**ISO27001（GB/T22080）申请认证基本要求**

1、申请组织应未列入国家信用信息严重失信主体有关名录，且应建立符合标准要求的文件化信息安全管理体系，在申请认证之前应完成内部审核和管理评审，并保证信息安全管理体系有效、充分运行三个月以上；根据CNAS-CC01《合格评定管理体系审核认证机构的要求》(ISO/IEC17021-1)的要求，ISO27001（GB/T22080）认证审核由第一阶段审核和第二阶段审核组成。通常情况下，要求第一阶段审核活动应在申请认证组织的场所进行，如不安排第一阶段现场审核，应说明充分的理由。

2、第一阶段审核的目的包括：a)审核申请组织的管理体系文件；b)评价申请组织的运作场所和现场的具体情况，并与申请的人员进行讨论，以确定第二阶段审核的准备情况；c) 审查申请组织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；d)收集关于申请组织的管理体系范围、过程和场所的必要信息，以及相关的法律法规要求和遵守情况；e)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； f)结合可能的重要因素充分了解申请组织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；g)评价申请组织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申请组织已为第二阶段审核作好准备。

3、申请组织应向ZOHO提供信息安全管理体系运行的充分信息，例如：a)对于多现场应说明各现场的认证范围、地址及人员分布等情况，ZOHO将以抽样的方式对多现场进行审核； b)没有完全纳入信息安全管理体系认证范围内的服务或活动的接（如，发生在同一现场）， 应在拟认证的信息安全管理体系中予以说明；c)当决定认证的覆盖范围时，应考虑组织生产或经营许可证的范围以及相应资质证明。

4、ISO27001（GB/T22080）审核是一项收集客观证据的符合性验证活动，为使审核顺利进行，组织应为ZOHO开展初次认证审核、跟踪审核、监督审核、再认证审核、特殊审核以及解决投诉等活动做出必要的安排，包括文件审核、现场审核、调阅相关记录和访问人员等各个方面。

5、组织获证后，应遵守ZOHO的有关要求，在进行宣传时应仅就获准认证的范围作出申明， 并遵守ZOHO有关认证证书及认证标志使用规定；在监督审核时ZOHO将对认证证书及标志的使用情况进行审核；

6、当组织的信息安全管理体系出现变化，或出现影响信息安全管理体系符合性的重大变

动时，应及时通知ZOHO；ZOHO将视情况进行监督审核、换证审核或再认证审核以保持证书的有效性；

7、组织应向ZOHO提供有关与相关方信息沟通和投诉的记录，以及采取纠正措施的记录。

8、申请ISO27001信息安全管理体系认证需提供以下资料：

① 为政府部门提供信息技术外包服务的机构或组织若其认证范围涉及政府信息，须提供经工业和信息化主管部门同意的通知文件方可受理，否则认证范围不能涉及政府信息。

② 通信、金融、铁路、民航、电力等基础信息网络和重要信息系统运营单位应提交事先报行业主管或监管部门同意的文件，其他涉及国计民生的国有企业提交事先报国有资产监督管理部门同意的文件，涉及国家秘密的应提交报保密行政管理部门同意的文件。

③ 法律地位证明文件复印件（如营业执照等）。

④ 适用时，法律法规要求的相关资质证明，如生产许可证、强制性认证证书、施工资质证书等。

⑤ 申请认证范围多场所活动清单（场所位置、员工人数、已注册的场所）。

⑥ 组织机构一览表。

⑦ 信息安全方针、信息安全目标文件。

⑧ 阐述 ISMS 的程序及文件。

⑨ 范围声明。

⑩ 适用性声明。

⑪ 包括在范围内的应用信息系统的描述（附件表 2）。

⑫ 范围内的 IT 基本设备的描述（附件表 3）。

⑬ 信息安全风险准则（信息安全接受准则、信息安全风险评估实施准则）及信息安全风险处置计划。

⑭ 运行操作规程清单（如：信息标记规程、资产处理规程、信息传输策略和规程、变更规程、软件安装控制规程、维护系统安全工程的原则、信息安全事件响应规程、实现信息安全连续性的维护规程等）。

⑮ 来自于合同或其他来源的附加标准。

9、信息安全认证审核人天标准：

* 1. 引言

针对从事不同活动的、不同规模和复杂度的客户组织的ISMS 范围所进行的认证审核， 本附录为确定审核时间提供指南。

ZOHO需要针对每一个被审核方及其被认证的ISMS 识别初次认证审核、监督审核和再认证审核（复评）所需花费的审核时间。在审核策划阶段，使用本附件可以确保使用一致的方法来确定适当的审核时间。同时，本附件的指南允许基于审核进程（尤其是第一阶段审核）中的发现和所考虑ISMS 范围的复杂性进行调整。

* 1. 确定审核时间的程序

经验表明，ISMS 的范围、所涉及雇员的数量（见本附件表1 审核时间表）、规模、特性、复杂性和潜在信息安全风险的严重性对任何一个特定审核所需的时间有决定性影响。

CNAS-CC17列出了可能影响审核时间配置的因素和准则，在合同评审过程中，需要参照这些准则以及其他因素对审核时间的配置所产生的潜在影响。需要注意的是，在确定审核时间时，宜考虑所有这些因素，而不能孤立地使用本附件提供的审核时间表。

下列示例说明了可能影响审核时间的因素的详细情况：

* + - 与 ISMS 范围的规模有关的因素（例如，使用的信息系统的数量、处理的信息量、用户的数量、特权用户的数量、IT 平台的数量、网络的数量及它们的规模）；
		- 与 ISMS 的复杂程度有关的因素（例如，信息系统的关键度、ISMS 的风险状况、所操作和处理的敏感和关键信息的多少及类型、电子交易的数量及类型、所有开发项目的数量和规模、远程工作的范围、ISMS 文件化的程度）；
		- 在 ISMS 范围内开展的业务类型，以及关于这些业务类型的安全、法律、法规、合同和业务要求；
		- 在 ISMS 各部分的实施过程中，所应用的技术的水平和多样性（例如，已实施的控制措施、文件和（或）过程控制、纠正和（或）预防措施、信息系统、IT 系统、网络等，而无论他们是固定的、移动的、无线的、外部的或内部的）；
		- 在ISMS 范围内场所的数量，这些场所的异同程度如何，是否所有的场所都被审核还是抽样；
		- 经证实的以往 ISMS 绩效；
		- 在ISMS 范围内，所使用的外包和第三方安排的程度，以及对这些服务的依赖程度；
		- 适用于认证的标准、法律和法规，以及任何可能适用的行业特定要求。

由于信息安全管理体系透过特定的ISMS 需要（例如，ISMS 方针、风险管理、ISMS 控制目标和控制措施）而增加了要求，一个信息安全管理体系的认证通常要比质量管理体系或环境管理体系认证花费更多的时间。ZOHO应：

* + - 审核客户组织用来确定其信息安全风险和影响的严重性所使用的方法的健全性和一致性；
		- 确认客户组织为达到合规性（所有相关的法规和其他适用于 ISMS 的要求）所设计的管理体系
		- 有完成此任务的能力，并且该管理体系得以实施和保持；
		- 确认客户组织正确选择和实施了控制目标和控制措施，其有效性已被测量，并且以“对安全失效的预防和适当的响应”为目的的过程是健全的且得以遵守；
		- 确认客户组织满足关于客户组织 ISMS 的文件要求；
		- 回应了由第一阶段审核所产生的增加的需求。
	1. 审核时间表

9.3.1 通则

表1 给出了初次审核天数的平均数量（在此处及后面的内容中，这个数量包括第一阶段和第二阶段审核的时间），经验表明，对于给定雇员数量的ISMS 范围来说，这一数量是适当的。经验还表明，对于相似规模的ISMS 范围，有些需要多一些的审核时间，有些需要少一些的审核时间。

对每一认证所需时间的变化取决于包括规模、审核范围、后勤、组织的复杂性和审核准备状态在内的诸多因素。ZOHO需在合同评审过程中检查这些因素及其他因素对所配置审核时间的潜在影响。因此，审核时间表不能孤立地使用。

表1 提供了可用于审核策划的框架，该表以所有班次雇员总数作为起始基数，根据适用于被审核ISMS 范围的因素的重要性对该基数进行调整，对每一因素赋予增、减权重以修正基数。

附件表 1 ：ISMS 审核时间表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 雇员数量 | QMS 初次审核审核时间（审核人日） | EMS 初次审核审核时间（审核人日） | ISMS 初次审核审核时间（审核人日） | 增加或减少的因素 | 总时间 |
| 1 ~ 10 | 2 | 3 | 5 | 见本附件 |  |
| 11 ~ 25 | 3 |  | 7 | 第2条 |  |
| 26 ~ 45 | 4 | 6 | 8.5 | “确定审核 |  |
| 46 ~ 65 | 5 |  | 10 | 时间的程 |  |
| 66 ~ 85 | 6 |  | 11 | 序” |  |
| 86 ~ 125 | 7 | 8 | 12 |  |  |
| 126 ~ 175 | 8 |  | 13 |  |  |
| 176 ~ 275 | 9 |  | 14 |  |  |
| 276 ~ 425 | 10 |  | 15 |  |  |
| 426 ~ 625 | 11 | 12 | 16.5 |  |  |
| 626 ~ 875 | 12 |  | 17.5 |  |  |
| 876 ~ 1175 | 13 |  | 18.5 |  |  |
| 1176 ~ 1550 | 14 |  | 19.5 |  |  |
| 1551 ~ 2025 | 15 | 18 | 21 |  |  |
| 2026 ~ 2675 | 16 |  | 22 |  |  |
| 2676 ~ 3450 | 17 |  | 23 |  |  |
| 3451 ~ 4350 | 18 |  | 24 |  |  |
| 4351 ~ 5450 | 19 |  | 25 |  |  |
| 5451 ~ 6800 | 20 |  | 26 |  |  |
| 6801 ~ 8500 | 21 |  | 27 |  |  |
| 8501 ~ 10700 | 22 |  | 28 |  |  |
| ＞ 10700 | 沿用 |  | 沿用 |  |  |
|  | 以上规律 | 以上规律 |  |