广州国迈科技有限公司良好审核案例

-----通过体系运行改善软件过程质量监测

受审方名称：广州市国迈科技有限公司

认证机构:北京东方纵横认证中心

审核组织成员：旷文渊(组长)　龚炎杰(组员)

审核时间：2014.11.18－ 2014.11.19

认证范围：信息安全应用软件的开发、计算机信息系统集成。

案例提供人：旷文渊

- **企业简介**

广州市国迈科技有限公司是一家专业从事计算机信息安全防护产品研发销售的现代化高科技公司，国迈科技对计算机、安全、通信三大领域都拥有深厚的知识积累和独到认识，拥有一批承担过国家级火炬计划项目、国家高技术产业发展计划项目、科技部创新基金项目等重点项目经验的专家，和长期专注于计算机安全领域的资深研究员，对 Windows 系统驱动、底层开发、加密、嵌入式软硬件系统开发、分布式计算、网络通信、数据库等领域具备强大的研发实力。

目前，国迈科技产品覆盖信息保密、安全移动存储介质、终端安全管理三大领域的内网安全产品线，自推出市场以来，深受广大用户的欢迎，荣获“中国最受欢迎的内网安全品牌”等荣誉奖项。广泛应用于军工企业、政府机构、公检法、科研单位、电信运营商、金融行业、医疗保险、信息密集性企业，及其他企业

和个人。

- **体系审核过程**

1、基本情况：

本次审核是组织第 2 次再认证审核。

受审核组织是 2007 年开始进行质量管理体系认证，是东方纵横的老认证客户。

审核时间：2014.11.18— 2014.11.19

组长：旷文渊，组员：龚炎杰

组织认证范围：信息安全应用软件的开发、计算机信息系统集成。

本次组长对该组织进行了 2013 年度的第 1 次监督和 2014 年度本次的再认证审核。

2、审核现场情况：

按审核计划进行现场审核。审核过程着重抽样对软件的开发项目（纸币流转追踪系统 V1.0、堡垒 U 盘 V3.0）和系统集成项目（广东省国土资源测绘院 主机监控与安全审计系统）中进行了过程审核。受审核方对审核过程非常顺利，双方沟通配合良好。

3、变更情况：

组织原认证范围为内网信息安全软件的开发、计算机信息系统集成。 审核组在进入现场审核后，发现企业有在业务范围上有扩展，除内网安全软件以外，也做综合性的安全类软件，软

件研发不再局限为内网信息安全 ，经与受审核方进行沟通，现场申请变更范围：信息安全应用软件的开发、计算机信息系统集成，获合同评审岗确认。审核组按变更后新范围进行审核。

- **主要的审核发现**

在审核测试部过程中，发现在对纸币流转追踪系统 V1.0 进行集成测试时，使用了一个软件数据插入检测工具进行功能测试，模拟输入整组数据时间，受测软件能否正常识别、整理和归档数据。

审核员对该检测软件的功能和使用方法进行了了解，并要求受审核方展示该检测软件的使用和测试结果的反馈。

演示过程显示，在发现检测异常时，会有小窗口弹窗提示错误。

询问受审核方，是否会有误报和错报情况发生。陪同人员说没有考虑过这个问题，一般不会出错，至于准不准，应该没问题，但没具体评估过，是根据以往的通用测试用例打包的。

后又询问该测试软件的使用范围和时机，是否所有开发的软件都要经过此软件测试，回复说组织开发大部分的保密型 U 盘软件都要经过此软件测试，一般在集成测试时进行测试。

后又与测试部主管沟通，了解此数据插入检测工具，主要是在集成测试阶段，模拟进行数据传输的工具，以识别和确认软件在硬件载体上能否正常工作，传输数据的准确性和及时性等。如测试通过，代表模块代码功能基本正确，可以进行软件的打包

编译，如不通过测试，需返回到单元测试，查找错误之处进行修订。

经与受审核部门确认，该测试软件由测试工程师依据平时的测试用例和数据汇编而成，因使用方便而慢慢引入使用，测试部没有对该软件的具体性能和功能进行过详细确认。

组织《软件检测过程控制程序》规定由测试部负责制定测试需求标准，但测试部明显未对该测试软件要求做评审确认。

审核组内部讨论，认为该审核证据不符合标准Q7.6关于软件用于监视和测量时需进行确认的要求，因此开出书面一般不符合。

具体内容为：未提供对自行编制的验证软件（数据插入检测工具）进行确认的记录。

- **主要的沟通过程**

审核组从标准条款方面进行了解释，告知标准原文要求计算机软件作为监测和测量工具时需确认。

审核组与受审核方明确该检测工具是对其他研发的软件进行功能和性能进行测量和衡量的工具，该工具的测试结果，可以用于判定软件的功能和性能实现，例如测试软件需要模拟连续输入10个数据，让被测试的软件进行处理，以判定被测试软件的处理结果（包括准确性和及时性），衡量受测软件性能和功能，因此属于监测和测量用的计算机软件 ，需对软件其满足预期用途的能力进行确认。

审核组以打比方的形式对监测和测量装置的控制进行说明，如果研发的被测软件是一个螺丝，那我们需检测螺丝长度，直径和螺牙，需要使用卡尺、千分尺和牙规，如果说专用测试用例是牙规，那我们的数据插入检测工具就像一把卡尺，这把卡尺测得准不准，就需要对卡尺进行校准，同理，数据插入检测工具准不准，就需我们对其测试功能进行确认。

审核组同受审核方就该软件的测试偏差性及其后果进行了共同分析。

该测试软件主要用于集成测试和系统测试阶段，如果在此阶段，该数据插入检测工具测试发现受测软件异常，则需返回给软件工程师进行模块代码修订和重新单元测试，如果通过测试，则进行后续的软件集成编译，再最终使用测试用例进行最后的系统测试。如果该检测软件失误，将该报告的错误不报，则软件编译成形后，用测试用例测试再发现问题，要再查找错误点，则需对软件的所有模块进行重新排查，此工作量非常大。

审核员同受审核方代表进行了沟通，假设了被测软件在新增了 1 个用户数据，需要修订数据库中的标识符，如果数据插入检测工具发现新增了 1 个用户，但数据库标识符没变，但检测工具不报告错误。在等到软件编译以后，那所有的涉及引用到这个用户数据标识符的模块都会错误，等到采用测试用例进行系统测试再发现这个问题点，要排除此错误，所有模块都需要重新排查。

直接的后果就是整个研发项目要延后发布，工程师工作量

增加、延长了项目研发周期、系统测试用例覆盖率需加大，甚至影响整个项目的交付。如果在系统测试时测试用例覆盖不全，则最终的软件功能可能存在性能缺陷，威胁客户数量的正确性的安全性。

受审核方以往进行软件测试，在系统测试时采用每款软件定制的测试用例进行最终的模拟运算，并没有使用专用测试软件进行集成测试，该数据插入检测工具是结合往年的软件研发项目测试数据，用于对保密型U盘保护软件进行数据功能测试的而汇编而成自编自用的软件，使用该软件，可以减少单元测试到系统测试中的错误，加快测试进度，但组织认为仅是研发过程中的通用性测试，每款软件又有专用测试用例，因此没有组织对该软件的确认评估，经简单编译后，验证能正常运行就直接投入使用了。

测试部负责人也告知，确认偶尔会有经数据插入检测工具发现的错误反馈，所以在保证软件测试准确性和后果预防上，该软件有一定的效果和作用，提高了过程控制的有效性和前瞻性。但该测试软件到底准不准，真没有仔细确认过。通过此次沟通，确实理解了该软件需要准确的重要性。

- **组织的改进**

出现不符合情况，主要是组织相关人员对标准条款要求不明确。经过解释和沟通，组织认识到对标准理解不深，审核组提出的不符合项合理、专业，由管理者代表对不符合项的内容进行了确认。

针对不符合，组织制定了纠正和预防措施，包括：

——通过培训的方式，对研发部、测试部相关人员进行了重新培训，重新学习标准7.6章节和监视和测量装置的控制要求。

——针对现在的测试软件，由测试部重新编写该测试软件的测试用例进行测试，验证和确认现有的测试软件 的功能完整和适用性。

对使用此数据插入检测工具测试的已完成研发的项目，抽取1—2 个项目重新测试进行复查，同时针对复查的结果，项目的测试用例，评估使用数据插入检测工具测试的结果与使用测试用例进行测试的偏差。后抽取了堡垒U盘V3.0项目进行复查测试，证明使用数据插入检测工具测试的结果与使用测试用例测试的结果没有偏差。

组织自查自纠，检查是否有其他软件用于监视和测量的情况，经分析现阶段暂只有这一款测试软件，但有一些正在新开发过程中。。

组织在该检测软件的测试用例编制过程中，通过测试用例的覆盖情况，进一步评估了该测试软件的功能性和适用性。

针对监视和测量用途的软件，组织内部组织讨论，对后续的类似软件，探讨新的确认方法和形式。

- **改进的成效**

通过此项不符合项的整改，使受审核方测试部对软件行业的Q7.6条款监视和测量装置控制有了进一步的了解和认识。

受审核组织正在进行新一批自测工具的编制，通过此次不符合，对正在编制过程中检测工具的评估更加清楚和明确，通过确认，使“检测标准”的更准确和有效，对测试项目更有针对性。

使受审核组织认识到使用检测软件对软件研发过程中质量的监测需求和目的，虽然至今暂未发生过测试失误，但不代表以后不会失误，现今的改善，为后续的软件研发过程质量控制提供了保证。

部门经理居广雄告知：

通过此不符合项的整改，不仅对软件的功能和性能测试要求更加明确，对测试方式和方法的控制有了进一步的认识，理解过程管理的重要求，测试用例是一种纵向的分析，而对软件研发进行监视和测量软件则变成一种横向评估，为后续改善软件的综合性能提供了保障基础。

通过采用有效的监测工具，进行过程质量监控，能够有效避免过程中的工作偏差，完善软件产品质量，同时，节省了项目研发成本，降低研发成本，减少工作量。如果 1 个项目在集成测试时未能发现功能或性能上问题，等到系统测试或交付测试再来发现和解决，项目延期和成本增长的损失不可估量，严重的过程失误，甚至可能导致项目失败。所以后续也会加强软件研发过程中的质量监控。

- **项目总结—对受审核方**

受审核组织通过多年的体系运行，已经建立了标准化的管

理体系，在内部有效推行，与组织的实施运作有效结合。

——通过多年的坚持和持续，已明确感觉到体系的有效性和适用性，从新入员工到快速融合成项目组，从 IT 行业的专业性到客户群体的满意和认可（公检法司系统，对准确性要求严苛），再到多年的市场快速扩展，充分体现了体系在公司内部的推动力量。

——组织内部进行体系管理，对部门职责、工作流程进行了明确，减少了工作交叉，清晰了工作内容，对管理人员和执行人员对减少了工作和负面影响，充分体现了体系在公司内部标准化、流程化优势。

——质量管理体系是其他管理工作的基础，受审核方除了质量管理体系，还有其他体系，比如涉密安全产品管理体系等，但质量体系如终是基础，如统一的文件管理方式、流程管理方法、质量记录管理、质控点的控制等，都是异曲同工，使企业内部管理更简单和统一。

——体系工作为产品和服务质量提供了保证基础，通过过程管理，减少了负面结果的发生，从而提供了合格产品和服务，增强了客户满意。例如公司从未发生过交付验收测试不合格的情况。

——对外宣传：虽然现在的 ISO9001 质量管理体系认证市场泛滥，但组织面对的公检法司等相关的机关单位，在工作方面的严谨细致比市场化的商业公司认识更深刻，组织通过认证，一方面提高产品质量和企业素质，另一方面也容易得到客户的认可。

- **项目总结—对审核方**

——专业性：针对受审核的产品特点要有认识和理解。此项目受审核方主要信息安全软件，对软件的功能性和准确性有较强的要求，只有通过专业的测试和功能验证，才能保证软件的适用性，因此审核过程提出了对过程测试软件的确认问题。对组织认证范围的准确描述，使用认证范围即符合企业实际，又符合认证准测和审核机构风险控制要求。

——服务精神：体系认证在中国推行几十年了，很多组织对体系运行形成了自己的认识，对标准的理解也有不同之处，审核员应以服务和沟通的态度对待受审核方，对不理解的地方进行适当的沟通和相互理解。在本案中，正是通过审核员与受审核方的融洽沟通，合理的比喻象征，标准条文的合理解释，对偏差后查的共同分析，才取得不符合项的共识。

——职业性：基本公平公正的态度，在审核准则的前提下开展工作。本项目受审核方除信息安全软件的研发，还有安全移动存储介质等硬件产品的销售，但并不在本次认证范围内，组织也未要求覆盖该范围，因此只针对组织的主要活动进行认证范围的变更。

——良好的沟通：在不符合的确认，到认证范围的变更，到审核过程的工作询问，良好的沟通是保证现场审核顺利进行的前提，本案中，通过良好沟通，获取适宜的证据，解决认证范围变更和不符合的确认，良好的沟通均起到了事半功倍的效果。

- **备注说明**

1、说明：

本案例仅以受审核方的认证范围信息安全应用软件的开发的内容进行评价和总结。

2 、相关证明资料—数据插入检测工具的测试用例和测试报告，见附件。