附件一： ISO27001 信息**安全**管理体系审核时间表

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。

2， 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（下面将更加详细地解释）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。3 审核时间表
  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。

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 |  |

**说明：**

1，在表1中涉及的“雇员”是指其工作活动与ISMS 范围有关的所有人员。所有班次雇员的总数是确定审核时间的起点。 2，雇员的有效数量包括审核期间在场的非长期（季节性的、临时的及分包的）员工。认证机构宜与拟审核的组织就最好地反映组织全部范围的审核时间达成一致意见。适当时，可考

虑季度、月份、星期、日期和班次。

3，对于非全日制雇员，宜根据其工作小时数与全日制雇员的比较，并比照全日制雇员处理。

4，“审核时间”包括审核员或审核组在第一阶段审核、第二阶段审核和策划（适当时，包括非现场文件评审）时所使用的时间，其中包括接触组织、人员、记录、文件和过程所用的时间，以及编制审核报告所用的时间。审核策划和编制审核报告一起所用的“审核时间”通常不宜使总的现场“审核时间”减少到表1所给出时间的70%以下。当策划和编制审核报告而需要增加时间时，不能以此为由而减少现场审核时间。审核员旅途时间未计在内，这应在表中所给出的审核时间的基础上另外增加。

注1：70%是基于ISMS 审核经验所考虑的因素。

5，如果使用了远程审核技术（例如，交互式基于网络的协作、网络会议、电话会议和/或组织过程的电子验证）与客户组织接触，这些活动宜在审核计划中加以识别，可以考虑将其作为现场审核时间的一部分。

6，如果审核计划中远程审核活动占据大于30%的现场审核时间，宜有理由证明审核计划是适当的，并在实施前得到有关认可机构的专门批准。

注2：现场审核时间是指分配给单独场所的现场审核时间。远程场所的电子审核被视为远程审核，即使电子审核是在组织的物理场所进行。

7，表1 中的“审核时间”以用于审核的“审核人日”表示。典型的一个审核人日是一个完整的正常工作日。

8，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。宜适时地核查其所策划的监督审核时间，以考虑组织的变更及管理体系的成熟度等，至少宜在再认证审核时进行该核查。 9，用于再认证审核的全部时间还取决于标准ISO17021 的9.4.1.2 中所确定活动的结果。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，大约是初次认证审核时间的2/3。

10，再认证审核时间遵照上述并超出例行的监督审核时间，但当再认证审核与计划的例行监督审核一起实施时，再认证审核也要满足监督审核的要求。 11，对于明确了雇员数量的典型ISMS 范围，一旦确定了所需审核时间的常规基点后，除了本附件已经列出的事项外，还需考虑进行一些调整，以便解决一些差异，这些差异可能影响到为实施一个有效的ISMS审核所需的实际审核时间。 12，需要增加审核时间的因素，例如（不限于）：

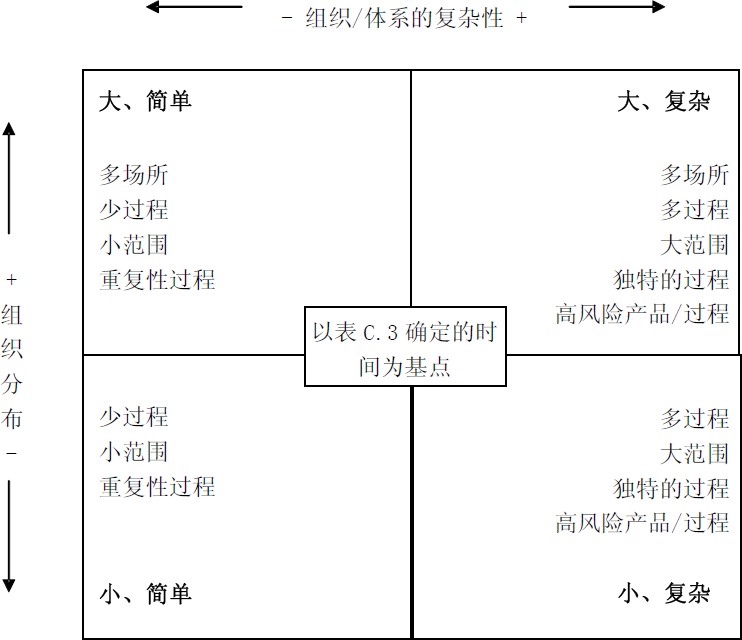
* + - 在 ISMS 范围之中复杂的后勤条件，涉及到不止一处建筑物或场所；
    - 员工语言超过一种（需要翻译或影响审核员个人独立工作）；
    - 法规要求高；
    - ISMS 覆盖了极其复杂的过程或大量的独特活动；
    - 过程中同时包括硬件、软件、过程和服务；
    - 需要访问临时场所的活动以确认管理体系需认证的永久场所的活动，（见下注3）。13，允许减少审核时间的因素，例如（不限于）：
    - 没有风险或者有低风险的产品和（或）过程；
    - 对组织已经有些了解（例如，如果组织已经按照其他标准通过了同一个认证机构的认证）；
    - 客户组织的认证准备情况（例如，已经被其他的第三方认证方案所认证或承认）；
    - 过程只涉及单一的常规活动（例如，只有服务）；
    - 成熟的管理体系；
    - 大部分雇员从事相同的简单任务。

注3：在认证申请者或被认证组织于临时场所提供其产品或服务时，将对此类场所的评价纳入到认证审核和监督方案中是十分重要的。

14，临时场所是认证文件所注明的场所和（或）位置以外的位置，其活动在认证范围内，并在规定的时间周期內实施。此类场所范围可从大项目管理场所到较小的服务或安装场所。是否需要访问这些场所及对其抽样范围的决定宜基于由于系统不符合所引起的未能满足需要或期望的产品或服务的风险评价。所选择的场所样本宜考虑到活动的规模和类型，体现出组织的能力需求和服务变化的范围，以及项目进展的不同阶段。

15，宜考虑ISMS 范围、过程和产品（包括服务）的所有属性，并公平地对有效审核所需增加或减少审核时间的合理因素进行调整。增加时间的因素可被减少时间的因素冲抵。在任何情况下，对审核时间表中所提供时间的调整，应保持足够的证据和记录来证实其变化的合理性。

下图展示了在表 1 中的审核时间的增加因素和减少因素的潜在交互作用。



1