ISO 27001:2005 – 标准注释及 IRCA ISMS 审核员转换要求

范围:

本文:

1. 说明了保持 IRCA 信息安全管理审核员注册资格及按新 ISO/IEC 27001:2005 标准实施审核时应满足的 CPD 要求。
2. 概括了 ISO 27001:2005 对于信息安全管理体系审核员的影响。
3. 说明了与 BS 7799-2:2002 相比，ISO 27001:2005 标准的具体变化。

感谢:

对于 Brian Henry 先生（IRCA 信息安全管理体系评审员）为制定本文所做的工作和努力 IRCA 表示感谢。

1. ISMS 审核员注册转换

ISO 27001:2005 的公布是官方正式发表 ISMS 要求的里程碑。我们要求 IRCA 注册 ISMS 审核员不仅要理解标准，而且也应了解标准的变化内容对于 ISMS 审核活动的影响。

新标准ISO 27001:2005和BS 7799:2002间的区别并不难区分。因为在标准修订阶段，为了便于今后的转换，标准制定人员已尽量考虑了两个标准的兼容性和一致性。 ISO/IEC27001:2005和BS 7799-2:2002之间的区别主要在于编辑和格式化方面，较2002版和BS 7799-2:1999间的差异要小得多。

然而，应该注意的是审核员如果没有对 ISO/IEC 17799:2005 透彻的理解就不可能有效地按照 ISO/IEC27001:2005 进行审核。因为该标准规定了 ISMS 指南、总原则和操作准则。

ISO 17799:2005 是在 2005 年六月发布的。与该标准前一版本 ISO/IEC 17799:2000 相比，它新增了 17 条实施标准的建议和最佳操作指南，并对少部分旧条款加以合并和/或删除。新标准总共有 134 项实施建议和指南，而在 ISO 27001:2005 附录“A”中则相应包含了 38 个控制目标和 134 条控制要求。

ISO/IEC 17799:2005 的编号将在短期内不会发生变化。目前计划在 2007 年 4 月发布 ISO/IEC 27002 标准号，但标准的内容将保持不变。

IRCA 注册 ISMS 审核员转换要求

所有 IRCA 注册 ISMS 审核员在按新标准实施可接受的审核活动***之前***应完成至少 **4 小时的持续专业发展活动 (CPD)** 。

专业发展活动应能使 ISMS 审核员能具备并理解 SIO/IEC 27001:2005 和 ISO/IEC 17799:2005 标准（及其它引用标准）知识以便使他们按 ISO 17799:2005 要求实施审核的技能得到提高。

审核员应向 IRCA 提交有关 CPD 证明材料及相关 IRCA/173 专业发展记录（经验证核实的）以及 IRCA/106 审核记录证明审核是按照 ISO/IEC 27001 标准实施的。

为了便于审核员完成转换活动，审核员可以与升级或复查换证同时进行转换。

转换何时开始？

我们将从 2006 年元月一日起开始受理转换 CPD 和按 ISO/IEC 27001:2005 进行的审核经历。

IRCA 将接受哪种 CPD 活动？

我们不要求 ISMS 审核员接受专门的转换 CPD 活动。审核员可以通过若干种途径完成满足 IRCA 要求的 CPD 活动；

- 自学，阅读新标准及相应的支持性文件、出版物。
- 阅读（本文和其它相关文章）
- 岗位培训
- 公司内部的培训和讲座
- 参加相关 ISMS 会议、研讨会
- 完成并通过专门的 ISO/IEC 27001 标准 ISMS 培训课程

IRCA 将提供可接受的 ISO/IEC 27001:2005CPD 活动和研讨会清单。但审核员可进行的 CPD 活动将不仅限于清单上的培训，我们也有可能接受其它形式 CPD 活动。 这些活动通常由 IRCA 批准的培训机构或 OEAs 提供，由于 IRCA 没有对它们进行正式批准，尽管我们承认这些 CPD 活动，但这些活动将不受 IRCA 的控制。上述清单一旦正式公布，您可直接通过我们的网站 www.irca.org 查询有关的课程和活动。 或者，审核员也可以通过电话+ 44（0）207 245 6833 与 IRCA 联系获得上述信息。

2. 介绍 – ISO 27001:2005 对审核员的影响

ISO 27001:2005 发布是业内人士期待已久的，该标准是基于 BS 7799-2:2002 制定出来的。新标准的出台代表了 ISMS 认证国际认可及其发展过程中重大的一步。它于 2005 年 10 月 15 日发布，而原 BS 7799-2:2002 也因此被取消作废。

人们预计 ISO 27001:2005 的出现将吸引那些欲实施 ISMS 组织极大的兴趣，这些组织将要求按新标准获得认证。目前 ISMS 认证主要在英国和日本比较盛行，新标准的出台将使这一范围扩大到世界其它国家和地区。

目前世界上大约有 2000 张按 BS 7799-2:2002 标准发放的证书，而认可机构正在制定 ISO 27001:2005 过渡期间认证机构转换要求。目前来看转换截止日期将是 2007 年 10 月 31 日。

对于现有的 BS 7799-2:2002 获证企业，对于 ISO 27001:2005 标准的评审将在日常的监督审核中完成。而新申请的企业将直接按 ISO 27001:2005 进行审核。

审核员应知道 ISO 27001:2005 标准只是 ISO/IEC 27000 系列标准中第一个发布的标准。而还有下列许多标准已经或正在拟定过程中：

ISO/IEC 27000 ISMS 原则和术语

ISO/IEC 27002 ISMS 安全技术- 操作准则 （ISO/IEC 17799:2005）

ISO/IEC 27003 ISMS 实施指南

ISO/IEC 27004 ISMS 计量制及测量

ISO/IEC 27005 ISMS 风险管理

ISO/IEC 27006 ISMS 业务持续性和灾难恢复服务

人们预计 ISMS 将在世界上更广泛的地区及企业得到蓬勃发展。毫无疑问，ISMS 审核员因此在不久的将来获得新的机会和挑战，为此，他们应做好适当的准备去迎接这些挑战。

3. ISO 27001：2005 要求-主要变化综述

以下是各条款要求的主要变化及对审核员的影响。

引言及介绍

没有大的变化。ISO 27001:2005 仍与 BS 7799-2:2002 一样对标准进行了总体的介绍。仍继续沿用过程方法的要求，只是增加了更多的解释内容。

仍重点强调标准与 ISO 9001:2000 和 ISO 14001:2004 的一致性，并说明标准的制定旨在使组织能实现 ISMS 与相关管理体系要求的一致或兼容。

范围 – 1

本条款指出标准适用于所有组织。并强调企业为实现标准符合性，标准的 4-8 条中不能删剪的强制条款。

规范性引用文件 – 2

ISO 27001:2005 将直接引用 ISO/IEC 17799:2005。

术语和定义 – 3

标准增加了部分定义，而其他定义或经修改或替换以便与其他标准（如 ISO/IEC13335-1：2004 和 ISO/IEC TR 18044：2004）实现统一。此外，部分定义也经修订避免了对于标准的误解。

总则 – 4.1

本条款更明确了对于文件化 ISMS 的运行、监控和评审要求。

建立和监控 ISMS - 4.2

4.2.1 建立 ISMS

a) 规定了范围 – 本条款要求经修订以确保范围声明不仅包括 ISMS 的范围，还包括体系的界限。原版本的标准确实隐含了对体系界限的要求，但新标准则明确要求说明体系的界限并说明任何剪裁内容的详细情况。

b) 定义 ISMS 方针政策 – 微小的文件编辑上的变化 – 现经修订确保其与组织战略风险管理内容一致。

增加了新“注释”说明 ISMS 方针应是信息安全方针的组成部分。

c) 定义组织的风险评估方法- 内容结构被重新组合，增加了一个内容清单。该清单明确指出风险评估方法的选择应能产生有可比性且能复现的结果。

增加了新“注释”说明风险评估方法见 ISO/IEC TR 13335-3。

d) 识别风险 – 内容没有变化，但边注说明了“资产拥有方”的含义。

e) 分析和评估风险 – 旧版本称为“评价风险”- 只是文字编辑上的变化如“业务伤害”现改为“对组织的业务影响”。

g) 选择控制目标 – 内容相应地增加以说明控制目标的选择和实施，目标的监控应满足风险评估和风险处置过程提出的要求。增加了一句话，要求选择目标时应考虑接受风险准则以及法律法规、合同要求。

增加了控制目标的选择和监控要求，经修改的“注释”对附录 A 的内容和目的进行了解释。

h)和 i) 获得管理层对实施和运行 ISMS 的批准和授权 – 原内容经重组。

j) 拟定可应用性声明 – 增加原内容并将其重新格式化为一内容清单，说明可应用性声明应包括现行的控制目标及其监控。

新“注释”说明可应用性声明应提供风险处置相关决定的概述，并在需要忽略某种风险的情况时说明原因，以避免错误地遗漏对某个风险的控制。

4.2.2 实施和运行 ISMS

a) 制定风险处理计划 – 适宜的管理措施中增加了“资源”一词。

d) 定义如何测量 – 除了实施和利用 ISMS 要求以外，新标准还要求界定如何测量一个或一组控制措施的有效性的方法，并说明如何运用这些测量方法评价控制过程的有效性（即产生可比性和能复现的结果）。增加了新的“注释”内容，指出控制有效性的测量应能说明既定控制目标的完成情况。

f) 管理运行 – 增加了 ISMS 修饰词，说明需管理运行的领域。

g) 管理资源 – 增加了 ISMS 修饰词，说明需管理资源的领域。

4.2.3 监控和评审 ISMS

a) 执行监控程序 – 要求程序的实施从简单的监控到对程序的评审。在分条款 a) 2 中“失败的”一词被替换为“未遂的”以确保标准覆盖所有不符合标准的情况和事故。

增加了分条款 a）4，要求监控和评审应有助于安全事件的检测，并通过统计指数预防安全事故的发生。分条款 5 经修改要求组织应确定违反安全要求避免措施的有效性。

b) 实施定期的评审 – 本条款经修订要求组织定期的评审活动应包含有效性测量结果。同时，原标准的“安全方针”变为“ISMS 方针”，这将影响 ISMS 的相关评审内容。

c) 控制有效性的测量 – 这是原标准监控和评审 ISMS 要求的附加要求。新标准要求对控制有效性进行测量以验证安全要求是否得到满足。

d) 评审风险评估 – 内容经修改规定应按计划的周期对风险评估进行评审。分条款 d）5 对原标准要求进行了补充，要求在评审时应确定对已实施的、处理违反安全要求纠正措施的有效性进行评价。分条款 d)6 增加了“修订的合同义务”一词

e) 实施内部 ISMS 审核 – 内容没有变化，但索引了标准新增的第 6 部分。新“注释”说明什么是内审及谁实施内审。

f) 实施管理评审 - 删除了每年至少一次的频次要求。

g) 更新安全计划 – 新要求

4.2.4 保持和改进 ISMS

c) 沟通措施和改进 – 内容经修改，规定沟通的内容不仅限于措施或改进的结果，还应有适当的深度，并说明将如何实施措施和完成改进活动。

文件化要求 – 4.3

4.3.1 总则

新增加的介绍段落详细解释了管理决定记录中应包含的内容，以确保各项措施可以追溯到管理决定和方针，同时保证结果的复现性。标准明确强调了证明一系列活动内在关系的重要性，如从选择控制方法到风险评价结果及风险处置过程，最终追溯到ISMS方针和目标。

a) 文件化声明- 将“ISMS 方针和目标”替代“安全方针和控制目标。”

b) ISMS 范围 – 删除了“ISMS 程序和控制”。

c) 增加了“ISMS 的支持程序和控制”。

d) 对于风险评估方法的描述 – 内容更加明确，确保风险评估方法说明包含在文件体系中。

g) 文件化程序 – 增加相应的要求说明测量控制有效性的方法。

4.3.2 文件控制

d) 确保相关版本 – 由“相关文件最新版本”变为“适用文件的相关版本”。

f) 确保相关方能获得文件 – 内容经修订澄清确保需要文件的各方能获得文件，并能按照适宜的文件程序转化、储存或销毁文件。

4.3.3 记录控制

第一段的第二句变为“它们应被保护和控制”。第三句话经修改包括“法规要求和合同义务”。第五句增加了控制应“予以文件化和实施”。本要求原 BS 7799-2:2002 的最后一句被删除。

第二段在“安全事故”前增加了“重大”一词。

新标准给出了记录内容实例。

管理职责 - 5

5.1 管理承诺

a) 建立 ISMS – “信息安全方针”一词由“ISMS 方针”替代，因为标准的焦点涉及 ISMS 领域。

b) 确保 ISMS - “信息安全方针”一词由“ISMS 方针”替代，因为标准的焦点涉及 ISMS 领域。

e) 提供充分的资源- ISMS 活动的描述与 ISMS 的定义一致。

f) 准则的决定 – 这一要求经修订包括有关“接受风险和可接受风险级别准则”方面的决定。

g) 确保内审 – 这是对管理承诺的澄清和附加内容，以确保内部 ISMS 审核的实施。包括引入新的 6 条款。

5.2 资源管理

5.2.1 资源提供

a) 建立、实施、运行 – 内容增加包括与 ISMS 相关的整个系列的活动。

5.2.2 培训意识和能力

b) 提供培训 – 内容经修改包括采取其它要求的可能性（如：聘用有能力的人员）。这一变化使标准与 ISO 9001:2000 一致。

c) 评价有效性 – 这一要求简化为：“评价所采取活动的有效性”。

内部 ISMS 审核 – 6

原 BS 7799-2:2002 的 6.4 条款变为 ISO 27001:2005 的主条款，除了以下内容外其它内容仍保持不变：

第四段 – 第二句的“改进活动”变为“跟踪活动”。

增加了新的“注释”说明见 ISO 19011:2002 了解质量和或环境管理体系审核指南。

ISMS 管理评审- 7

由于新增的 6 条款，本条款的编号相应发生变化。

7.1 总则 – 编号发生变化 – 第一段 – 在第一句“时间间隔”（从原（BS 7799-2:2002 中删除）前增加了“至少一年”的时间限定。

同时“安全方针和安全目标”被替换为“信息安全方针和信息安全目标”以便说明评审的内容。

7.2 评审输入 – 编号的变化 – 内容简化为“应包括管理评审的输入。”

7.3 评审输出 – 编号的变化

b) 风险的更新 – 增加了“更新风险评估和风险处置计划的更新”这一要求

c) 程序的修改 - 内容增加了“程序和控制的变化”

c) 5 合同义务 – 被澄清

c) 6 风险级别 – 增加了“风险的级别和/或风险接受准则”

e) 方法的改进 – 内容的澄清。

ISMS 改进 – 8

由于新增的 6 条款，条款号发生变化。

8.1 持续改进

第一段 - 在“安全目标”前增加了“信息”一词。

8.2 纠正措施

条款号发生变化 – 原“与 ISMS 实施和运行相关”被替换为“按 ISMS 要求”

a） 识别不符合 – 内容被简化。

8.3 预防措施

第一段 – 条款号发生变化 – “防止未来的不符合”被改为“按 ISMS 要求”。
b) 评价需求 – 新内容

第二段 – 新增段落，要求组织应识别变化的风险同时还应识别相应的预防措施。本条款要求主要指发生重大变化的风险。

附录 A
被更新 – 控制目标和控制与 ISO/IEC 17799:2005 中的指南一致。

附录 B
没有包括 BS 7799-2:2002 的内容，将在 ISO/IEC 27003 ISMS 实施指南的制定时使用。原 B.1 表成为 ISO/IEC 27001:2005 ISO/IEC 27003ISMS 实施指南的附录 B。

附录 C
本附录被更新以与 ISO 9001:2000 及 ISO 14001:2004 相应的变化保持一致。

附录 D
原附录被删除

索引

本部分被更新以体现相关标准和其它出版物的最新变化。

您如果有任何问题，请通过 registration@irca.org 与我们联系.

了解有关 IRCA ISMS 审核员注册信息，请访问 www.irca.org.

获取我们免费的审核刊物《*IRCA 信息*》*请致函*
registration@irca.org 或登陆 www.irca.org.

End