审核报告.

上海菱威深信息技术有限公司

报告编辑人 **Lin (Helen) Chang**

审核开始日期 23/09/2013

综述.

报告编辑人 Lin (Helen) Chang 相关的审核活动如下：

SMO/审核类别/审核日期/审核时间	证书/认证标准	地点地址
7934205 初次认证第一阶段审核 23/09/2013 2 人天 员工人数 150	IS 595020 ISO/IEC 27001:2005	上海菱威深信息技术有限公司 中国 上海 峨山路 91 弄 100 号 浦东新区 2 号楼 9 楼 200127

第一阶段审核的目的是确认组织进入第二阶段审核的准备情况，并确保其有效策划。

管理总结.

总体结论

组织第二阶段审核基本准备充分,已确定的不符合项需要在下一阶段审核前被纠正，处理的有效性会在第二阶段被评估。
第二阶段现场审核人天数为 4.0 天。审核范围是提供应用软件设计、开发和运维、IT 基础设施方案设计，远程监视和维护服务的信息安全管理。这个与 2013 年 7 月 2 日发布的 1.20 版的适用性声明是一致的.

上次审核没有未关闭的不符合。

7 需要跟进的不符合及其它发现点将在后面的报告中提出。

轻微不符合为偶然的缺失，并不意味着管理体系的相关流程失控。应调查导致不符合的根本原因以确定相应的纠正措施。纠正措施是否被有效实施将在下次审核中确认。

请向 BSI 提交纠正措施计划包括不符合内容，原因分析，相应的纠正措施及其责任人和实施计划。 请于 18/10/2013 前通过电子邮件或者传真的方式将纠正预防措施计划提交至以下联系方式，并请在计划上注明相关报告号码。

强制性要求.

合理的删减

证书合理的删减已得到确认：IS 595020

明细：

A.10.9.1，A.10.9.2 已删减，由于公司没有电子商务相关的业务和服务，可以接受。

被审核区域和审核发现.

高层和信息安全体系策划： 4.1,4.2,4.3,5.1,5.2, A.5, 7,8.1

体系策划 4.1,5.1,5.2,A.5

认证组织为的认证范围已确认，符合营业执照内容, 物理地点已确认为一个，有效认证人数为 150 人，信息安全体系从 2012 年 11 月建立。

所有 ISO27001:2005 的要求都被识别，相应的流程已经建立并运行，所需资源都已提供。信息安全管理手册定义了信息安全管理体系的方针、目标、管理架构，并在组织内部得到沟通。

SOA 适用性声明　文控 4.3　A5-A15

适用性声明版本《适用性声明》SOA　v1.20
A.10.9.1,A.10.9.2,　由于没有电子商务和在线交易，删减可以接受。

风险评估和处理 4.2.1, 4.2.2,
《风险评估管理规定》描述了风险评估和处理方法论，风险评估有文档化的记录和报告，有明确的风险接受准则，并制定和实施了风险处置计划，主要的风险处置措施已落实并进行了跟踪验证。

本处开出一个轻微不符合。

管理评审　7.1,7.2,7.3
公司经营委员会规定每三个月组织一次评审会议。最近一次管理层会议发生在 2013 年 3 月,相应的管理评审输入和和输出基本符合标准的要求。

本次开出一个观察项。

OBSHC1： 管理评审已实施，但是相应的策划文件可考虑进一步细化，以利于执行。

Team B ：6, 8,4.3, 5.2.2,A6, A.8,A.10.2,A.13,A.14, A.15

1.Internal Audit 内审
内部审查制度 1.0 版本
2013 年 6 月 3-14 日进行内部审核，一般不符合：5 项，改善建议项：5 项。对应的内容在跟踪过程中。
内审涉及的部门，项目包括：应用系统设计、开发和维护；IT 基础设施的设计、监视和维护。
2.Effectiveness Measurement 有效性测量
ISMS 有效性测量管理规定，建立了有效性的测量机制，并定期进行监视和测量。
3.Incident Management 事件管理
有事件管理
4.BCM 业务连续性管理
对关键业务进行了定义和影响分析，并对例如：文件服务器、防火墙等列入连续性计划管理。
5.Compliance 合规性
对适用的法律法规进行了识别和评价。
6.HR policy and Security Training
人事策略和安全培训
7.Third party management 第三方管理

制定了第三方管理的策略，并在执行。
8.Document Control,Record Control 文件控制，记录控制
制定了文件控制和记录控制策略。

此次审核提出的轻微不符合.

序号	区域/流程	条款
973047N0	高层和信息安全体系策划	4.2.1d）
范围	IS 595020 at IVISIO-0047462296-000	
内容	公司已实施了资产识别风险评估，但是资产识别有遗漏。	
要求:	d) Identify the risks. 1) Identify the assets within the scope of the ISMS, and the owners2) of these assets. 2) Identify the threats to those assets. 3) Identify the vulnerabilities that might be exploited by the threats. 4) Identify the impacts that losses of confidentiality, integrity and availability may have on the assets. 2) The term 'owner' identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term 'owner' does not mean that the person actually has any property rights to the asset.	
客观证据:	抽样 ITS 基盘和 BS MCG，客户系统的数据，项目管理文档和源代码没有在资产台账内识别。	

序号	区域/流程	条款
973047N1	Team B	A.9.1.2
范围	IS 595020 at IVISIO-0047462296-000	
内容	在物理入口控制方面存在缺失	
要求:	Physical entry controls - Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	
客观证据:	在物理入口控制方面存在如下缺失: 1.公司出入门禁卡分为员工卡、驻场卡和贵宾卡，卡号为：07580 的驻场卡，为原驻场人员还回的卡，但没有取消相应的门禁权限，又发放给访客，该卡的权限可以访问公司办公区、项目区、仓库。 2.部分贵宾卡能访问到除会议室区开发区，不符合公司规定的贵宾卡只能访问大门的权限的要求。	

序号	区域/流程	条款
973047N2	Team B	6
范围	IS 595020 at IVISIO-0047462296-000	
内容	在内部审核方面存在缺失。	

要求:	Internal ISMS audits The organization shall conduct internal ISMS audits at planned intervals to determine whether the control objectives, controls, processes and procedures of its ISMS: a) conform to the requirements of this International Standard and relevant legislation or regulations; b) conform to the identified information security requirements; c) are effectively implemented and maintained; and d) perform as expected. An audit programme shall be planned, taking into consideration the status and importance of the processes and areas to be audited, as well as the results of previous audits. The audit criteria, scope, frequency and methods shall be defined. The selection of auditors and conduct of audits shall ensure objectivity and impartiality of the audit process. Auditors shall not audit their own work. The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records (see 4.3.3) shall be defined in a documented procedure. The management responsible for the area being audited shall ensure that actions are taken without undue delay to eliminate detected nonconformities and their causes. Follow-up activities shall include the verification of the actions taken and the reporting of verification results (see 8). NOTE: ISO 19011:2002, Guidelines for quality and/or environmental management systems auditing, may provide helpful guidance for carrying out the internal ISMS audits.
客观证据:	在内部审核方面，存在如下缺失： 1.在 V1.0 内部审核制度中缺少对内部审核发现的纠正，纠正措施以及原因分析，后续改善效果的跟踪等的职责没有明确规定。 2.在策划的每年一次的内部审核有漏项，例如：2013 年 6 月 3-14 日进行的内部审核检查表中缺少对 4.1 条款的审核记录。

序号	区域/流程	条款
973047N3	Team B	4.3.2
范围	IS 595020 at IVISIO-0047462296-000	
内容	在文件控制方面存在缺失。	
要求:	Control of documents Documents required by the ISMS shall be protected and controlled. A documented procedure shall be established to define the management actions needed to: a) approve documents for adequacy prior to issue; b) review and update documents as necessary and re-approve documents; c) ensure that changes and the current revision status of documents are identified; d) ensure that relevant versions of applicable documents are available at points of use; e) ensure that documents remain legible and readily identifiable; f) ensure that documents are available to those who need them, and are transferred, stored and ultimately disposed of in accordance with the procedures applicable to their classification; g) ensure that documents of external origin are identified; h) ensure that the distribution of documents is controlled; i) prevent the unintended use of obsolete documents; and j) apply suitable identification to them if they are retained for any purpose.	

客观证据:	在文件控制方面存在如下缺失： 抽样 2013 年 7 月 1 日修订的《就业规则》，从 2003 年发布以来，共进行了 5 次修订，没有相应版本变化的标识，同时也未有更改的痕迹的记录。

序号	区域/流程	条款
973047N4	Team B	A.14.1.2
范围	IS 595020 at IVISIO-0047462296-000	
内容	在业务连续性和风险评估方面存在缺失	
要求:	Business continuity and Risk Assessment - Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.	
客观证据:	在业务连续性管理方面存在如下缺失： 1.在关键业务定义和影响分析中，需要关注关键业务影响的灾难的恢复时间要求、当前控制措施的明确等内容。 2.对列入业务连续性计划的防火墙的恢复计划需要按照计划的安排进行演练。	

序号	区域/流程	条款
973047N5	Team B	A.15.1.1
范围	IS 595020 at IVISIO-0047462296-000	
内容	在可用法律法规方面存在缺失	
要求:	Identification of applicable legislations - All relevant statutory, regulatory and contractual requirements and the organization’s approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the organization.	
客观证据:	在可用法律法规方面存在如下缺失： 公司所识别的法律法规中，没有识别到中华人民共和国著作权法。	

序号	区域/流程	条款
973047N6	Team B	A.10.5.1
范围	IS 595020 at IVISIO-0047462296-000	
内容	在信息备份方面存在缺失	
要求:	Information Backup - Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.	
客观证据:	在信息备份方面存在如下缺失： 对监控的信息备份，日志备份，在管理制定中没有明确对其备份的保存时间、测试周期的要求。	
行动		

是否已关闭?	是

审核参加人员.

被认证组织代表:

姓名	职位
永山一郎	副总
成 勇 Mr.	技术统括部长

BSI 参加审核人员:

姓名	职位
Lin (Helen) Chang	审核组长
Yanjie(Vicky) Li	审核组员

下次审核计划.

审核目的

第二阶段审核的目的是评价组织管理体系的实施情况，包括有效性。确保组织的管理体系已有效覆盖拟认证范围内的所有要素及管理体系标准的所有要求。如果本次审核是多地点审核的一部分，最终认证推荐将由所有地点的审核发现决定。

日期	审核员	时间	区域/流程	条款

如您在确认的审核日期前 30 天内提出取消审核，BSI 保留收取您相当于一个人天的审核费用的权利。

注.

审核以抽样方式进行因而某些不符合可能存在但没有被识别出。

如果您需要将审核报告复印件提供给其它组织，请确保提供的报告页数齐全。

英标管理体系认证（北京）有限公司 中国 上海 淮海中路 1325 号 爱美高大厦 23 楼 200031 电话：+86 21 64312638 传真： +86 21 64740637 电子邮件（用于纠正预防措施计划）： Helen.chang@bsigroup.com ； capbj@bsigroup.com