中国合格评定国家认可委员会文件

认可委（秘）（2012）4号

关于发布CNAS-CC17：2012《信息安全管理体系认证机构要求》及其转换实施安排的通知

各信息安全管理体系认证机构及相关人员：

中国合格评定国家认可委员会（CNAS）于2012年1月10日发布了CNAS-CC17:2012《信息安全管理体系认证机构要求》（等同采用ISO/IEC 27006:2011），文件将于2012年4月1日实施并代替CNAS-CC17:2009。

现就CNAS-CC17:2012的实施安排以及信息安全管理体系（ISMS）认证机构认可转换相关工作的安排予以通知。

一、CNAS-CC17:2012的转换期

已经依据CNAS-CC17:2009准则获得CNAS认可的ISMS认证机构，应于2013年2月1日前完成CNAS-CC17:2012准则认可转换的工

作。转换期自2012年4月1日至2013年1月31日。

截止至2013年2月1日，依据CNAS-CC17:2009认可的ISMS认证机构若没有完成CNAS-CC17:2012认可转换，其ISMS认可资格将被撤销。

二、转换准备

（一）CNAS的转换准备

自文件发布之日起至2012年3月31日之前,CNAS将为转换工作做出相应准备，包括配套规范文件的修订准备、转换评审工作流程策划以及依据CNAS-CC17:2012实施评审所需的人员和资源准备等。

（二）认证机构的转换准备

已获得CNAS认可的ISMS认证机构，应识别CNAS-CC17:2012的新要求，及其与ISMS认证机构自身管理体系之间的差异。为符合CNAS-CC17:2012的要求，认证机构应制定过渡计划，确定需要对其管理体系进行的修改，并确定完成这些修改所需的时间。ISMS认证机构应确保为满足CNAS-CC17:2012要求，对其管理体系的修改调整及实施工作于2013年2月1日前完成。

在此基础上，认证机构与CNAS商定转换评审及认可转换的具体安排。

三、转换实施

CNAS-CC01:2011与CNAS-CC17:2012共同作为CNAS对ISMS认证机构的认可准则，CNAS-CC17:2012遵循了CNAS-CC01:2011的文件

结构并对ISMS认证机构提出了增加的特定要求和指南。因此，ISMS认证机构申请CNAS-CC17:2012的转换，应确保CNAS-CC01:2011的相关要求也得到了满足。

ISMS认证机构的认可转换将采用CNAS-CC17:2012与CNAS-CC01:2011转换结合进行的方式。

（一）申请认可转换

自2012年4月1日起至2012年10月31日，CNAS接受已认可ISMS认证机构CNAS-CC17:2012转换的认可申请。至2012年11月1日后不再接受已认可ISMS认证机构针对CNAS-CC17:2012的认可转换申请，未申请转换的ISMS认证机构其依据CNAS-CC17:2009的认可资格将于2013年2月1日撤销。

（二）转换实施

CNAS受理ISMS认证机构对CNAS-CC17:2012的转换申请后，将安排对认证机构进行转换评审，评审内容包括CNAS-CC17:2012及CNAS-CC01:2011等认可规范的相关要求。若认证机构申请CNAS-CC17:2012转换与其他管理体系的CNAS-CC01:2011转换评审一同进行，CNAS将策划并实施结合评审。

（三）不符合与认可转换决定

在CNAS-CC17:2012转换评审中发现的不符合可能包括对CNAS-CC17:2012新要求的不符合，以及对CNAS-CC17:2009原要求的不符合，转换评审中对CNAS-CC17不符合的关闭验证时限不超过一个月。其中，ISMS认证机构对CNAS-CC17:2012新要求的不合符

仅用来评价认证机构CNAS-CC17:2012转换实施的完成情况，仅在确定ISMS认可转换结果的过程中起作用。

在2013年2月1日前，对完成认可转换评审的认证机构，CNAS将就其ISMS领域认可转换作出决定。

四、认证机构新申请ISMS领域认可的安排

自本通知发布之日起,对尚未获得 ISMS 领域认可资格的认证机构,CNAS 将暂停接受其在 ISMS 领域的认可申请;CNAS 将于 2012 年 4 月 1 日起受理此类认证机构在 ISMS 领域的认可申请,并按照 CNAS-CC17:2012 等相关要求实施认可。

CNAS-CC17:2012《信息安全管理体系认证机构要求》可在 CNAS 网站“认可规范”栏目获得，请相关认证机构及相关人员遵照执行。

附件：CNAS-CC17:2012《信息安全管理体系认证机构要求》修订内容对照表

二〇一二年一月十日

主题词：文件　发布　实施安排　通知

抄送：本秘书处：存档（2）。

中国合格评定国家认可委员会　　2012 年 1 月 10 日印发

录入：田珊珊　　校对：任青钺

附件：

CNAS-CC17:2012《信息安全管理体系认证机构要求》修订内容对照表

序号	条款	CNAS-CC17:2009	CNAS-CC17:2012	说明
1	前言	~~ISO/IEC 27006:2007~~	ISO/IEC 27006:2011	修改（3 处）
2	前言	——	本文件代替了 CNAS-CC17:2009。	增加
3	引言	CNAS-CC01:2007； ISO/IEC17021:2006	CNAS-CC01:2007→CMAS-CC01:2011 ISO/IEC17021:2006→ISO/IEC17021:2011	修改（6 处）
4	引言	使用“宜”（should）这一术语~~以表示尽管本文件中与 CNAS-CC01:2007 和 GB/T 22080-2008 的要求相对应的条款是指南性的，构成了对这两个文件中要求的应用指南，但仍然期望认证机构采纳。~~	使用“宜”（should）这一术语表示建议。	修改
5	引言	~~认证机构在贯彻本文件的指南性条款时所形成的任何不同，可视为一个例外。针对这种不同，只有当认证机构向 CNAS 证实那些例外以等效的方式满足 CNAS-CC01:2007 和 GB/T 22080-2008 的相关条款要求以及本文件的意图时，并仅在具体问题具体分析的基础上才被允许。~~	——	删除
6	引言	——	注：本文件中“管理体系”和“体系”可以互换使用。管理体系的定义见GB/T 19000-2008（ISO 9000:2005，IDT）。请勿将本文件中使用的管理体系与其他类型的系统混淆，例如IT系统。	增加
7	——	正文及附录中各处对 CNAS-CC01:2007 的引用。	统一修改为 CNAS-CC01:2011。（含 ISO/IEC 17021:2011）	修改（38 处）
8	2	~~GB/T 19011 质量和（或）环境管理体系审核指南（GB/T 19011-2003，ISO/IEC 19011:2002，IDT）~~	ISO 19011:2011 管理体系审核指南	修改
9	5.2.1b）	…认证机构~~宜~~仅限于提供可以公开自由获取的通用的信息和建议，即他们~~不宜~~针对具体公司提供那些违反下面 c)要求的建议；	…认证机构应仅限于提供可以公开自由获取的通用的信息和建议，即他们不应针对具体公司提供那些违反下面 c)要求的建议；	修改
10	5.2.1c）	…提供或公开发布有关认证机构对认证审核标准的要求予以说明的信息；	… 提供或公开发布有关认证机构对认证审核标准的要求予以说明的信息（见 9.1.1）；	增加
11	5.2.1d）	…这些活动~~不宜~~导致提供违反本条款的建议和意见。认证机构需能够确认这些活动不违反这些要求，…	这些活动不应导致提供违反本条款的建议和意见。认证机构应能够确认这些活动不违反这些要求，	修改
12	7.1.1	~~IS 7.1 管理层能力~~	IS 7.1.1 总体考虑	修改
13	7.1.2	——	IS 7.1.2能力准则的确定 附录 B 中提供了知识和技能的附加信息以支持 CNAS-CC01:2011 的能力准则。	新增条款

序号	条款	CNAS-CC17:2009	CNAS-CC17:2012	说明
14	7.2.1.3.2	a)具备管理认证审核过程的知识和~~素质~~；	a)具备管理认证审核过程的知识和技能；	修改
15	8.1.1	IS 8.1 授予、保持、扩大、缩小、暂停和~~撤消~~认证的程序	IS 8.1 授予、保持、扩大、缩小、暂停和撤销认证的程序	修正
16	8.1.1	a)、b）…依据 ~~GB/T19011、~~CNAS-CC01…	a)、b）…依据 CNAS-CC01…	删除（2 处）
17	8.2.1	…此外，认证证书~~宜~~包括引用的适用性声明的特定版本。	…此外，认证证书应包括引用的适用性声明的特定版本。	修改
18	8.2.1 注	——	注：适用性声明的变更如不改变认证范围中控制措施的覆盖范围，不需要更新认证证书。	新增
19	8.4.1	…认证机构~~宜~~确保客户组织仅使用由认证机构书面授权所规定的标志。	…认证机构应确保客户组织仅使用由认证机构书面授权所规定的标志。	修改
20	9.1.3	…所安排的时间~~宜以下列因素为依据~~：	…所安排的时间应考虑以下因素：	修改
21				
22	9.1.4.2 c）	…这种选择~~宜~~基于判断以反映上述 b)中所列因素，同时也考虑随机因素；	…这种选择应基于判断以反映上述 b)中所列因素，同时也考虑随机因素；	修改
23	9.1.4.2 e）	根据上述要求，设计监督方案，~~并在合理的时间内覆盖客户组织的所有场所或 ISMS 认证范围内的所有场所~~；	根据上述要求，设计审核方案，并在三年的时间内覆盖 ISMS 认证范围内的代表性样本；	修改
24	9.1.5	认证机构的程序~~不宜~~预先假定 ISMS 实施的特殊方式或文件和记录的特殊格式。	认证机构的程序不应预先假定 ISMS 实施的特殊方式或文件和记录的特殊格式。	修改
25	9.1.5	如适宜，审核计划~~宜~~识别在审核中使用的网络支持的审核技术。	如适宜，审核计划应识别在审核中使用的网络支持的审核技术。	修改
26	9.1.6.1	认证机构~~可以采用适合其需要~~的报告程序~~，但这些程序至少~~应确保：	认证机构的报告程序应确保：	删除
27	9.1.6.2	**审核报告~~宜~~提供以下信息：**	**审核报告应提供以下信息或对这些信息的引用：**	修改
28	9.1.6.3	**~~提供给认证机构的~~审核报告应足够详细，以帮助和支持认证决定。**	**审核报告应足够详细，以帮助和支持认证决定。**	删除
29	9.1.6.3 c）	…包括支持它们的客观证据和这些不符合所涉及的 ~~ISMS 标准~~ GB/T 22080-2008 或…	…包括支持它们的客观证据和这些不符合所涉及的 GB/T 22080-2008 或…	删除
30	9.1.6.3	在审核过程中，有关被评价样本的信息~~宜~~包含在审核报告或其他认证资料中。	在审核过程中，有关被评价样本的信息应包含在审核报告或其他认证资料中。	修改
31	9.1.6.3	…对审核报告的要求，报告还~~宜~~包括：	…对审核报告的要求，报告还应包括：	修改
32	9.2.1 c）	…但审核组整体上~~宜~~对被审核的领域具备足够的认识和经验）。	…但审核组整体上应对被审核的领域具备足够的认识和经验）。	修改
33	9.2.3.1	第一阶段审核包括，但不宜仅限于文件评审。	第一阶段审核应包括，但不宜仅限于文件评审。	增加
34	9.2.3.3.3	~~注：GB/T19011为实施管理体系的结合审核提供指南。~~	——	删除
35	9.2.4	…报告至少~~宜~~包括本文件的 IS 9.1.6 中要求的信息。	…报告至少应包括本文件的 IS 9.1.6 中要求的信息。	修改
36	9.2.5	…决定授予和（或）撤销认证的实体（可能是个人）~~宜~~在各方面具备相应的知识和经验，…	…决定授予和（或）撤销认证的实体（可能是个人）应在各方面具备相应的知识和经验，…	修改

序号	条款	CNAS-CC17:2009	CNAS-CC17:2012	说明
37	9.3.1.1	…监督方案~~通常宜~~包括：	…监督审核方案应包括：	修改
38	9.3.1.3	认证机构的监督~~至少宜~~包括 ~~CNAS-CC01:2007~~ 中对监督审核的要求，并且，~~宜考虑~~以下事项：	认证机构的监督应包括 CNAS-CC01:2011 中对监督审核的要求，并且，应覆盖以下事项：	修改
39	9.3.1.3 b)	认证机构的监督方案~~宜~~由认证机构确定。…	认证机构的监督方案应由认证机构确定。…	修改
40	9.3.1.3 d)	对认证证书的使用进行监督。	认证机构应对认证证书的使用进行监督。	增加
41	9.3.1.3	由监督审核所产生的报告至少~~宜~~覆盖本文件的9.3.1.2中的全部要求。	由监督审核所产生的报告至少应覆盖本文件的9.3.1.2中的全部要求。	修改
42	9.4.1	…允许采取纠正措施的时间~~宜~~与不符合的严重程度和风险相适宜，…	…允许采取纠正措施的时间应与不符合的严重程度和风险相适宜，…	修改
43	9.5.1	…认证机构应该按照特别规定~~进行监督活动~~。	…认证机构应该按照特别规定必要时实施特殊审核以及必要活动。	修改
44	9.8.1	认证机构~~宜~~要求获证客户组织在收到投诉后，…	认证机构应要求获证客户组织在收到投诉后，…	修改
45	9.8.1	认证机构~~宜要求~~客户组织利用上述调查活动制定补救和（或）纠正的措施，这包括为以下方面所采取的措施：	认证机构应确保客户组织利用上述调查活动制定补救和（或）纠正的措施，这应包括为以下方面所采取的措施：	修改
46	10.2	方式一： 按照 ~~GB/T19001-2000~~ 的管理体系要求	方式一： 按照 GB/T19001-2008 的管理体系要求	修改
47	附录 A 表 A.1	——	表中的数字仅作说明用，认证机构宜确定自身适用的值。	增加
48	附录 B B.1	有很多途径可以证实审核员的知识和经验，例如，使用承认的资格以~~证实~~知识和经验。审核员注册~~等方式~~可以用来~~证实~~需要的知识和经验。	有很多途径可以证实审核员的知识和经验，例如，使用承认的资格以评价知识和经验。依据人员认证方案的审核员注册记录也可以用来评价需要的知识和经验。	修改
49	附录 B B.2.1	…审核员还宜知晓 27000 标准族的其他标准。	…审核员还宜知晓 ISO/IEC 27000 标准族的其他标准。	增加
50	附录 C	表 ~~C.3~~	表 C.1	修改表号(8 处)
51	附录 C C.3.2	用于再认证审核的全部时间还取决于 ~~GB/T 27021-2007 的 9.4.1.2~~ 中所确定活动的结果。…无论结论如何，本文件的 IS9.1.3 的指南适用。	用于再认证审核的全部时间还取决于本文件 IS 9.1.6 及 CNAS-CC01:2011 的 9.4 中所确定活动的结果。…无论结论如何，本文件的 IS 9.1.3 的指南适用。	修正
52	附录 C C.3.2	…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。	…对审核时间表中所提供时间的调整，宜保持足够的证据和记录来证实其变化的合理性。	修改
53	附录 C 图 C.1	——	图 C.1 审核时间的增加因素和减少因素的潜在交互作用	增加图题
54	附录 D D.2.1	技术类的控制措施的绩效证据可以通过系统测试（见~~下面~~），…	技术类的控制措施的绩效证据可以通过系统测试（见 D.2.2），…	修改

——其他还包括个别标点或编辑调整，不涉及内容变更。