系做重大修改，或者发生影响其获证基础的其他变更，实施特殊审核所必需的活动应遵从特别规定。

3.9.1 扩大认证范围

对于已授予的认证，审核部应对扩大认证范围的申请进行评审，并确定任何必要的审核活动，以做出是否可予扩大的决定。这类审核活动可以结合监督审核同时进行。

 深圳市深大国际认证有限公司 SHENDA INTERNATIONAL CERTIFICATION CO., LTD		版次	A/1
		文件编号	CTS SDIC-WI-TC121
文件名称	信息安全管理体系认证实施规则	生效日期	2025 年 8 月 28 日

3.9.2 提前较短时间通知的审核

为调查投诉、质量事故、对变更做出回应或对被暂停的客户进行追踪，可能需要在提前较短时间或不通知认证客户的情况下进行审核：

- (1) 审核部应说明并使认证客户提前了解将在何种条件下进行此类审核；
- (2) 由于认证客户缺乏对审核组成员的任命表示反对的机会，审核部应在指派审核组时给予更多的关注；
- (3) 认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，自市场监管部门发出通报起 30 日内，审核部应对该组织实施监督审核。

3.10 不符合项及验证

3.10.1 审核组对审核发现签发书面的审核发现，包括不符合项，并要求认证客户分析原因、采取纠正措施。审核组根据《SDIC-OP-AD-001 审核过程管理程序》要求对认证客户不符合的纠正和纠正措施有效性进行验证。

3.10.2 对审核中发现的不符合项，审核组应要求认证客户在规定的时限内进行原因分析，采取相应的纠正措施。

3.10.3 审核组应对认证客户所采取的纠正措施的有效性进行验证。认证客户可以针对轻微不符合项制定纠正措施计划，由深大认证在下次审核时验证。

3.10.4 严重不符合项的验证时限应满足以下要求：

- (1) 初次认证：在二阶段审核结束之日起 6 个月内完成；
- (2) 监督审核：在审核结束之日起 3 个月内完成；
- (3) 再认证：在审核结束之日起 1 个月内完成。

3.10.5 对于认证客户未能在规定的时限内完成对不符合项所采取措施的情况，深大认证不应做出授予认证、保持认证或更新认证的决定。

3.11 审核报告

3.11.1 审核组根据《SDIC-OP-AD-001 审核过程管理程序》对审核活动形成书面审核报告，经评审后交认证客户。

 深圳市深大国际认证有限公司 SHENDA INTERNATIONAL CERTIFICATION CO., LTD		版次	A/1
		文件编号	CTS SDIC-WI-TC121
文件名称	信息安全管理体系认证实施规则	生效日期	2025年8月28日

3.11.2 审核组应就每次审核向认证客户提供书面的审核报告。审核组长应对审核报告的内容负责。

3.11.3 审核报告的内容应准确、简明和清晰，反映认证客户管理体系的真实状况，描述对照标准的符合性和有效性的客观证据信息，及对认证结论的推荐意见。

3.11.4 审核报告至少应包括或引用以下内容：

- (1) 深大认证名称；
- (2) 认证客户的名称和地址及其代表；
- (3) 审核类型（例如初次、监督、再认证或其他类型审核）
- (4) 结合、联合或一体化审核情况（适用时）；
- (5) 信息安全风险分析进行认证审核的说明，及审核准则；
- (6) 审核目的及其是否达到的确认；
- (7) 审核范围，特别是标识出所审核的组织、职能单元或过程，以及审核时间；
- (8) 任何偏离审核计划的情况及其理由；
- (9) 任何影响审核方案的重要事项；
- (10) 审核组成员姓名、身份及任何与审核组同行的人员；
- (11) 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；
- (12) 应描述与审核类型的要求一致的审核发现、审核证据（或审核证据的引用）以及审核结论，重点反映认证客户主要产品和服务提供过程与控制情况、内部审核和管理评审的过程、所取得的绩效，认证客户实际情况与其预期质量目标之间存在的差距和改进机会；
- (13) 行政监管部门在质量方面抽查的不合格情况，及相关原因分析和整改措施的有效性（适用时）；
- (14) 上次审核后发生的影响认证客户管理体系的重要变更（适用时）；
- (15) 认证客户对认证证书和认证标志的使用进行着有效的控制（适用时）；
- (16) 对以前不符合采取的纠正措施有效性的验证情况（适用时）；

 深圳市深大国际认证有限公司 SHENDA INTERNATIONAL CERTIFICATION CO., LTD		版次	A/1
		文件编号	CTS SDIC-WI-TC121
文件名称	信息安全管理体系认证实施规则	生效日期	2025年8月28日

(17) 已识别出的任何未解决的问题；

(18) 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；

(19) 关于 ISMS 是否获得认证的建议，以及支持该建议的信息。

(20) 说明审核基于对可获得信息的抽样过程的免责声明；

(21) 审核组的推荐意见以及对认证范围适宜性的结论。

3.11.5 深大认证应保留用于证实审核报告中相关信息的证据。

3.11.6 深大认证应将审核报告提交认证客户。

3.11.7 对终止审核的项目，审核组应将终止审核的原因以及已开展的工作情况形成报告，深大认证应将此报告提交给认证客户。

3.12 技术审查及复核

3.12.1 技术审查

技术委员会收到审核组长按审核文件归档清单所提交的审核资料（包括：审核报告及其附件等）时，合格评定人员将对所有审核资料进行审查。此审查是认证决定中一项重要活动。其审查内容至少包括：

(1) 档案完整性及规范性的检查

a) 按照归档清单要求的档案，包括档案提交的形式（电子档&纸质档）

b) 签字/盖章完整；

c) 审核档案填写符合规范要求

d) 审核档案没有错别字或其他逻辑性错误

(2) 审核过程中的有效性评审

a) 审核计划的编制

--无遗漏条款；

--审核员时间安排合理；

--专业条款由专业审核员审核或安排了技术专家；

 深圳市深大国际认证有限公司 SHENDA INTERNATIONAL CERTIFICATION CO., LTD		版次	A/1
		文件编号	CTS SDIC-WI-TC121
文件名称	信息安全管理体系认证实施规则	生效日期	2025年8月28日

—审核的体系与审核员资质相符。

b) 审核过程记录

—无遗漏部门和条款；

—覆盖了审核范围；

—无与企业实际信息不符的描述；

—体现了对关键过程的审核，记录描述完整、充分、可追溯；

—对不符合进行了描述与标识。

c) 不符合报告中对不符合描述准确完整；

d) 纠正措施合理有效，关闭不符合理由充分；

e) 审核报告信息与审核记录一致；

f) 其他需关注的内容，如有无任何未解决的问题。

3.12.2 在作出授予或拒绝认证、扩大或缩小认证范围、更新、暂停或恢复或者撤销认证的决定前，指派至少一名未参与审核的人员复核与审核相关的信息和结果，复核应确认：

a) 审核组提供的信息是否足以确定认证要求的满足情况和认证范围；

b) 对于所有严重不符合，是否已审查、接受和验证了纠正和纠正措施；

c) 对于所有轻微不符合，是否已审查和接受了客户对纠正和纠正措施的计划。

3.12.3 除非复核和认证决定由同一人做出，否则基于复核的认证决定的建议应形成文件。

3.12.4 复核的内容应包括审核组提交的以下信息：

a) 审核报告；

b) 对不符合的意见，适用时，还包括对客户采取的纠正和纠正措施的意见；

c) 对提供给深大认证用于申请评审的信息的确认；

d) 对是否达到审核目的的确认；

e) 对是否授予认证的推荐性意见及附带的任何条件或评论。

 深圳市深大国际认证有限公司 SHENDA INTERNATIONAL CERTIFICATION CO., LTD		版次	A/1
		文件编号	CTS SDIC-WI-TC121
文件名称	信息安全管理体系认证实施规则	生效日期	2025 年 8 月 28 日

3.13. 认证决定、认证证书颁发

3.13.1 按照《SDIC-OP-HR-008 认证决定、证书颁发和审核、审查、检查资料处理程序》4.5 的要求作出认证决定和颁发证书。

3.13.2 我司在颁发认证证书后，将在 30 个工作日内按照规定的要求将认证结果相关信息报送国家认监委。

3.13.3 合格评定应在对审核报告、不符合项的纠正措施及验证情况和其他信息进行综合评价的基础上，做出认证决定。认证决定人员应为深大认证管理控制下的专职认证人员，并不得为审核组成员，能力应满足关于深大认证资质审批的相关要求。认证决定过程不得外包，认证决定须由中华人民共和国境内的工作人员做出。

3.13.4 合格评定应有充分的证据确认认证客户满足下列条件时，做出授予、更新、扩大认证范围的决定：

- (1) 满足认证条件；
- (2) 对于严重不符合，已评审、接受并验证了纠正措施的有效性；对于轻微不符合，已评审、接受了认证客户的纠正措施或计划采取的纠正措施；
- (3) 认证客户的 管理体系 总体符合《信息安全管理体系 RB/T 089-2022 标准》要求且运行有效；
- (4) 认证客户按照认证合同规定履行了相关义务。

3.13.5 初次认证审核的认证决定应在现场审核后 6 个月内完成。否则应在推荐认证注册前再实施一次第二阶段审核。

3.13.6 再认证审核的认证决定应在上一认证周期认证证书到期前完成，否则应在推荐认证注册前再实施一次第二阶段审核。

3.13.7 认证客户不能满足 3.13.4 要求的，深大认证应以书面形式告知并说明其未通过认证的原因。

3.13.8 对于监督审核，深大认证在满足下列条件时，可根据审核组长的肯定性

 深圳市深大国际认证有限公司 SHENDA INTERNATIONAL CERTIFICATION CO., LTD		版次	A/1
		文件编号	CTS SDIC-WI-TC121
文件名称	信息安全管理体系认证实施规则	生效日期	2025年8月28日

结论保持对认证客户的认证，无需再进行独立的认证决定：

- (1) 监督审核未发现严重不符合项及其他可能导致认证资格暂停、撤销的情况；
- (2) 认证客户认证信息未发生变更，不存在扩大、缩小认证范围的情况；
- (3) 深大认证建立了监督审核的监视机制并予以实施，可确保监督审核活动的有效性。

4 认证证书、标志及认可标识的使用

4.1 认证证书的管理

按照《SDIC-WI-HR-013 认证标识、认证证书、认可标识的使用管理规定》进行认证证书的管理。

4.2 认证证书和认证标志

4.2.1 认证客户可以在认证有效期内使用管理体系认证标志，并接受深大认证的监督管理。

4.2.3 认证客户应当在广告等有关宣传中正确使用认证标志，不得在产品上标注 认证标志，只有在注明认证客户通过管理体系认证的情况下方可在产品的包装上标注 管理体系认证标志。

4.2.4 深大认证发现认证客户未正确使用认证证书和认证标志的，应当要求认证客户立即采取有效纠正措施，并跟踪监督纠正情况。

4.3 认证证书

4.3.1 深大认证应及时向认证决定符合要求的组织出具认证证书，认证证书的签发日期不应早于做出认证决定日期。

4.3.2 管理体系认证证书的有效期限最长为3年，初次认证证书有效期的起算日期为认证决定日期，再认证证书有效期的起算日期不得晚于最近一次有效认证证书的截止日期。

4.3.3 对每张认证证书应赋予一个认证证书编号，认证证书编号应遵循一定的规律，按照规定执行。

 深圳市深大国际认证有限公司 SHENDA INTERNATIONAL CERTIFICATION CO., LTD		版次	A/1
		文件编号	CTS SDIC-WI-TC121
文件名称	信息安全管理体系认证实施规则	生效日期	2025年8月28日

4.3.4 认证证书在中华人民共和国境内使用的，证书使用的语言至少应包括中文。

4.3.5 认证证书的信息应真实、准确，不产生误导，并至少包含以下内容：

(1) 认证客户名称、统一社会信用代码、注册地址、认证范围所覆盖的经营地址。若认证的管理体系范围覆盖多场所，应表述认证所覆盖的所有场所的地址信息；

注：认证证书中可不包括临时场所，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。

(2) 认证客户管理体系符合《信息安全管理体系 RB/T 089-2022 标准》所覆盖的产品、活动、服务的范围；包括每个场所相应的认证范围，且没有误导或歧义（适用时）；

(3) 认证依据的认证标准所采用的当时有效版本的完整标准号；

(4) 证书签发日期和有效截止日期，证书应注明：认证客户必须定期接受监督审核并经审核合格此证书方继续有效的提示信息。

(5) 证书编号（或唯一的识别代码）；

(6) 深大认证名称、地址；

(7) 认证标志、相关的认可标识及认可注册号（适用时）；

(8) 证书信息及证书状态的查询途径。

4.4 认证标志

4.4.1 按照《认证标识、认证证书、认可标识和认可证书的使用规定》对认证证书及标识进行管理。深大认证自行制定的认证标志的式样、文字和名称，不得违反法律、行政法规的规定，不得与国家推行的认证标志相同或者近似，不得妨碍社会管理，不得有损社会道德风尚。

4.4.2 深大认证标识如下：



 深圳市深大国际认证有限公司 SHENDA INTERNATIONAL CERTIFICATION CO., LTD		版次	A/1
		文件编号	CTS SDIC-WI-TC121
文件名称	信息安全管理体系认证实施规则	生效日期	2025年8月28日

5 认证证书的状态管理

5.1 证书状态管理的内容

按照深大《SDIC-OP-TC-005 暂停、撤销、扩大、缩小和终止认证程序》进行认证证书的状态管理。管理的内容包括暂停、撤销、扩大、缩小和终止。

5.2. 暂停认证证书的条件

获证组织有以下情形之一的，经调查核实后的 5 个工作日内暂停其认证资格，并保留相应证据：

- (1) 管理体系 持续或严重不满足认证要求的；
- (2) 不满足 管理体系 适用的法律法规要求，且未采取有效纠正 措施的；
- (3) 受到与质量相关的行政处罚；
- (4) 发生较大或重大质量事故，反映获证组织 管理体系 运行存 在重大缺陷的；
- (5) 拒绝配合市场监管部门的认证执法检查监督检查，或者提 供虚假材料或信息的；
- (6) 持有的与 管理体系 范围有关的行政许可文件、资质证书、 强制性认证证书等过期失效的；
- (7) 不能按照规定的时间间隔接受监督审核的；
- (8) 未按相关规定正确引用和宣传获得的认证资格和有关 信息，包括认证证书和认证标志的使用，造成严重影响或后果的；
- (9) 不承担、履行认证合同约定的责任和义务的；
- (10) 被有关行政监管部门责令停业整顿的；
- (11) 发生与质量相关的重大舆情；
- (12) 主动请求暂停的；
- (13) 其他应暂停认证资格的。

		版次	A/1
		文件编号	CTS SDIC-WI-TC121
文件名称	信息安全管理体系认证实施规则	生效日期	2025 年 8 月 28 日

5.3. 证书暂停

5.3.1 深大认证可根据暂停的原因和性质确定暂停期限，暂停期限最长不得超过 6 个月。

5.3.2 暂停期间，如获证组织采取有效的纠正措施，造成暂停的原因已消除的，深大认证应恢复其认证资格，并保留相应证据。

5.4 认证资格的撤销

5.4.1 获证组织有以下情形之一的，深大认证应在获得相关信息并确认后 5 个工作日内撤销其认证资格，并保留相应证据：

- (1) 被注销或撤销法律地位证明文件的；
- (2) 被国家企业信用信息公示系统和“信用中国”列入严重违法失信名单的；
- (3) 认证资格的暂停期限已满，但导致暂停的问题未得到解决或有效纠正的；
- (4) 因获证组织违规造成重大产品和服务等质量安全事故的；
- (5) 有其他严重违反 管理体系 相关法律法规行为，受到相关行政监管部门处罚的；
- (6) 管理体系没有运行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，或者深大认证已要求其纠正但超过 1 个月仍未纠正的；
- (8) 其他应撤销认证资格的。

5.5 认证资格的注销

获证组织主动申请不再保持认证资格时，深大认证应注销其 认证资格，并保留相应证据。

5.6 认证资格的恢复

当证实认证客户已经解决了证书暂停的原因后，按照认证决定程序，给予认证客户恢复认证资格。

 深圳市深大国际认证有限公司 SHENDA INTERNATIONAL CERTIFICATION CO., LTD		版次	A/1
		文件编号	CTS SDIC-WI-TC121
文件名称	信息安全管理体系认证实施规则	生效日期	2025年8月28日

6 其它要求

6.1 受理组织的申诉和投诉

按照《SDIC-OP-HR-014 申诉和投诉处理管理程序》进行申诉和投诉的管理。

6.2 认证记录的管理

6.2.1 按照《SDIC-OP-HR-001 文件和记录控制程序》进行记录的管理，建立文件化的认证记录、认证资料归档留存制度，记录认证活动全过程并妥善保存，归档留存时间为认证证书有效期届满或者被注销、撤销之日起2年以上。

6.2.2 认证记录应真实、准确、完整，以证实认证活动得到有效实施。认证记录包括但不限于：

- (1) 认证申请书；
- (2) 认证申请评审记录；
- (3) 认证合同；
- (4) 审核方案；
- (5) 审核计划；
- (6) 首、末次会议签到表；
- (7) 现场审核记录；
- (8) 不符合项报告及验证记录；
- (9) 审核报告；
- (10) 认证决定记录。

6.2.2 在认证证书有效期内，认证活动参与各方签字或者盖章的认证记录、资料等，应保存具有法律效力的纸质版原件。签字或盖章的认证记录至少包括：

- (1) 认证申请书；
- (2) 认证合同；
- (3) 审核计划； — 32 —
- (4) 首、末次会议签到表；

 深圳市深大国际认证有限公司 SHENDA INTERNATIONAL CERTIFICATION CO., LTD		版次	A/1
		文件编号	CTS SDIC-WI-TC121
文件名称	信息安全管理体系认证实施规则	生效日期	2025年8月28日

(5) 不符合项报告及验证记录。

10.4 认证记录应使用中文，以电子文档的形式保存认证记录的，应采用不可编辑的方式。

6.3 收费标准

我司依据《价格法》，制定收费标准，并受深圳市认证认可协会监管。申请组织可向我司索取。

6.4 对认证人员的条件和要求

6.4.1 认证人员能力要求

本机构认证人员包括审核员、技术专家、认证规则和认证方案制定人员、认证决定人员、专业能力评价人员、认证审核方案管理人员、认证申请评审人员，其选择、聘用、培训、考核和评价的基本要求与质量管理体系认证人员相同。

6.4.2 认证审核人员要求

应取的国家认监委确定的认证人员注册机构批准的 ISMS 审核员注册资格，选择具备信息安全管理相关工作经验的审核员。经过信息安全管理体系及相关知识培训。

7. 引用文件

7.1 相关规范/标准

(1) 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

(3) 质量管理体系认证实施规则

(4) ISO19011 管理体系审核指南

7.2 引用程序

1) 《认证申请及受理程序》

2) 《管理体系/服务/产品业务范围管理程序》

 深圳市深大国际认证有限公司 SHENDA INTERNATIONAL CERTIFICATION CO., LTD		版次	A/1
		文件编号	CTS SDIC-WI-TC121
文件名称	信息安全管理体系认证实施规则	生效日期	2025 年 8 月 28 日

- 3) 《审核策划操作规范》
- 4) 《审核过程管理程序》
- 5) 《认证决定、证书颁发和审核、审查、检查资料处理程序》
- 6) 《认证标识、认证证书、认可标识的使用管理规定》
- 7) 《暂停、撤销、扩大、缩小和终止认证程序
- 8) 《申诉和投诉处理管理程序》
- 9) 《文件和记录控制程序》

 深圳市深大国际认证有限公司 SHENDA INTERNATIONAL CERTIFICATION CO., LTD		版次	A/1
		文件编号	CTS SDIC-WI-TC121
文件名称	信息安全管理体系认证实施规则	生效日期	2025年8月28日

附件：ISMS/ITSMS 基础审核时间

ISMS 审核有效人数	ISMS 初审审核时间 (审核人日)	ITSMS 审核有效人数	ITSMS 初审审核时间 (审核人日)	总审核时间
1~10	5	1~15	3.5	
11~15	6	16~25	4.5	
16~25	7	26~45	5.5	
26~45	8.5	46~65	6	
46~65	10	66~85	7	
66~85	11	86~125	8	
86~125	12	126~175	9	
126~175	13	176~275	10	
176~275	14	276~425	11	
276~425	15	426~625	12	
426~625	16.5	626~875	13	
626~875	17.5	876~1175	15	
876~1175	18.5			
1176~1550	19.5			
1551~2025	21			
2026~2675	22			
2676~3450	23			
3451~4350	24			
4351~5450	25			
5451~6800	26			
68001~8500	27			

调整审核时间的因素见 CNAS-CC170:2015 B3.4

ISMS 增加减少审核时间的因素

序号	增加因素	增加的百分比	减少因素	减少的百分比
1.	认证范围所包含的产品服务过程数量较多,当数量 ≥ 3 时	10%	没有风险(注 a)或者低风险(注 b)的产品/过程,同时认证范围的产品与服务过程单一。	10%
2.	为了确认管理体系认证范围内永久场所的活动,需要访问临时场所的活动;	0.25 人日/个	过程只涉及单一的常规活动(例为了确认管理体系认证范围内 0.25 人日/个如,只有服务);	10%

 深圳市深大国际认证有限公司 SHENDA INTERNATIONAL CERTIFICATION CO., LTD		版次	A/1
		文件编号	CTS SDIC-WI-TC121
文件名称	信息安全管理体系认证实施规则	生效日期	2025年8月28日

3.	适用于 ISMS 的标准和法规数量很多,适用的专业法律法规之 5 个	10%	对组织已经有些了解(例如,如果组织获得了同一个认证机构的、另一个标准的认证),审核组在审核前可以查阅到相关的资料,了解组织	10%
4.	员工所说的语言超过一种(需要翻译或审核员个人无法独立工作),提供的文件使用了一种以上的语言;	10%/ 没多一种	高度成熟的管理体系。管理体系有效运行 2 个认证周期;(适用于转机构的组织)	10%
5.	ISMS 范围内所使用的风险控制措施 50%以上为外包或第三方控制;	20%	组织信息化程度较低,基本处于单机工作,信息系统较少(数量小于等于 2)时	10%
6.	认证范围内所包含的信息系统较多 (≥ 5) 信息化程度较高时	10%	客户的认证准备情况较好 (例如已经获得了另一个第三方认证方案的认证或承认);	10%

 深圳市深大国际认证有限公司 SHENDA INTERNATIONAL CERTIFICATION CO., LTD		版次	A/1
		文件编号	CTS SDIC-WI-TC121
文件名称	信息安全管理体系认证实施规则	生效日期	2025 年 8 月 28 日

附件 2 证书模板

ISO 27001 ISO 27001 ISO 27001 ISO 27001 ISO 27001 ISO 27001 ISO 27001 ISO 27001 ISO 27001 ISO 27001



CERTIFICATE

信息安全管理体系认证证书

证书编号: \${certno}

兹证明

XXXXXXXX 有限公司

统一社会信用代码: \${work_code}

注册地址: \${ep_addr}

经营/生产/加工地址: \${prod_addr}

建立的信息安全管理体系符合以下标准要求:

ISO/IEC 27001:2022

通过的认证范围如下:

\${cert_scope}

第一次
监督审核

第二次
监督审核

(本证有效期内每年需要进行监督审核, 证书是否继续有效, 以是否贴监督合格标志为准。)

签发人:



首次发证日期: \${s_date_cj}

本次发证日期: \${this_date_cj}

有效期至: \${e_date_cj}



认证机构名称: 深圳市深大国际认证有限公司

认证机构地址: 深圳市福田区园岭街道华林社区八卦三路八卦岭工业区 523 栋 307

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)、
深圳市深大国际认证有限公司官方网站 (www.sdgjrz.com) 上查询

