中天鸿图国际认证有限公司

信息安全管理体系认证实施规则

文件编号：ZTHT-GZ62：2024

版本：A/1

编制：技术部

审核：

批准：

2024-09-20发布　　2025-06-09修订　　2025-06-16实施

规则制/修订履历

制/修订日期	制/修订类别	版本/版次	修订内容说明	修订人/日期	审批人/日期
2024.09.20	■初始制订 □修订	A/0			
2025.06.09	■修订	A/1	三、认证人员要求第1条修改	胡贵玉	李海江

目 录

信息安全管理体系认证实施规则

一、适用范围

1.本规则对信息安全控制认证过程作出具体规定，明确信息安全控制认证过程的相关责任，保证信息安全管理认证活动的规范有效。

2.本规则用于信息安全控制认证活动。

3.本规则是中天鸿图国际认证有限公司（以下简称ZTHT）在信息安全管理体系认证活动中的基本要求，信息安全管理认证活动应当遵守本规则。

4. 信息安全管理体系在下文中用ISMS代替。

二、认证机构的要求

1.ZTHT是经国家登记主管机关依法登记注册、经中国国家认证认可监督管理委员会（CNCA）批准的第三方认证机构。

2.ZTHT建立内部制约、监督和责任机制，实现认证决定等工作环节相互分开，以符合公正性要求。

三、认证人员要求

（1）ISMS管理体系审核人员应取得中国认证认可协会的信息安全管理体系正式审核员资格，并保持资格有效。

（2）认证人员应遵守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。

四、认证依据

认证依据：ISO/IEC 27002:2022《信息安全、网络安全和隐私保护　信息安全管理体系 要求》

五、认证模式及认证流程

1 认证模式

ZTHT首先对认证受审核组织的信息安全管理体系进行初次审核，经过评定，确认是否批准认证注册；认证注册后，在认证周期内对获证组织的管理体系进行监督和再认证，确认是否持续满足认证要求。

2 认证流程

组织提交认证申请⇨申请受理⇨文件审核和现场审核⇨复核及认证决定⇨批准注册和颁发认证证书⇨证后监督活动⇨再认证

六、初次认证程序和要求

1 认证申请

1.1 申请组织具备基本条件

（1）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）已取得相关法规规定的行政许可（适用时）；

（3）了解信息安全体系的法律、法规、政策和标准等；

（4）申请组织已建立信息安全体系且运行时间在3个月以上，审核前应至少进行一次完整的内审和管理评审；

（5）生产、加工的产品或提供的服务符合中华人民共和国相关法律、法规和有关规范的要求；

（6）在一年内，未发生违反国家相关法律法规，未因负面情况受到相关监管部门处罚或媒体曝光，或未因负面情况而被其他相关认证机构撤销管理体系认证证书。

1.2 申请组织提交的文件和资料

（1）认证申请书；

（2）具有法律地位的证明文件（如：营业执照扫描件）；

（3）行政许可证明文件（适用时）；

（4）ISMS体系成文文件，如：管理策略、管理规定、实施细则、运行记录等。

（5）其他有关资料。

2 受理认证申请

2.1 申请评审

ZTHT根据申请认证的范围及场所、员工人数、完成认证活动所需时间和其他影响认证活动的因素，对认证申请组织提交的申请资料进行评审，并保存评审记录，综合确定是否受理认证申请。

2.2 评审结果处理

申请材料齐全并符合有关要求的，予以受理认证申请。未通过申请评审的，ZTHT书面通知申请组织在规定时间内补充和完善，或不受理认证申请并明示理由。

2.3 签订认证合同

ZTHT 决定受理认证申请后，在实施认证审核前，ZTHT 与申请组织签订具有法律效力的书面认证合同。

3 审核策划

3.1 审核时间

审核时间的确定，参照本机构ISMS审核时间有关要求执行。

3.2 审核组的组成

3.2.1 ZTHT根据ISMS体系认证覆盖的活动的专业技术领域选择具备相关能力的审核员组成审核组，必要时选择技术专家参加审核组，以提供技术支持。选择的技术专家应符合相关专业能力评价准则中关于技术专家的要求。

3.2.2 技术专家主要负责提供认证审核的技术支持，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。

3.3 审核计划

3.3.1 审核组长为每次审核制定书面的审核计划。审核计划包括以下内容：审核目的，审核准则，审核范围，现场审核的日期和场所，现场审核持续时间，审核组成员。

3.3.2 若审核覆盖范围覆盖多个场所,这些场所的ISMS体系所包括的要素相似，且这些场所都处于申请组织的授权和控制下，可以根据多现场组织审核抽样的有关要求，在审核中对这些场所进行抽样。如果不同场所的ISMS体系要素存在明显差异，则不能采用抽样审核的方法，应当逐一到各现场进行审核。

3.3.3 在审核活动开始前，审核组长应将审核计划提交申请组织确认，遇特殊情况临时变更计划时，将通知申请组织有关变更情况，并协商一致。

4 实施审核

4.1 审核过程

初次认证审核分一阶段审核和二阶段审核两个阶段进行，并包括文件审核和现场审核。

第一阶段审核应至少覆盖以下内容：

（1）结合现场情况，确认申请组织实际情况与ISMS体系成文信息描述的一致性，特别是体系文件中描述的方针和目标是否与申请组织的实际情况相一致；

（2）结合现场情况，审核申请组织人员理解和实施ISO/IEC 27002:2022 ISMS体系标准要求的情况，评价ISMS体系运行过程中是否实施了内部审核与管理评审，确认ISMS体系是否已运行并且超过3个月；

（3）确认申请组织建立的ISMS体系覆盖的活动内容和范围、申请组织的ISMS体系覆盖范围内有效人数、过程和场所，遵守相关法律法规及技术标准的情况；

（4）结合现场情况，确认企业结构能否满足ISMS体系运行的需要，各部门、各岗

位的职责是否明确；

（5）企业所有职工是否养成按体系文件或要求的行为习惯；

（6）与申请组织讨论确定第二阶段审核安排。

4.2 审核组应将第一阶段审核情况形成书面文件告知申请组织。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，要及时提醒申请组织特别关注。

4.3 第一阶段审核和第二阶段审核应安排适宜的间隔时间，使申请组织有充分的时间解决第一阶段中发现的问题。

4.4 第二阶段审核应当在申请组织现场进行。重点是审核资产管理体系符合ISO/IEC 27002:2022标准要求和有效运行情况，应至少覆盖以下内容：

（1）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。

（2）为实现方针而在相关职能、层次和过程上建立的各层级目标是否具体适用、可测量并得到沟通。

（3）对 ISMS 体系覆盖的过程和活动的管理及控制情况。

（4）申请组织实际工作记录是否真实，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）申请组织的内部审核和管理评审是否有效。

5 终止审核通报

发生以下情况时，审核组应向机构报告，经机构同意后终止审核。

（1）受审核方对审核活动不予配合，审核活动无法进行。

（2）受审核方实际情况与申请材料有重大不一致，ISMS 体系成文信息不符合现场实际。

（3）发现受审核方存在重大质量安全问题或其他严重违法行为。

（4）有证据证明受审核方 ISMS 体系运行未超过 3 个月或者无法证明超过 3 个月。

（5）其他导致审核程序无法完成的情况。

6 审核报告

6.1 审核组根据审核的结果，形成书面审核报告。审核报告描述审核活动的主要内容，包括：

（1）申请组织的名称和地址；

（2）申请组织活动范围和场所；

（3）审核的类型、准则和目的；

（4）审核组组长、审核组成员及其个人注册信息；

（5）审核活动的实施日期和地点；包括固定场所和临时场所；对偏离审核计划情况的说明，包括对审核风险及影响审核结论的不确定性的客观陈述。

（6）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，准确、具体、清晰描述，易于被申请组织理解。

（7）审核组对是否通过认证的意见建议。

6.2 保留用于证实审核报告中相关信息的证据，包括：相关事实的证据或记录、文字、照片或录像等资料。

6.3 本机构将在作出认证决定后30个工作日内将审核报告提交申请组织，并保留签收或提交的证据。

6.4 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，本机构将此报告及终止审核的原因提交给申请组织，保留签收或提交的证据。

7 不符合项的纠正和纠正措施及其结果的验证

7.1 对于审核中发现的不符合，审核组将出具书面不符合报告。对于一般不符合，申请组织应在一个月内分析原因，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。

7.2 ZTHT 将对申请组织所采取的纠正和纠正措施及其结果的有效性进行验证。对于严重不符合，申请组织应在 3 个月内采取纠正和纠正措施，ZTHT 将对纠正和纠正措施作现场验证。

8 复核

本机构组织复核人员对审核组提交的案卷的完整性、适宜性、充分性及有效性进行复核验证，若发现不满足要求情况，需报告不符合发现，并采取措施消除或降低不符合的负面影响，达到可接受的结果。

9 认证决定

9.1 ZTHT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。

9.2 认证决定人员为本机构雇员，与本机构签订有法律效益的劳动合同，在本机构的管理控制下，审核组成员不得参与对其审核项目的认证决定。

9.3 ZTHT会做好每项认证决定的记录，包括从审核组或其他来源获得的任何补充信息或澄清。

9.4 当有充分的客观证据证明申请组织满足下列要求的，可评定该申请组织符合ISMS

体系认证要求，ZTHT向其颁发符合ISMS体系认证证书：

（1）申请组织的体系符合认证依据的要求且运行有效。

（2）认证范围覆盖的产品和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。

9.5 当申请组织不能满足上述要求的，则评定该申请组织不符合ISMS体系认证要求,ZTHT将以书面形式告知申请组织并说明其未通过认证的原因。

七、监督审核程序

1.ZTHT将对持有ZTHT颁发的ISMS体系认证证书的组织（获证组织）进行跟踪，监督获证组织持续运行符合ISMS体系认证要求。

2.跟踪监督审核的最长时间间隔不超过12个月，当获证组织的ISMS体系发生重大变更，或企业发生重大服务质量安全问题或有其他与服务质量安全相关严重违法违规行为时，ZTHT将增加跟踪监督的频次或暂停该证书。

3. ISMS体系认证监督审核的时间根据ISMS体系认证审核时间管理规定的要求进行确定，并不少于初次审核人日数的1/3。

4.监督审核应在获证组织现场进行。

5.通常监督审核时至少覆盖以下内容：

（1）上次审核以来产品或服务提供绩效及影响产品或服务质量的重要变更、资源是否有变更；

（2）重要关键点是否按要求在正常和有效运行；

（3）对上次审核中确定的问题的改进情况；

（4）产品或服务涉及法律法规规定的，是否持续符合相关规定；

（5）获证组织总目标及各层级目标和产品或服务绩效的实现情况；

（6）获证组织对认证标志的使用或对认证资格的引用是否符合相关规定；

（7）是否及时接受和处理投诉；

（8）针对审核发现的问题或投诉的问题，是否有效改进。

6.对于监督审核中发现的不符合，获证组织应在规定时限内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。ZTHT将对获证组织所采取的纠正和纠正措施及其结果的有效性进行验证。

7.监督审核的审核报告按照“第六章”6.1要求。ZTHT将根据监督审核报告及其他相关信息，作出继续保持或暂停、撤销认证证书的决定。

八、再认证程序

1. ISMS体系认证证书有效期满前三个月，获证组织可向ZTHT提出再认证申请。

2. ISMS体系再认证程序与初次认证程序一致。在获证组织的管理体系及获证组织的内部和外部要素无重大变更时，再认证审核可省略一阶段审核。

3. ISMS体系再认证审核的时间根据ISMS体系审核时间规定的相关要求进行确定，并不少于初次审核人日数的2/3。

4.对于再认证审核中发现的不符合，获证组织应在规定时限内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。ZTHT将对获证组织所采取的纠正和纠正措施及其结果的有效性进行验证。

5.ZTHT按照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，向其颁发再认证证书。

九、暂停、恢复、撤销认证证书

1 暂停

获证组织有下列情形之一的，ZTHT将暂停其使用ISMS体系认证证书，暂停期限最长为六个月：

（1）ISMS体系持续或严重不满足认证要求；

（2）不承担、履行认证合同约定的责任和义务；

（3）被有关执法监管部门责令停业整顿；

（4）受到相关方对获证组织的重大投诉，但尚不需立即撤销认证证书；

（5）未能按规定间隔期接受监督审核；

（6）主动申请暂停认证证书。

2 恢复

（1）当暂停的获证组织在要求的时间内解决了造成暂停的问题，经确认符合相关规定，报总经理批准后恢复认证证书使用。

（2）在确定的认证资格暂停限期结束前，经ZTHT确认获证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，做出同意恢复认证资格的结论。

（3）恢复认证资格的获证组织要按照ZTHT的要求，从恢复决定之日起恢复使用认证证书和认证标志，以及任何其他对认证资格的引用。

3 撤销

获证组织有下列情形之一的，ZTHT将当撤销其ISMS体系认证证书：

（1）被注销或撤销法律地位证明文件或有关的行政许可证明和资质证书；

（2）出现重大的质量安全问题或有其他与服务质量相关的严重违法违规行为，经执法监管部门确认是获证组织违规造成；

（3）针对相关方的重大投诉，未能采取有效处理措施；

（4）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；

（5）虚报、瞒报获证所需信息；

（6）不接受相关监管部门或ZTHT对其监督。

（7）主动申请撤销认证证书。

十、认证证书和认证标志的使用

1 认证证书

1.1ISMS体系认证证书包括（但不限于）以下基本信息：

（1）获证组织名称、地址和统一社会信用代码（或组织机构代码）；

（2）认证覆盖的生产经营或服务的地址和业务范围；

（3）认证依据；

（4）证书编号；

（5）证书颁证日期、证书有效期；

（6）ZTHT名称、地址和认证标志。

（7）证书查询方式。

1.2. ISMS体系的认证证书有效期是三年,期间每年要接受发证机构的监督审核,三年证书到期后,要接受认证机构的再认证审核。

1.3. ZTHT按照认监委相关信息通报制度上报ISMS体系认证证书信息。

2 证书和标志的使用

申请组织通过认证并获得证书后，可以使用认证标志和证书。

3 使用规则

认证证书和认证标志的使用应符合本机构的管理规定。

4 违规使用的处理

获证组织对认证证书和认证标志存在误导性使用行为或违法行为，本机构保留视情况对获证组织采取暂停、撤销或进一步采取法律措施等权利。

十一、 信息公布

ZTHT将以书面方式通知获证组织有关暂停或撤销ISMS体系认证证书的信息和要求，并在ZTHT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。对于撤销认证证书的，ZTHT将收回撤销的ISMS体系认证证书，对于不能收回的证书，ZTHT将在公司

网站予以公布。被暂停或撤销ISMS体系认证证书的获证组织，不得以任何方式使用认证证书、认证标识或引用认证信息。

十二、申诉和投诉

获证组织对认证决定有异议时，本机构接受获证组织的申诉，并按申投诉处理程序进行处理，在60日内将处理结果形成书面通知申诉人。

书面通知应当告申诉人，若本机构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。

十三、认证记录管理

1. ZTHT应当建立认证记录保持制度，记录认证活动全过程并妥善保存。

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。

3. 可以电子文档方式保存记录。

4. 所有相关人员确认的记录，可以制作成电子文档保存使用，原件保存时间至少应当与认证证书有效期一致。