陕西盛田能源服务股份有限公司

管理体系审核实践案例

报送机构：北京天一正认证中心有限公司

申 报 人：岳增武

案例类型：ISMS 管理体系认证

认证技术交流研讨材料材料/良好认证案例推荐表

推荐机构名称(盖章)	北京天一正认证中心有限公司	
获证组织名称	陕西盛田能源服务股份有限公司	
案例类型	质量管理升级版■　产品认证□　服务认证□	
认证人员姓名	岳增武　李庆　李贞　张忠琪	

经验材料/案例特点简述及推荐意见(可加附页)

一．　企业基本情况：

受审核方陕西盛田能源服务股份有限公司注重人力资源建设、坚持技术创新和管理创新，不断更新软、硬件设备和信息化支持工具，具备了整套自主开发、研究创新和分析能力。公司的主营业务包括能源管理软件、能源数据采集嵌入式控制系统的开发设计、二氧化碳热泵机组的研发、能源信息系统集成服务等。

二．　案例特点：

审核组现场审核时发现企业未进行软件平台应急处理预案验证，这本身是个小事件，但审核组考虑到该平台的重要性和对信息技术的依赖，开具不符合项并重点关注。企业在纠正过程中证实了审核组的判断，不仅仅锻炼了应急操作人员，又进一步发现了该预案存在的缺陷。

三．　推荐意见：

企业通过进一步补充完善预案并采用演练进行验证，降低了企业的信息安全风险，实现审核增值。

作为良好审核案例予以推荐。

案例特点简述（见附页）

证明及简述材料(可加附页)

材料清单：■审核计划
■不合格项
■改进措施及企业整改成效证明
■其它可以说明和证明案例的材料（审核报告）

附页

陕西盛田能源服务股份有限公司 ISMS 审核案例

推荐机构：北京天一正认证中心有限公司

审核类型：信息安全管理体系初次审核

审核时间：2017 年 10 月 12 日至 2017 年 10 月 15 日

审核组成员：岳增武（组长）；李庆；李贞；张忠琪

推荐人：岳增武 李贞

一、案例发生的背景

1、审核范围：与能源管理系统软件的开发；能源数据采集嵌入式控制系统的开发及其系统的集成；二氧化碳热泵控制系统软件的开发；智慧楼宇控制系统软件的开发及其系统的集成；物联网检测设备、控制设备采集器的研发、生产和销售相关的信息安全管理活动。

2、审核场所：（略）

3、企业基本情况

受审核方陕西盛田能源服务股份有限公司注重人力资源建设、坚持技术创新和管理创新，不断更新软、硬件设备和信息化支持工具，具备了整套自主开发、研究创新和分析能力。公司的主营业务包括能源管理软件、能源数据采集嵌入式控制系统的开发设计、 二氧化碳热泵机组的研发、能源信息系统集成服务等。

为确保公司现有的产品研发、项目施工的顺利实施，于 2017 年依据 GB/T 22080-2016(ISO/IEC 27001:2013,IDT)标准建立了信息安

全管理体系。

北京天一正认证中心有限公司也于同年对陕西盛田能源服务股份有限公司实施了初次审核，那么，如何通过审核的实施，给该公司提供有价值的认证服务，成为本次审核的关注要点。

二、审核案例发现和沟通过程

企业维持正常业务运转，均需要依靠硬件、软件、人员、信息等各类信息安全资产，如果其中一项或多项信息安全资产由于某种原因无法使用，公司的正常业务就会受到影响。这些信息安全资产缺失的时间越长，公司恢复正常运作就需要花费越长的时间。

为防止公司业务活动中断，保护其关键业务过程免受信息系统重大失误或灾难影响，并确保及时恢复，在 GB/T 22080-2016 标准中明确提出了，企业在业务连续性管理的信息安全方面，应制定和实施包含信息安全的连续性计划。

在审核支撑陕西盛田能源服务股份有限公司项目运作的软件平台时发现："该应用系统存在中断或失败后不能在业务需要的水平和时间内恢复的风险。"

陕西盛田能源服务股份有限公司依据标准制定了《软件平台应急处理预案》，依据预案该对各支撑业务的信息系统进行管理。

但审核组在审核时发现：

（1）通过查看公司提供的《业务持续性和影响分析报告》，了解到陕西盛田能源服务股份有限公司最重要的信息系统是运行在软件平台上，该软件平台统管施工和管理调度，具有高度保密性、可用

性和完整性。

（2）审核西咸物联E能源项目，发现该项目运作的软件平台存在中断或失败后不能在业务需要的水平和时间内恢复的风险，公司制定了相关软件平台应急处理预案，但未提供对于该处理预案进行验证的证据。

（3）审核现场访谈了相关人员，相关人员认为，涉及该软件平台的人员不多，采用口头交流讨论的方式，即可确定软件平台应急处理预案的可行性，未按策划的要求实施验证，也不了解该软件平台在中断或失败后的业务恢复水平和时间。

问题分析：

（1）由于该软件平台的运行需要网络和信息技术的支持， 如果网络不能正常工作或者信息技术支持不力，则该软件平台将面临较大风险。

（2）尽管公司相关人员口头讨论了该软件平台应急处理预案的可行性，但在实际灾难来临时，许多操作人员经常会因缺乏对突发事件的应对经验，而遗漏相关步骤。

（3）应对灾难的大部分工作主要由网络管理员负责，公司也规定了网络管理员不在现场时，由现场负责人承担网络管理员的职责，但在访谈时发现，由于没有具体演练，该负责人并不知晓关键主机的具体IP地址，对于备份数据所处位置和防火墙策略设置的具体细节也不太清楚，存在着灾难来临时软件平台不能及时恢复使用的重大风

险。

依据以上审核发现和问题分析，审核组开具了不符合项：“查西咸物联E能源项目，未提供对于项目现场进行软件平台应急处理预案进行验证的证据。”

三、改进及取得的成效

经以上审核证据的支撑及分析，陕西盛田能源服务股份有限公司的领导对我们发现的问题予以肯定并接受，并表示，审核组指出的均为系统安全存在隐患的薄弱环节，需要通过技术、行政等手段加强整改。软件平台是陕西盛田能源服务股份有限公司项目现场的核心系统，一旦该系统不能及时恢复，就会造成关键竞争力的削弱、业务的中断，也会给合作伙伴和客户的信心造成沉重打击，因此应从细微之处着眼，未雨绸缪。

现场审核后，陕西盛田能源服务股份有限公司对提出的不符合项进行了原因分析并采取了纠正和纠正措施，实施举一反三，排查同类问题并一并整改，取得了良好的管理成效。

改进过程：

（1）组织网络管理员和施工现场人员学习《业务持续性和影响分析报告》和《软件平台应急处理预案》，识别软件平台可能存在的网络不通、应用系统数据库不同步、硬件故障、应用系统数据损坏、用户被误删除等风险，并据此给出相应的解决办法。

（2）通过现场演练验证预案的可行性，网络管理员和施工现场

人员均参加，重点是演练技术操作细节，如备份与恢复、网络故障、防火墙策略等。

（3）进一步完善方案，修订《软件平台应急处理预案》，明确要求预防、防护、紧急响应业务恢复等多方面的活动， 这些活动必须制定为具体的可实施方案。形成了《操作系统备份与恢复》、《网络故障排查手册》作业文档。

取得的成效：

（1）提高了员工对信息安全业务持续性的系统认识。公司识别出软件平台是支撑业务的关键系统，但简单的考虑软件平台本身的恢复是不够的，灾难来临的形式是多样的，可能会是网络中断、也可能会是域控失败，这些都需要网络技术和信息技术支持。

（2）业务连续性计划成为了企业管理的一部分。通过本次不符合的整改，该公司修订了《业务持续性计划和管理程序》，明确持续性计划包括的活动和必须制定的可实施方案。业务连续性计划已经成了公司日常工作的一部分，确保了该计划的切实可行。

（3）企业反映此项改进为其更具操作性的实施应急演练找到了更好的方法，通过制订与业务连续性相关的一系列计划和文档，不但确保了演练的持续改进，而且在模拟演练中也证明在网络管理员不在现场的情况下，其他人员也能依据计划和相关文档及时恢复应用系统，有效减轻了只能依赖网络管理员恢复应用系统的重大风险。审核组将会在今年的监督审核中对这个不符合项的改进作现场验证。

四、体会

过去，人们有一种误解认为预案制定了，灾难就可以避免了。没有意识到在突发事件来临前就应做出应对计划和操作细则并进行演练，以期望将灾难的损失降到最低，尽快恢复公司业务。

公司管理层应审时度势、未雨绸缪，统筹考虑成本和收益之间的平衡，建立风险可控的、系统化的信息系统恢复方案，确保业务的及时恢复。

业务连续性是一种预防性机制，它明确了公司的关键业务以及对业务可能造成的威胁，并据此采取相应的技术手段，制定计划和流程，确保这些关键职能在任何环境下都能持续发挥作用。

SH/BG11

表格生效日期
2017-07-20

项目号：17I000431

北京天一正认证中心有限公司审核计划

受审核方	陕西盛田能源服务股份有限公司				
注册地址	陕西省西安市高新区沣惠南路34号摩尔中心B座1602-1 710065			邮编	710065
办公地址	陕西省西安市高新区沣惠南路34号摩尔中心B座1602-1			邮编	710065
生产地址	陕西省西安市高新区沣惠南路34号摩尔中心B座1602-1			邮编	710065
联系人	雒林萍	电话	029-61873303，15109285853	传真	029-86775759
审核类别	I：正式审核	审核日期	2017年10月12日上午 09:00:00 至 2017年10月15日上午 12:30:00（共3.5天）		
审核目的	■ 初审 □第一阶段审核：了解组织管理体系的建立及运行情况，确认组织管理体系文件是否满足认证标准和法律法规的要求，是否具备第二阶段审核的条件。 ■第二阶段审核：评价组织管理体系与所选定的认证标准的符合性、有效性及满足法律、法规(或合同)要求的能力，确定是否推荐注册。 □ 再认证：验证组织的管理体系整体的持续有效性，以及认证范围的持续相关性和适宜性，确定是否推荐再认证注册。 □ 监 督：验证组织管理体系是否持续满足要求，确定是否推荐保持认证注册。 □ 专 项：评价组织变化的管理体系与所选定的认证标准的符合性、有效性及满足法律、法规（或合同）要求的能力，确定是否同意组织的申请并换发认证证书。 □ 恢 复：确认在暂停期内，获证组织的管理体系的运行情况，证书、标志使用情况。 □ 其 他：				
审核范围（体系覆盖的产品及其过程/活动）	主证书范围及专业代码/技术领域代码：I：与能源管理系统软件的开发；能源数据采集嵌入式控制系统的开发及其系统的集成；二氧化碳热泵控制系统软件的开发；智慧楼宇控制系统软件的开发及其系统的集成；物联网检测设备、控制设备采集器的研发、生产和销售相关的信息安全管理活动。（适用性声明版本：V1.0）(04.08；04.13/04h；04m)；				
	子证书范围及专业代码/技术领域代码（必要时）：见附件				
审核依据	■ GB/T 22080-2016 GB/T22080-2016 / ISO/IEC 27001:2013 ■管理体系文件有效版本 版 ■相关的法律法规及其他要求 ■合同 □				
I 申请不适用条款：	无	审核使用的语言：	■汉语 □		
审核报告发放清单	■受审核方 ■北京天一正认证中心有限公司 □委托方（适用时）				

审核组成员构成

分工	姓名	注册资格	注册证号	专业/技术领域	联系电话	备注	编号
组长	岳增武	I：审核员	2017-N1ISMS-1214131	I：04.08；I：04.13	17602976932		A
组员	李庆	I：审核员	2017-N1ISMS-1015806	I：04h；I：04m	13718169952		B
组员	李贞	I：实习	2017-N0ISMS-1100987		15319954107		C
组员	张忠琪	I：实习	2017-N0ISMS-1203383		18509236037		D

注（组内专家填写）： ，工作单位： ，职称：

审核组长：	审批：	受审核方代表：
岳增武 2017 年 9 月 28 日	陈峰森 2017 年 9 月 30 日	2017年10月12日

承 诺：在审核过程中接触的有关受审核方特定产品或机密信息，未经受审核方书面同意，绝不透露给第三方。当法律要求提供信息时，除法律限制外，中心将书面告知受审核方所提供的信息。

北京天一正认证中心有限公司审核计划（续）

审核日程表

首次会议			10月12日9时00分至9时30分	请受审核方最高管理者及相关部门负责人参加		
末次会议			10月15日12时00分至12时30分	参加人员同首次会议		
日期	第 1 组			第 2 组		
	时间	编号	部门和要素	时间	编号	部门和要素
10.12	9:30~18:00	AD	办公室： 4.4；5.3；6.1；6.2；7.1；7.2；7.3；7.4；7.5；8.1；8.2；8.3；9.1；9.2；10.1；10.2；A5；A6；A7；A8；A9；A11；A16；A18	9:30~18:00	BC	管理层： 4.1；4.2；4.3；4.4；5.1；5.2；5.3；6.1；6.2；7.1；7.4；7.5.1；9.1；9.3；10.2；A5.1；A6.1；A7.2；A8；A9；A11；A16.1；A17；A18.1；A18.2 信息安全外部抽查；顾客对信息安全申投诉及处置；认证覆盖范围确认
10.13	8:30~17:30	AD	工程运维部： 6.1；6.2；7.1；7.4；8.1；8.2；8.3；9.1；10.1；10.2；A6；A8；A9；A11；A12；A13；A16；A17；A18 认证覆盖范围确认	8:30~17:30	BC	技术部： 4.3；6.1；6.2；7.1；7.2；7.5；8.1；8.2；8.3；9.1；10.1；10.2；A5；A6；A8；A9；A10；A11；A12；A13；A14；A16；A17；A18； 认证覆盖范围确认
10.14	8:30~12:30	AD	继续工程运维部：（集成现场：西咸物联E能源项目，位于咸阳世纪大道启迪大厦；距公司40公里，往返车程1小时，8:00出发，12:30返回）	8:30~12:30	BC	继续审核技术部
	13:30~17:30	AD	财务部： 8.1；8.2；8.3；A8；A9；A11；A12.3；A12.4；A16	13:30~17:30	BC	市场部： 6.1；6.2；7.4；8.1；8.2；8.3；9.1；A8；A15；A16
10.15	8:30~11:30	ABCD	补充审核、内部评议			
	11:30~12:00	ABCD	与被审核方管理层沟通。			

注意：1. 如果组织为多场所，应将每个场所的地址明示，必要时可附页。

2. 审核计划每天安排现场检查时间不少于8小时，以保证有充足的时间用于收集客观证据；如有异地场所（包括多场所和临时场所），审核计划中应标明前往异地场所路途时间。有夜班生产应考虑抽样安排。

3. QES初审二阶段/再认证审核应覆盖体系全部条款，审核重点：内审、管理评审，QES绩效及对其有影响的产品、过程、区域、部门及人员能力，顾客或相关方申/投诉及处理。再认证审核还应查认证证书、标志使用和体系运行情况，上次审核不符合项的验证（明示条款，并以下划线标识）。

4. 监督审核计划参照“定期监督审核方案”要求编制，如有不妥，可调整并作出说明。

5. 监督审核必查的内容：除必查的条款外，还包括认证证书和标志使用情况、上次审核不符合项的验证（明示条款，并以下划线标识）、顾客（相关方）申/投诉及处理，体系变更。

SH/BG19

生效日期
2017-07-20

项目号： 17I000431

不 符 合 项 报 告

No. 3 / 3

审核类型	□初审一阶段 ■初审二阶段 □第 次监督 □再认证 □		
受审核方	陕西盛田能源服务股份有限公司	受审核部门	工程运维部
接受审核人员	陈前龙	陪同人员	翟浩楠
审核依据	■GB/T22080-2016 / ISO/IEC 27001:2013 ■管理体系有效文件 ■相关法律法规和其他要求	严重程度	□严重 ■一般

不符合事实描述

查西咸物联E能源项目，未提供对于项目现场进行软件平台应急处理预案进行验证的证据。

以上事实不符合 ■GB/T22080-2016 / ISO/IEC 27001:2013标准 A17.1.3 条款，关于“验证，评审和评估信息安全的连续性” 的规定；也不符合组织的管理体系文件 《信息安全适用性声明（SoA）A/0》中A17.1.3的规定。

审核员：[illegible]、张杰琪 审核组长：[illegible] 受审核方代表：王帆

日 期：2017.10.15 日 期：2017.10.15 日 期：2017.10.15

纠正措施要求	□采取纠正措施 ■纠正并采取纠正措施
纠正措施验证方式及所需时间	受审核方所采取的措施经自行验证有效后，自现场审核后30日内报审核组进行： □现场验证 ■书面验证，保留现场验证的权利

纠正措施验证（包括验证的主要内容和结果）

2017年10月23日收到企业提供的不符合纠正措施表、测试验证记录，补充完善后的《平台应急处理预案》、《操作系统备份与恢复操作规程》、《网络故障排查手册》等材料，经书面验证，企业采取的纠正和纠正措施可以接受，下年度监督审核时有效性做进一步验证。

审核员：[illegible] 日期：2017.10.23

注：1.初审时，受审核方应在现场审核后45天内针对一般不符合采取纠正措施，并向审核组提交必要的证明材料并经审查接受。严重不符合项可视情况延长，但最长不超过90天。

2.监督和再认证时，受审核方应在现场审核后30天内针对一般不符合采取纠正措施，并向审核组提交必要的证明材料并经审查接受。严重不符合项最长不超过15天（再认证时，应在当前认证证书终止日期前）。

3.如受审核方逾期未能有效关闭不符合，北京天一正认证中心有限公司将按照相关要求对其认证资格进行处置。

SH/BG19 附

生效日期
2017-07-20

项目号：17I000431

不符合项纠正措施表

不符合项事实摘要：

西威物联E能源项目，未提供对于项目现场进行软件平台应急处理预案进行验证的证据。

纠正情况：

针对西威物联E能源项目重新进行软件平台应急处理预案进行演练，以验证预案的可用性。

原因分析：

工程运维部负责人认为公司相关人员口头讨论了该软件平台应急处理预案的可行性就可以代替验证，对实际灾难来临时许多操作人员经常会因缺乏对突发事件的应对经验而遗漏相关步骤等情况考虑不周，所以没有进行演练。

纠正措施：

1、组织网络管理员和施工现场人员学习《业务持续性和影响分析报告》和《软件平台应急处理预案》；

2、进一步完善方案，修订《业务持续性和影响分析报告》、《软件平台应急处理预案》，形成了《操作系统备份与恢复》、《网络故障排查手册》作业文档。

3、在《业务持续性和影响分析报告》中规定由工程运维部负责任人每季度对现场实施情况进行监督检查。

预定完成日期：2017.10.20

举一反三检查情况：

对公司其他类型的应急预案进行验证，目前均可行，后续将每半年验证一次。

受审核方内审组对纠正及纠正措施有效性验证：（请附纠正及纠正措施实施证据，复印件即可）

通过对西威物联E能源项目软件平台应急处理预案的验证演练，有效地达到了预期的效果，验证了预案的可用性及实用性。有关部门完善了相关报告及手册文档，达到了举一反三的效果

验证人：解林萍　　日期：2017.10.21

注：此表全部由受审核方填写。

受审核方代表：王强　　日期：2017.10.21

陕西盛田能源服务股份有限公司

验证测试记录

STNY/QR-QP.03-04

№：001

验证内容	软件平台应急处理预案		验证地点	项目现场	
验证时间	2017 年 10 月 20 日		指导人	王强	
培训对象	网管和现场操作人员		记录人	雒林萍	
应到人数	5 人	实到人数	5 人	缺席人数	0
培训人员签到表	刘万里 陈新飞 孟文杰 秦伟 雒林萍				

验证记录

为了提高本公司信息安全处置能力，公司特举办这次软件平台应急处理预案验证和演练，旨在使有关人员深入了解该平台应急处置流程，提高公司信息安全保证能力，验证和演练内容主要如下：

1、学习公司文件《业务持续性和影响分析报告》、《软件平台应急处理预案》，并组织讨论；

2、组织网管和现场操作人员对《软件平台应急处理预案》进行演练；

3、修改完善相关预案；

4、补充演练。

效果评价

通过对软件平台应急处理的现场演练，现场及相关管理人员深入了解了平台的应急处置流程，进一步提高了公司信息安全保证能力，有效保证了业务连续性的进行，效果优良。

评价人：雒林萍　　时间：2017.10.21

陕西盛田能源服务股份有限公司
Shanxi Shengtian Energy Solution Service Co.,Ltd.

受控

西咸物联E能源软件平台应急处理预案

（本文件自2017年10月20日起执行）

STNY-D-42-01

编制：孔令敦 2017.1020

审核：王斌 2017.10.20

批准：徐军 2017.10.20

一、系统信息

系统全称	西咸物联 E 能源软件平台
甲方单位	西咸新区物联科技有限公司
乙方单位	陕西盛田能源服务股份有限公司
系统管理部门	软件开发部
系统运行环境	系统访问地址：http://117.34.95.36:9194/LoginPage.aspx 采集服务器 IP：117.34.95.36 采集服务器操作系统：windows Server 2008 应用服务器 IP：117.34.95.37 应用服务器操作系统：windows Server 2008 应用服务中间件：Tomcat 8.5 数据库服务器 IP：117.34.95.38 数据库服务器操作系统：windows Server 2008 数据库名称：SQL Server 2008 其它注意事项：

二、系统负责人

	所属部门	姓名	联系方式
直接负责人	软件开发部	巩亚魁	办公座机：02985550454 手机：18509266958
间接负责人	软件开发部	徐辉	办公座机：02985550454 手机：18729360797
部门负责人	软件开发部	孔令歆	办公座机：02985550454 手机：13363957124
		王斌	办公座机：02985550454 手机：18691938500

三、系统故障分类

故障分类	故障描述

故障分类	故障描述
采集服务故障	采集服务发生故障，导致数据通讯出现中断或者异常，统称为“采集服务故障”
应用服务故障	应用服务中间件 Tomcat 的应用服务发生故障，导致应用服务自动关闭、系统登录页面无法访问、程序部署文件异常、服务日志内容异常、APP 无法访问时，统称为“应用服务故障”。
数据库故障	数据库管理系统软件（SQL Server）或数据库本身发生故障，导致数据库中业务数据无法访问、数据库日志异常等情况发生，统称为“数据库故障”。
网络故障	本地局域网络发生故障导致局域网不通、系统无法访问、系统访问报错等情况，统称为“网络故障”。
服务器硬件故障	应用服务器、数据库服务器发生硬件故障，导致服务器关闭或损坏、应用服务或数据库无法访问等情况发生，统称为“服务器硬件故障”。
非法入侵系统或服务器	应用服务遭到未授权入侵、应用服务器或数据库服务器遭到未授权访问，导致应用服务无法访问、数据库无法访问、数据丢失或泄密等情况，统称为“非法入侵系统或服务器”。

四、系统预防措施

1、采集程序备份

直接负责人负责采集系统的程序备份工作，要求在部门代码库中保持系统程序最新版本。在进行程序修改和更新过程中必须保证服务器端和代码库中的程序版本一致。

间接负责人有责任及权利监督检查直接负责人的采集系统程序备份工作。

2、应用程序备份

直接负责人负责应用系统的程序备份工作，要求在部门代码库中保持系统程序最新版本。在进行程序修改和更新过程中必须保证服务器端和代码库中的程序版本一致。

间接负责人有责任及权利监督检查直接负责人的应用系统程序备份工作。

3、数据库备份

直接负责人负责数据库系统的程序备份工作，要求在部门代码库中保持系统程序最新版本。在进行程序修改和更新过程中必须保证服务器端和代码库中的程序版本一致。

间接负责人有责任及权利监督检查直接负责人的数据库系统程序备份工作。

直接负责人负责设置数据库自动备份策略，并要求定期对备份文件进行检查。备份基本原则：

1) 要求数据库定期进行备份

2) 要求定期删除过期备份文件，以保证硬盘空间足够产生新备份文件

3) 要求定期检查数据库管理软件相关的日志信息，确保数据库管理系统的正常运行

间接负责人有责任及权利监督检查直接负责人的数据库备份工作。

4、应用系统管理员账号、密码管理

直接负责人负责应用系统（包括权限平台、工作流平台等软件）管理员登录账号、密码的管理工作，要求账号和密码要具有一定复杂度（字母、数字、符号混合使用），并定期进行更改，账号和密码未经上级领导授权不得随意告诉他人使用。

间接负责人有责任及权利监督检查间接负责人的账号、密码管理工作。

5、服务器操作系统账号、密码管理

直接负责人负责采集、应用和数据库服务器端操作系统登录账号、密码的管理工作，要求账号和密码要具有一定复杂度（字母、数字、符号混合使用），并定期进行更改，账号和密码未经上级领导授权不得随意告诉他人使用。

间接负责人有责任及权利监督检查直接负责人的账号、密码管理工作。

五、系统应急处理措施

当系统发生故障时，系统直接负责人应立即通知部门经理，并即刻前往故障现场，如因特殊情况无法及时赶到，应立即通知间接负责人代替前往。

系统负责人到达故障现场后，应首先判断故障的类型和严重性，根据结论决定是否需要其他相关人等（部门经理、另一系统负责人、其他相关部门负责人等）也立刻赶往现场协助排障，如

有需要则立即电话通知。

在故障现场，系统负责人全权指挥系统的应急处理过程，根据故障类型安排相关人等的应急处理工作。

1) **当发生采集服务故障时，应按如下步骤依次尝试排障：**

a) 尝试重新启动采集服务，并检查故障是否恢复；

b) 尝试重新启动采集中间件服务，并检查故障是否恢复；

c) 采集服务启动后，检查其所占 CPU 和内存大小，排查是否所占资源异常；

d) 检查采集服务相关日志文件，寻找故障发生原因；

e) 检查操作系统相关日志文件，寻找故障发生原因，如有必要可重新启动操作系统；

f) 检查采集程序部署文件，排查是否有文件异常上传或改变；

g) 检查采集服务控制台，排查是否有异常文件被部署并发布；

2) **当发生应用服务故障时，应按如下步骤依次尝试排障：**

a) 尝试重新启动应用服务，并检查故障是否恢复；

b) 应用服务启动后，检查其所占 CPU 和内存大小，排查是否所占资源异常；

c) 检查应用服务相关日志文件，寻找故障发生原因；

d) 检查操作系统相关日志文件，寻找故障发生原因，如有必要可重新启动操作系统；

e) 检查数据库中的系统登录记录表，排查是否有异常登录发生；

f) 检查应用程序部署文件，排查是否有文件异常上传或改变；

g) 检查应用服务控制台，排查是否有异常文件被部署并发布；

3) **当发生数据库故障时，应按如下步骤依次尝试排障：**

a) 不要重启数据库或数据库应用服务器；

b) 先检查数据库最近一次备份文件是否存在，如存在则先拷贝至移动存储设备中一份，尝试手动备份当前数据库数据，并将备份文件拷贝至移动存储设备中；

c) 如数据库无法访问，先登录应用服务控制台，排查数据库链接是否异常；

d) 使用 SQL Server 数据库管理软件尝试连接数据库，排查数据库是否运行正常；

e) 检查数据库相关日志文件，排查数据库是否运行正常；

f) 检查数据库中系统登录记录表，排查是否有异常登录发生；

g) 尝试重启数据库或数据库应用服务器，并检查故障是否恢复；

h) 如有必要可重新安装数据库系统，并利用备份文件将原有业务数据恢复最新版本；

4) **当发生网络故障时，应按如下步骤依次尝试排障：**

a) 检查服务器网卡、交换机等网络设备，排查是否硬件损坏或松动；

b) 如确认是网络故障，应立即联系网络管理部门到达现场进行排障；

c) 网络排障后，应立即检查应用服务和数据库访问是否正常，并检查数据库备份文件是否缺失，如有上述情况发生应立即予以补救；

5) **当发生服务器硬件故障时，应按如下步骤依次尝试排障：**

a) 当发生服务器硬件故障时，如果服务器已经关闭，不要擅自开机，以免因短路等原因对服务器造成再次伤害；

b) 立即联系服务器管理部门，要求其立刻派人到达故障现场对服务器及相关附属硬件资源进行排查；

c) 故障排除后，应立即对服务器上与应用系统相关的重要文件、数据、程序等进行备份，备份应采用移动存储设备或网络异机拷贝方式进行，以免硬件损坏导致信息丢失；

d) 备份工作完成后，应对服务器上的应用服务运行环境进行一次全面检查，目的是排查硬件故障是否导致系统运行环境发生异常变化，如发生异常变化应及时修复或调整；

6) **当发生系统或服务器遭受非法入侵时，应按如下步骤依次尝试排障：**

a) 发现系统或服务器遭受非法入侵后，应立即断开网络、关闭应用服务，以防止被继续入侵产生更大损失；

b) 检查应用系统运行环境和服务器，排查非法入侵的途径和方式，认真检查应用系统、数据库、服务器中是否留有病毒、木马、人为存放的恶意后门程序等；

c) 紧急更改应用系统、服务器操作系统等相关登录账号和密码，防止再次遭受非法入侵；

d) 如有必要可暂时停止应用服务的使用，寻找问题解决办法，对所有管辖下的服务器进行紧急安全补救，确保其它服务器不发生同样的非法入侵情况；

e) 对非法入侵的后果进行评估，如实向上汇报非法入侵情况和解决方案；

f) 系统故障排除后，现场系统负责人需填报一张“系统故障排除记录表”，将本次故

障情况、排障经过、排障结果等情况如实填写记录在案，该表由系统负责人和部门经理签字确认，然后正式归档以备今后查阅对比使用。

六、签字页

我已阅读了本预案中各部分的内容，并充分了解了我所拥有的权利和责任。我保证在本系统发生故障时，将严格按照应急处理预案中的内容进行排障，并在排障过程中尽到我所应尽到的责任和义务。

系统负责人（签字）： 部门经理（签字）：

签字日期： 签字日期：

系统故障排除记录表

系统名称			
故障发生日期		故障排除日期	
故障处理人		协助人员	
故障描述			
排障经过描述			
排障结果			
系统负责人签字： 签字日期：		部门经理签字： 签字日期：	

陕西盛田能源服务有限公司
Shanxi Shengtian Energy Solution Service Co.,Ltd.

受控

操作系统备份与恢复操作规程

（本文件自 2017 年 10 月 20 日起执行）

STNY-C-34

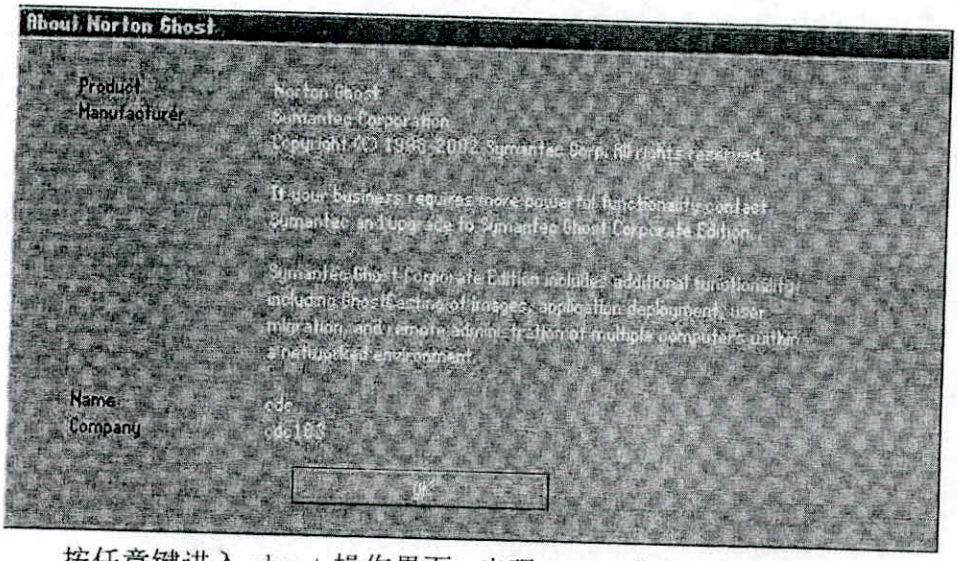
编制：孔令敏. 2017.10.20

审核：王[illegible] 2017.10.20

批准：[illegible] 2017.10.20

一、使用 Ghost 软件工具进行备份

运行 ghost：（我们通常把 ghost 文件复制到启动软盘（U 盘）里，也可将其刻录进启动光盘，用启动盘进入 Dos 环境后，在提示符下输入 ghost，回车即可运行 ghost，首先出现的是关于界面，如图 1：



按任意键进入 ghost 操作界面，出现 ghost 菜单，主菜单共有 4 项，从下至上分别为 Quit（退出）、Options（选项）、Peer to Peer（点对对，主要用于网络中）、Local（本地）。一般情况下我们只用到 Local 菜单项，其下有三个子项：Disk（硬盘备份与还原）、Partition（磁盘分区备份与还原）、Check（硬盘检测）。

由于 Ghost 在备份还原是按扇区来进行复制，在操作时一定要小心，不要把目标盘（分区）弄错了，要不将目标盘（分区）的数据全部抹掉。

二、 分区备份

（一） Partition 菜单简介

其下有三个子菜单：

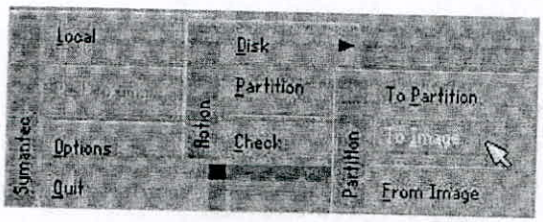
To Partion：将一个分区（称源分区）直接复制到另一个分区（目标分区），注意操作时，目标分区空间不能小于源分区；

To Image：将一个分区备份为一个镜像文件，注意存放镜像文件的分区不能比源分区小，最好是比源分区大；

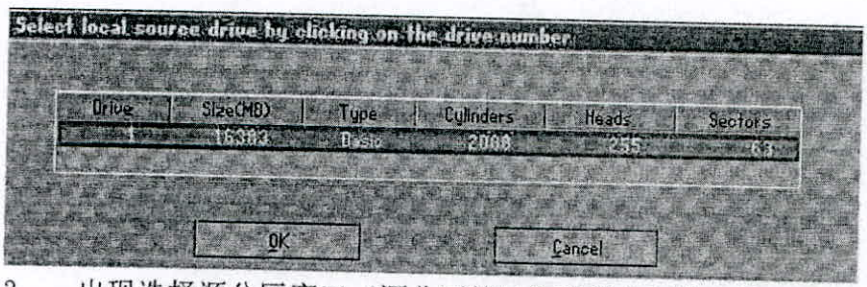
From Image：从镜像文件中恢复分区（将备份的分区还原）。

（二） 分区镜像文件的制作

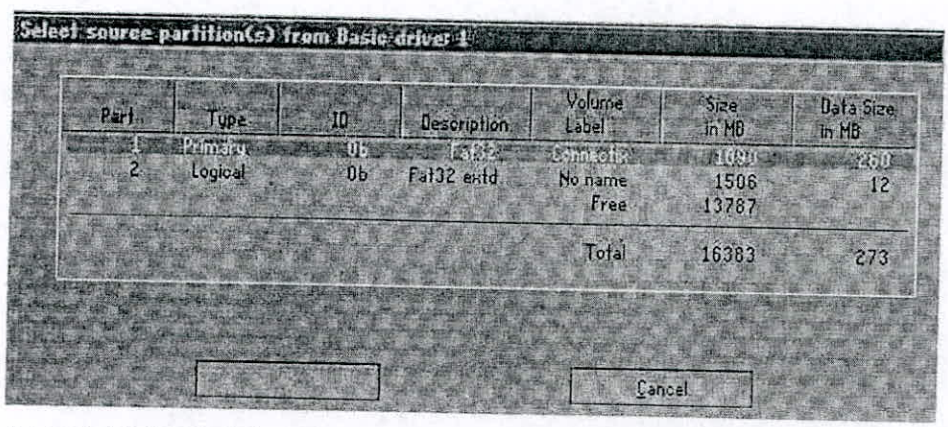
1、 运行 ghost 后，用光标方向键将光标从“Local”经“Disk”、“Partition”移动到“To Image”菜单项上，如图 2，然后按回车。



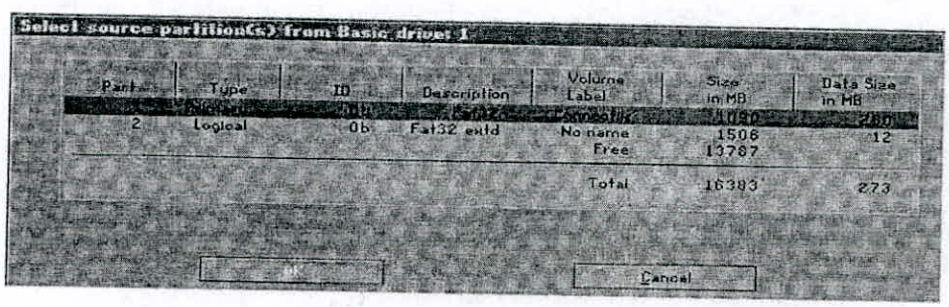
2、 出现选择本地硬盘窗口，如图 3，再按回车键。



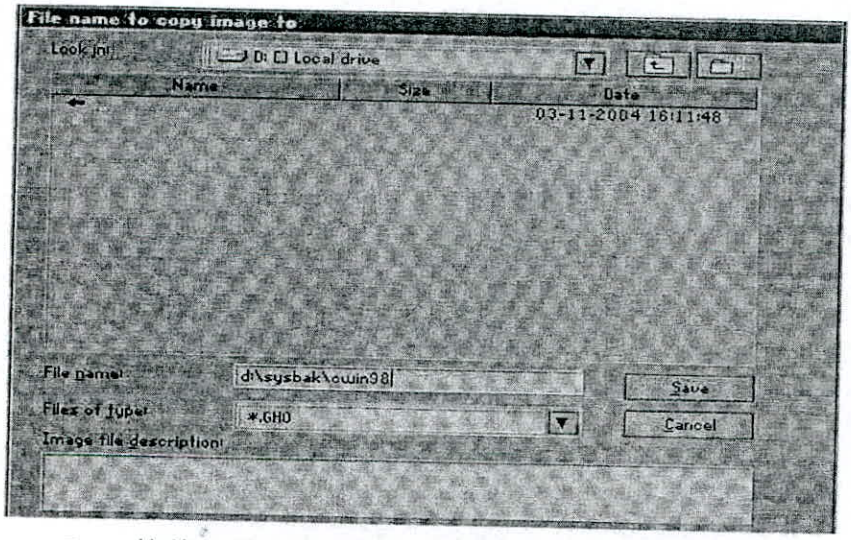
3、 出现选择源分区窗口（源分区就是你要把它制作成镜像文件的那个分区），如图 4:



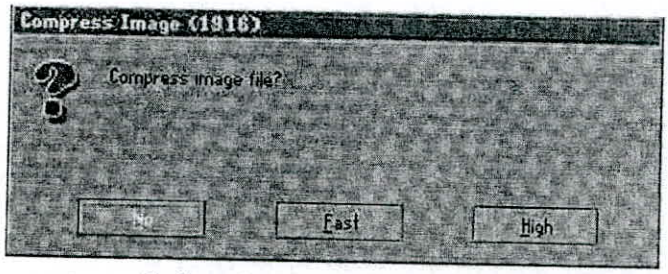
用上下光标键将蓝色光条定位到我们要制作镜像文件的分区上，按回车键确认我们要选择的源分区，再按一下 Tab 键将光标定位到 OK 键上（此时 OK 键变为白色），如图 5，再按回车键。



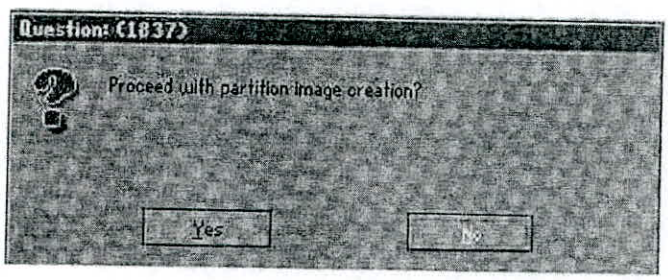
4、 进入镜像文件存储目录，默认存储目录是 ghost 文件所在的目录，在 File name 处输入镜像文件的文件名，也可带路径输入文件名（此时要保证输入的路径是存在的，否则会提示非法路径），如输入 D: sysbak cwin98，表示将镜像文件 cwin98.gho 保存到 D: sysbak 目录下，如图 6，输好文件名后，再回车。



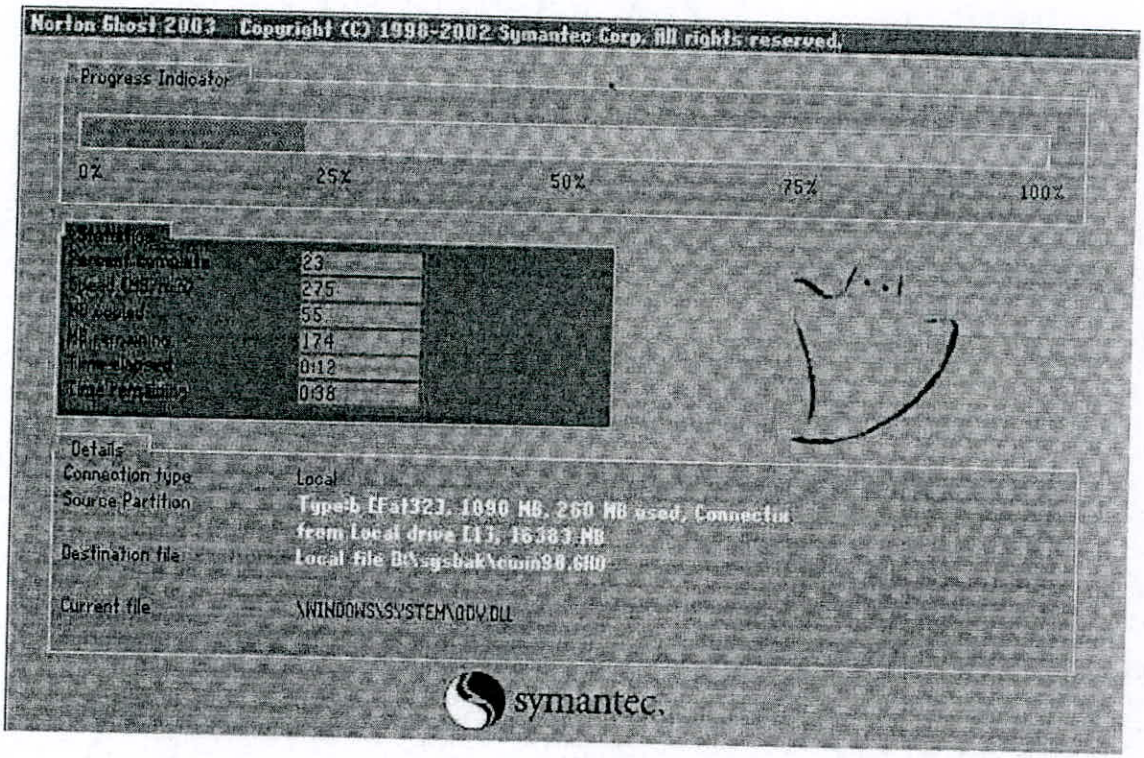
5、 接着出现“是否要压缩镜像文件”窗口，如图 7，有“No（不压缩）、Fast（快速压缩）、High（高压缩比压缩）”，压缩比越低，保存速度越快。一般选 Fast 即可，用向右光标方向键移动到 Fast 上，回车确定；



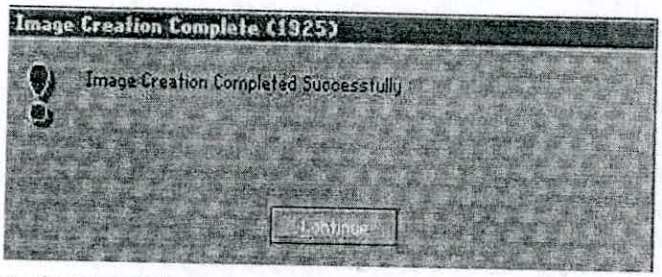
6、 接着又出现一个提示窗口，如图 8 所示，用光标方向键移动到“Yes”上，回车确定。



7、 Ghost 开始制作镜像文件，如图 9 所示：



8、 建立镜像文件成功后，会出现提示创建成功窗口，如图 10：



回车即可回到 Ghost 界面；

9、 再按 Q 键，回车后即可退出 ghost。

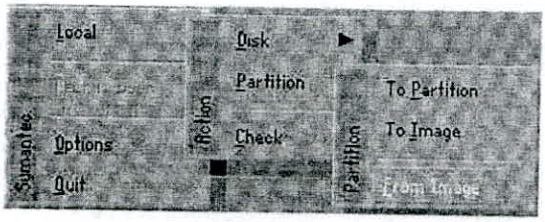
至此，分区镜像文件制作完毕！ 也蛮简单的嘛：）。

三、 从镜像文件还原分区

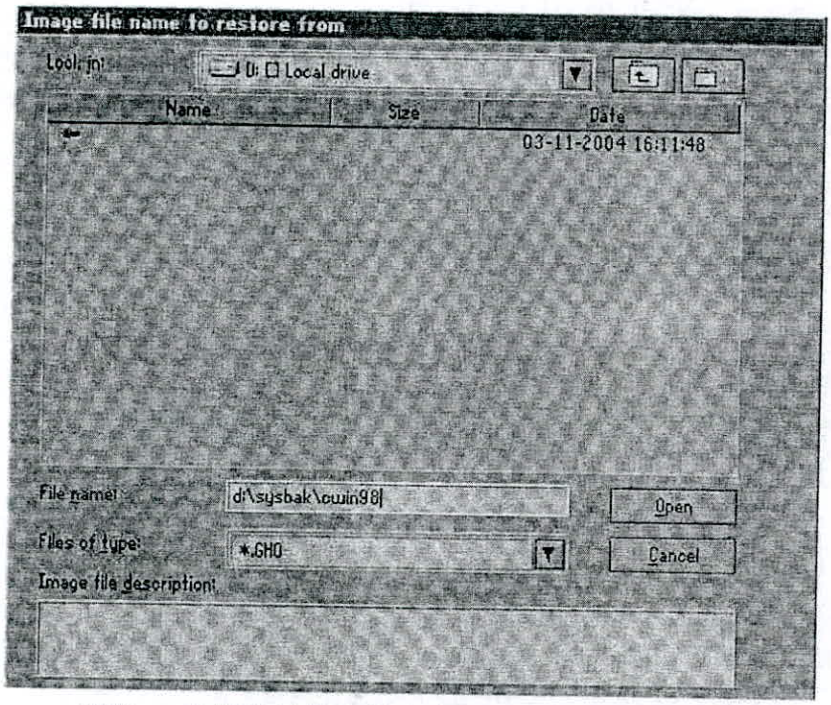
制作好镜像文件，我们就可以在系统崩溃后还原，这样又能恢复到制作镜像文件时的系统状态。下面介绍镜像文件的还原。

（一）在 DOS 状态下，进入 Ghost 所在目录，输入 Ghost 回车，即可运行 Ghost。

（二）出现 Ghost 主菜单后，用光标方向键移动到菜单“Local－Partition－From Image”，如图 11 所示，然后回车。

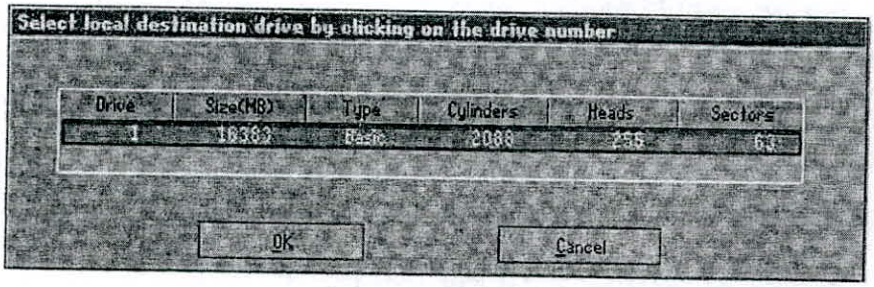


（三） 出现“镜像文件还原位置窗口”，如图 12 所示，在 File name 处输入镜像文件的完整路径及文件名（你也可以用光标方向键配合 Tab 键分别选择镜像文件所在路径、输入文件名，但比较麻烦），如 d: sysbak cwin98.gho，再回车。



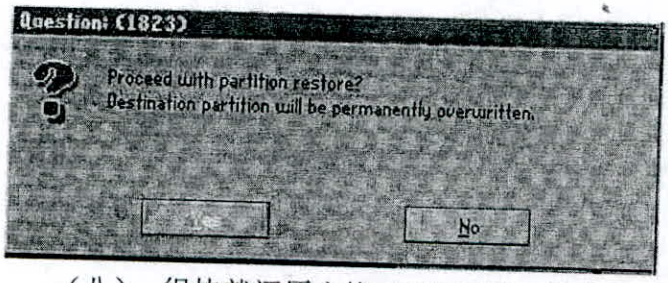
（四） 出现从镜像文件中选择源分区窗口，直接回车。

（五） 又出现选择本地硬盘窗口，如图 13 所示，再回车。

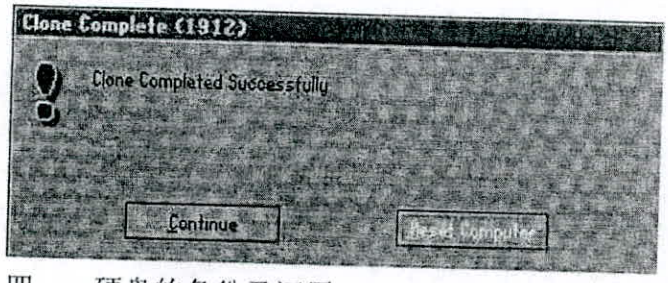


（六） 出现选择从硬盘选择目标分区窗口，我们用光标键选择目标分区（即要还原到哪个分区），回车。

（七） 出现提问窗口，如图 14 所示，选 Yes 回车确定，ghost 开始还原分区信息。



（八） 很快就还原完毕，出现还原完毕窗口，如图 15 所示，选 Reset Computer 回车重启电脑。



四、 硬盘的备份及还原

Ghost 的 Disk 菜单下的子菜单项可以实现硬盘到硬盘的直接对拷（Disk—To Disk）、硬盘到镜像文件（Disk—To Image）、从镜像文件还原硬盘内容（Disk—From Image）。

在多台电脑的配置完全相同的情况下，我们可以先在一台电脑上安装好操作系统及软件，然后用 ghost 的硬盘对拷功能将系统完整地“复制”一份到其它电脑，这样装操作系统可比传统方法快多了哦：）。

Ghost 的 Disk 菜单各项使用与 Partition 大同小异，而且使用也不是很多，在此就不赘述了。

五、 Ghost 使用方案

1、最佳方案：完成操作系统及各种驱动的安装后，将常用的软件（如杀毒、媒体播放软件、office 办公软件等）安装到系统所在盘，接着安装操作系统和常用软件的各种升级补丁，然后优化系统，最后你就可以用启动盘启动到 Dos 下做系统盘的克隆备份了，注意备份盘的大小不能小于系统盘！

2、 如果你因疏忽，在装好系统一段间后才想起要克隆备份，那也没关系，备份前你最好先将系统盘里的垃圾文件清除，注册表里的垃圾信息清除（推荐用 Windows 优化大师），然后整理系统盘磁盘碎片，整理完成后到 Dos 下进行克隆备份。

3、 什么情况下该恢复克隆备份？

当你感觉系统运行缓慢时（此时多半是由于经常安装卸载软件，残留或误删了一些文件，导致系统紊乱）、系统崩溃时、中了比较难杀除的病毒时，你就要进行克隆还原了！有时如果长时间没整理磁盘碎片，你又不想花上半个小时甚至更长时间整理时，你也可以直接恢复克隆备份，这样比单纯整理磁盘碎片效果要好得多！

4、最后强调：在备份还原时一定要注意选对目标硬盘或分区

陕西盛田能源服务股份有限公司
Shanxi Shengtian Energy Solution Service Co.,Ltd.

受控

网络故障排查手册

（本文件自 2017 年 10 月 20 日起执行）

STNY-C-33

编制：孔令敬 2017.10.20

审核：王锦 2017.10.20

批准：[illegible] 2017.10.20

【互联网专线】

一、客户所有电脑不能上网，网管正常

1、 可以远程登陆路由器可能的故障原因及解决思路：

2、 有可能是客户侧路由器配置口插入网线。

3、 内网中 ARP 病毒。

4、 交换机故障，查看是否上电

5、 查看交换机连接到路由器的网线是否有松动

（1）客户无法 ping 通网关(192.168.1.1)

查看是否获取到正常的 IP 地址（192.168.1.X），或者禁用网卡再启用，还是不行就重启下电脑。

（2）客户可以 ping 通网关

可以尝试重启下电脑，因为有可能是客户浏览器问题导致。

（3）本地连接受限

1. 查看下路由器 DHCP 是否有配置，如果有就叫客户禁用网卡再启用，
2. 还是不行就重启下电脑。
3. 如果还是受限就叫客户手动配置 IP 地址（192.168.1.100 以后的没有人用的）跟首选 DNS

6、 无法远程登陆路由器可能的故障原因及解决思路：

1. 查看网管是否掉点，查看系统附件是否有路由器配置附件，打开查看是否有配置远程登入
2. 尝试 PING 客户侧外网 IP 地址，请到跳板上 PING，因为部分集团有配置禁 PING，只有跳板才可以 PING 通。
3. 查看设备是否有上电。

假如无法远程登陆路由器没必要判断以下三种情况（除非可以 PING 通客户侧外网 IP）

（1）客户无法 ping 通网关

1. 确认网关是否上电
2. 确认连接网线是否连通
3. 确认网络是否完好

（2）客户可以 ping 通网关

1. 确认网关与内网是否连通
2. 内网设备是否上电

（3）本地连接受限

1. 网卡驱动是否正常安装，更新网卡驱动
2. 定位网络连接故障原因，然后复位网络

二、客户部分电脑不能上网

1. 基本为客户侧内网问题，假如对方懂网络就直接跟他说我们可以连接到你们那边的路由器，外网一切正常，请查看下内网问题。（内网的问题基本为客户自己解决）
2. 可以与客户沟通，将设备重启

三、客户反映网速慢

1. 询问客户具体什么慢，是打开网页慢还是下载速度慢

2. 如果是打开网页慢，询问下是开打所以网页慢还是特别哪几个网页慢，教客户电脑手动配置DNS。如果更改完客户侧电脑的 DNS 可以解决网络慢的问题，就在路由器上配置将 DNS 更改，更改完与客户说将本地网卡禁用再启用下，因为路由器下配置需要将网卡重新启用后才生效。
3. 还有一种可能打开网页慢是因为客户内网有人在下载之类的，登入路由器，2M 带宽极限下载速度是 250KB/S.但是操作系统会预留 10%左右的带宽做系统使用,所以实际带宽也就在 225KB/S 左右.加上线路的一些问题,某些软件的自动更新占用;杀毒软件的占用,可用的下载带宽也就在 210 左右了吧.210 左右就算已经很高了。
迈普如下：查看箭头处是多少值，然后换算下，是不是在申请带宽范围内， 记得迈普和华为是 b/s 需要换算成 B/s，1B/s=8b/s。

```
新东方培训学校#sh interface fastethernet 0
fastethernet0:
    line protocol is up
    Flags: (0xc008063) BROADCAST MULTICAST ARP RUNNING
    Type: ETHERNET_CSMACD
    Internet address: 112.5.128.35/24
    Broadcast address: 112.5.128.255
    Queue strategy: FIFO , Output queue: 0/256 (current/max packets)(0)
    Metric: 0, MTU: 1500, BW: 100000 Kbps, DLY: 100 usec, VRF: global
    Reliability 255/255, Txload 1/255, Rxload 1/255
    Ethernet address is 0001.7aae.40d0
    5 minutes input rate 84000 bits/sec, 67 packets/sec
    5 minutes output rate 600000 bits/sec, 83 packets/sec
    346420569 packets received; 418184731 packets sent
    55457 multicast packets received
    339366 multicast packets sent
    2923 input errors; 0 output errors
    0 collisions; 5285 dropped
    Unknown protocol 0
    Rate:  100Mbit/s Duplex:  full duplex
    Tx late collision 0, Tx retransmit limit 0, Tx underrun 0
    Tx carrier sense 0, Rx length violation 0
    Rx not aligned 0, Rx CRC error 0, Rx overrun 0
    Rx too small 0, Rx alloc mbuf fail 0
新东方培训学校#
```

input 是下载带宽，output 是上传带宽，如果换算出来的总下载或上传接近给予的带宽就是说明客户侧现在正有人在下载之类的，从而导致网速慢。 于客户说明情况就可以了

四、客户反映访问部分网站慢
1.有可能是 DNS 解析问题，尝试更换 DNS
2.查看路由器带宽使用情况，是否接近给予的带宽就是说明客户侧现在正有人在下载之类的，从而导致网速慢。 于客户说明情况就可以了

五、客户有外接路由器

【路由器的常见操作】
1、 ping 较多数据包 tracert 等常见命令
中兴（1000 个包，长度 100）

ping x.x.x.x repeat 1000 limit 0 size 100

tracert x.x.x.x

迈普（1000 个包，长度 100）
使用扩展 ping
ping
ip
x.x.x.x
1000
100
一直回车结束

tracert x.x.x.x

华为（1000 个包，长度 100）
ping -c 1000 -s 100 x.x.x.x

tracert x.x.x.x

2、限速（路由器上限速没用，对于迅雷等软件不管用，不建议在路由器上做限速，建议客户内部使用网管软件 P2P 等软件来管理）

3、端口映射
迈普
在 conf t 模式下：
ip nat inside source static tcp 192.168.1.111 3389 113.18.101.193 3389
ip nat inside source list 1001 interface fastethernet0 overload

4、查看端口流量、在线用户数及端口状态
迈普
在线数：show arp
查看端口流量、端口状态:

```
新东方培训学校#sh interface fastethernet 0
fastethernet0:
     line protocol is up
     Flags: (0xc008063) BROADCAST MULTICAST ARP RUNNING
     Type: ETHERNET_CSMACD
     Internet address: 112.5.128.35/24
     Broadcast address: 112.5.128.255
     Queue strategy: FIFO , Output queue: 0/256 (current/max packets)(0)
     Metric: 0, MTU: 1500, BW: 100000 Kbps, DLY: 100 usec, VRF: global
     Reliability 255/255, Txload 1/255, Rxload 1/255
     Ethernet address is 0001.7aae.40d0
     5 minutes input rate 84000 bits/sec, 67 packets/sec
     5 minutes output rate 600000 bits/sec, 83 packets/sec
     346420569 packets received; 418184731 packets sent
     55457 multicast packets received
     339366 multicast packets sent
     2923 input errors; 0 output errors
     0 collisions; 5285 dropped
     Unknown protocol 0
     Rate:  100Mbit/s Duplex:  full duplex
     Tx late collision 0, Tx retransmit limit 0, Tx underrun 0
     Tx carrier sense 0, Rx length violation 0
     Rx not aligned 0, Rx CRC error 0, Rx overrun 0
     Rx too small 0, Rx alloc mbuf fail 0

新东方培训学校#
```

5、添加无线路由器

不用再移动路由器设置，只要在客户的无线路由器设置就可以了：

1. 将无线路由器的 IP 地址更改成其他内网网段（比如客户内网网段为 192.168.1.X，则无线路由器 IP 可设置为 192.168.10.1）
2. 关闭无线路由器的 DHCP 功能
3. 交换机连接无线路由器时不要接在无线路由器的 WLAN 口，而是接在无线路由器的 LAN 口

6、客户装软件要求开放某些端口 （就是以上的端口映射）

【M100 设备告警信息】

1. 第一路 LOS 灯是否亮起来，亮起来表示光缆告警，第二路 LOS 灯基本为备用，亮不亮无所谓。
2. MAJ 灯亮起表示重大告警，基本为光缆故障
3. MIN 灯表示简单告警，基本为误码或者光衰有一点异常之类的，但是基本不会影响业务。

【ONU 的设备告警信息】

电源旁边的 LINK 灯如果不亮基本为光缆故障

【广域网专线】

网管掉点

查看是否 M100 上有出现第一路 LOS 灯亮起

网管未掉点

查看 MAJ 灯与 MIN 灯是否有亮起

【语音专线】
处理拨测，预处理还可以做什么呢？
询问客户具体情况，是否全部电话无法拨打还是其他什么情况

网管若掉点且客户侧已上电，是否只能去现场测试光路？
恩，是的，最好能询问客户什么时候开始故障的

生效日期
2017-07-20

北京天一正认证中心有限公司
BEIJING TIANYIZHENG CERTIFICATION CENTER LIMITED COMPANY

管理体系认证审核报告

■ISMS　■初审 ❒再认证❒第 次监督 ❒体系变化

受审核方： 陕西盛田能源服务股份有限公司

审核组长：

批　　准：

（认证中心　公章）

注册地址：北京市西城区月坛北小街 2 号院 1 号楼　邮　编：100830
办公地址：北京市丰台区小屯路航天石化大厦 11 层　邮　编：100071
网址：www.btcc.com.cn　E-mail：btcc@btcc.com.cn

管理体系认证审核报告（续）

一、基本信息						
组织名称	陕西盛田能源服务股份有限公司					
注册地址	陕西省西安市高新区沣惠南路 34 号摩尔中心 B 座 1602-1 710065					
办公地址	陕西省西安市高新区沣惠南路 34 号摩尔中心 B 座 1602-1 710065					
生产地址	陕西省西安市高新区沣惠南路 34 号摩尔中心 B 座 1602-1 710065					
法人代表	管小乔			管理者代表	王斌	
联系人	雒林萍	电话	029-61873303，15109285853	传真	029-86775759	
上次审核时间（监督或再认证适用）			年 月 日 至 年 月 日(共 天)			
审核类别	I：正式审核	审核日期	2017 年 10 月 12 日上午 09:00:00 至 2017 年 10 月 15 日上午 12:30:00（共 3.5 天）			
审核目的	■初 审：评价组织管理体系与所选定的认证标准的符合性、有效性及满足法律、法规(或合同)要求的能力，确定是否推荐注册。 □ 再认证：验证组织的管理体系整体的持续有效性，以及认证范围的持续相关性和适宜性，确定是否推荐再认证注册。 □ 监 督：验证组织管理体系是否持续满足要求，确定是否推荐保持认证注册。 □ 机构转换：验证组织管理体系是否持续满足要求，确定是否推荐转换认证注册资格。 □ 专 项：评价组织变化的管理体系与所选定的认证标准的符合性、有效性及满足法律、法规（或合同）要求的能力，确定是否同意组织的申请并换发认证证书。 □ 恢 复：确认在暂停期内，获证组织的管理体系的运行情况，证书、标志使用情况。					
体系覆盖范围	评审范围	A.产品和活动范围 I：与能源管理系统软件的开发；能源数据采集嵌入式控制系统的开发及其系统的集成；二氧化碳热泵控制系统软件的开发；智慧楼宇控制系统软件的开发及其系统的集成；物联网检测设备、控制设备采集器的研发、生产和销售相关的信息安全管理活动。（适用性声明版本：V1.0；时间：2017.3.1）(04.08；04.13/04h；04m)； B.组织单元/场所、活动和过程详见“审核计划”。					
	审核界定范围	A.产品和活动范围 同上 B.被审核的组织单元/场所、活动和过程详见审核综述。					
	变化理由						
	场所边界、活动的界定	办公活动:陕西省西安市高新区沣惠南路 34 号摩尔中心 B 座 1602-1。 生产活动：陕西省西安市高新区沣惠南路 34 号摩尔中心 B 座 1602-1 以及系统集成现场的认证范围内的相关活动。					

管理体系认证审核报告（续）

审核依据	■GB/T22080-2016/ ISO/IEC 27001:2013 ■管理体系文件有效版本 ■相关的法律法规及其他要求 ■合同 □			
审核组成员	组内职务	姓名	注册资格	注册证号
	组长	岳增武	I：审核员	2017-N1ISMS-1214131
	组员	李庆	I：审核员	2017-N1ISMS-1015806
	组员	李贞	I：实习	2017-N0ISMS-1100987
	组员	张忠琪	I：实习	2017-N0ISMS-1203383

二、审核综述

1. 审核组分 2 个小组审核了下列部门的管理活动，主要审核路线及审核方法：

采取按部门审核的方法；A 组审核了办公室、工程运维部、财务部；B 组审核了管理层、技术部、市场部；审核路线主要是：A 组：会议室审核文件资料-部门办公室-集成现场-财务室；B 组：会议室审核文件资料-总经理办领导层交流-各部门办公室-网管机房。

2. 审核地点：陕西省西安市高新区沣惠南路 34 号摩尔中心 B 座 1602-1 和集成现场（西咸物联 E 能源项目，位于咸阳世纪大道启迪大厦）

3. 是否使用电视电话或网络交流、远程电子方式等电子化手段进行了审核： □是 ■否

4. 本次审核多现场/临时场所抽样的名称：无

5. 审核中共发现不符合项 3 个，其中严重不符合项 0 个，一般不符合项 3 个，详见不符合项报告。不符合项按标准条款和部门分布：

部门： 办公室； 技术部； 工程运维部。

条款： A8.1.1； A11.2.4； A17.1.3；

6. 不符合项是否形成区域性或系统性分布： □是 ■否

7. 审核计划完成情况（如偏离审核计划情况的说明）：

按照审核计划全部完成审核任务。

8. 文审情况：体系文件审核日期：2017 年 9 月 19 日；文审结论：基本符合要求。

上次审核以来管理体系基本情况概述(监督审核、再认证、专项审核适用)：

1. 主要人员（法人代表、最高管理者、管理者代表、体系归口部门负责人） □无； □有，阐述变化：

2. 组织机构和/或分支机构的变化：□无； □有，阐述变化：

3. 组织名称/注册地址/经营地址： □无； □有，现变更为：

4. 法律地位文件及资质文件是否变化：□否； □是，现变更为：

5. 体系信息文件是否变化：□否； □是,更为情况：

管理体系认证审核报告（续）

安全风险均已降低为低风险（当前可接受风险）。

3 信息安全适用性声明策划情况 适用性声明的策划情况：■符合；□基本符合；□不符合

适用性声明的策划情况描述：编号 STNY-A-02 的《适用性声明》，版本：V1.0；颁布时间：2017.3.1；不适用条款 A14.1.2、A14.1.3、A14.2.7，理由：公司无网上交易业务和外包开放。符合公司实际。

4 信息安全控制措施

1）信息安全策略是否符合相应标准要求：■符合；□基本符合；□不符合；说明：

2）信息安全组织是否符合相应标准要求：■符合；□基本符合；□不符合；说明：

3）人力资源安全是否符合相应标准要求：■符合；□基本符合；□不符合；说明：

4）资源管理是否符合相应标准要求：□符合；■基本符合；□不符合；说明：办公室信息资产清单(STNY-D-01-02)，未见软件著作权无形资产。已开具一般不符合项。

5）访问控制是否符合相应标准要求：□符合；■基本符合；□不符合；说明：

6）密码控制是否符合相应标准要求：■符合；□基本符合；□不符合；说明：

7）物理和环境安全是否符合相应标准要求：□符合；■基本符合；□不符合；说明：未见技术部对已策划的2017年8月27日的检查计划进行实施的记录。已开具一般不符合项。

8）运行安全是否符合相应标准要求：■符合；□基本符合；□不符合；说明：

9）通信安全是否符合相应标准要求：■符合；□基本符合；□不符合；说明：

10）系统获取、开发和维护是否符合相应标准要求：■符合；□基本符合；□不符合；说明：

11）供应商关系是否符合相应标准要求：■符合；□基本符合；□不符合；说明：

12）信息安全事件管理是否符合相应标准要求：■符合；□基本符合；□不符合；说明：

13）业务连续性管理的信息安全方面是否符合相应标准要求：□符合；■基本符合；□不符合；说明：西咸物联E能源项目，未提供对于项目现场进行软件平台应急处理预案进行验证的证据，已开具一般不符合项。

14）符合性是否符合相应标准要求：■符合；□基本符合；□不符合；说明：

15）

5 信息安全策划和控制需改进的方面：

（三）监视、 测量、分析和评价

1. 监视、测量、分析和评价的对象、方法、时机是否符合组织情况：■符合；□基本符合；□不符合

阐述监视和测量的方法及结果：

该公司通过实施不定时间间隔的安全检查、适用标准法律法规及其他要求合规性评价、内部审核、事故报告调查处理、电子监控、定期技术符合性评审等控制措施并报告结果。监视和测量有效。

2. 内部审核的策划及实施情况：■符合；□基本符合；□不符合

1）查阅了内部审核控制程序（文件名称/发布时间）STNY-B-06 《内部审核控制程序》，2017.3.1；

2)最近一次内部审核时间：2017.7.1-2017.7.2 ;发现不符合项数量：2，针对不符合项所采取的纠正措施：■有效；□基本有效；□无效

3）访谈了下列内部审核员（姓名/资格）：王斌 证书编号：YHZX-I-2017-005； 雒林萍 证书编号：YHZX-I-2017-006。

4)查阅了内部审核报告（日期:2017.8.2），对体系■符合性、■充分性和■有效性进行了评价，指出了体系的薄弱环节：无

5）内审持续满足要求、保持信任的情况（再认证适用）：

管理体系认证审核报告（续）

3. 管理评审策划及实施情况：■符合；□基本符合；□不符合

1）描述最近一次管理评审的实施时间、主持人、输入、输出文件：2017 年 08 月 21 日，由总经理徐方军主持，管理评审输入有：信息安全管理体系运行的改进建议；本部门相关的外部反馈意见；本部门改进信息安全管理体系继续的技术、产品和程序；预防和纠正措施的实施情况；本部门相关的有效性测量、考核情况及建议；风险评估未考虑的威胁和薄弱点；提供的资源满足需要的情况；与本部门相关的其他情况；信息安全管理体系变更和改进的建议。等；管理评审输出：《管理评审报告》。

2）管理评审的输入是否符合标准要求：■符合；□基本符合；□不符合

3）管理评审的输出对改进体系是否有价值：■是；□基本具有；□不具有

4）管理评审改进措施的落实情况：1、计算机系统的点检监督监测频次可以再次增加；2、信息沟通还需进一步通畅；3、员工自觉学习的氛围还要加强；4、培训的方式要不断改进；5、现场记录填写的质量存在问题较多，需进一步加强；6、内审员的监督作用需要加强并充分发挥。6 项改进计划 2017 年 12 月份前完成，目前进展顺利。

4.合规义务的识别、获取、确定及合规性评价情况（ISMS 适用）：■符合；□基本符合；□不符合

1）查阅了法律法规、标准和其它要求清单（名称/时间）：《适用的法律法规、标准及其他要求清单》，时间：2017.10.10；（针对一阶段问题进行完善）。

2）查阅了合规性评价报告（编号/结论/时间）：编号： STNY-D-40-01；《信息安全法律法规实施控制一览表》，结论：对公司信息化类、版权类、其他安全类、劳动类共 42 项法律法规进行识别评价，符合规定要求；时间：2017.10.10。

5.测量、分析需改进的方面：

对信息安全事件的报告及调查处理流程需要进一步规范。

（四）改进

1、组织确定和改进的措施和活动类型有：□纠正；□纠正措施；■持续改进；□突变；□创新；□重组

2、不合格和纠正措施实施情况：■符合；□基本符合；□不符合

查阅了下列纠正措施报告（记录名称/时间）：

《纠正措施制定实施报告》，STNY-D-04-02，体系开始运行以后进行的检查中，20170328、20170628 在技术部分别发现的问题：1.测试、正式、开发数据库未分离。2.备份异常。针对以上不合格分别分析了原因，采取了纠正措施，记录了措施实施情况，分别于 20170413 和 20170629 验证了实施结果。

3、持续改进活动描述：

体系方面：已建立体系，在执行过程中各方面会提出改进需求，不断进行改进。及时修改完善文件（附件）。

管理方面，加强信息安全、风险的评审及应对措施的落实；发现风险和措施有遗漏或有误的要进行修正，提出预案；对环境的变化要明确，落实的要求，要形成记录制度的落实和加强等。

ISMS 信息资产的识别和风险的识别及措施和绩效测量综合评价：

共识别信息资产 131 项，信息资产总数量：个；重要资产数量：18 个；风险总数量：50 个；高风险数量：2 个。经过执行风险处置计划对高等级风险和中等级风险进行处理，全部信息安全风险均已降低为低风险（当前可接受风险）；信息资产的识别和风险的识别及措施基本到位。

公司高层领导重视，公司总经理亲自负责并全程参与，副总经理兼管代具体指导组织实施，有力地推动了公司信息安全管理体系的建立、实施、保持和改进工作。信息安全方针得到贯彻，信息安全总目标和各部门信息安全分目标实现，各部门职责权限分明，并得到很好地落实；内部沟通有效，员工信息安全意识明显提高，信息安

管理体系认证审核报告（续）

全管理过程基本受控，持续改进的机制已经建立。

四、审核结论及后续活动

审核结论

受审核方根据本公司及其覆盖产品的实际情况，按 GB/T 22080-2016 标准要求建立、实施、保持和改进的信息安全管理体系，基本符合标准要求，审核中未发现严重不符合项，体系运行正常、整体持续有效，信息安全管理过程基本受控，满足法律法规和信息安全管理要求。

本次审核，共计开出书面不符合项报告 3 项，均属于一般不符合项，对公司的信息安全管理体系整体的有效性没有产生影响。待受审核方对 3 项书面的一般不符合项在规定的期限内纠正并采取有效的纠正措施、提供书面整改材料、经审核组书面验证有效后，同意向北京天一正认证中心有限公司推荐信息安全管理体系的“认证注册”。

审核组对受审核方完成纠正措施所需时间要求

请受审核方制定和实施纠正措施，并将实施效果及证实材料，自现场审核后 30 日（再认证组织宜在原证书到期前至少 5 个工作日）内提交审核组进行：

☐ 现场验证　　■ 书面验证，保留现场验证的权利　　☐

审核方案策划

1. 建议下次审核的时间为 2017 年 10 月， 但应在本次现场审核完成起 12 个月内进行。

2. 需改进的方面和对下次审核关注点的建议：

建议下次审核重点关注精益信息部计算机技术防范措施落实、信息安全事件事态响应等；

本报告与末次会议宣讲内容的差异说明（如有的话）无

声明：本次审核基于抽样检查，因此，不可能包含受审核方管理体系覆盖的产品或服务的全部活动。同样，未发现的不符合项可能存在于目前管理体系的运行中。

审核报告发放清单　　■受审核方　■北京天一正认证中心有限公司　☐委托方（适用时）

审核报告含附件　　件，共 9 页	编制：[illegible]　2017 年 10 月 23 日

不符合项纠正和纠正措施有效性验证情况：

（应包括纠正和纠正措施材料收到的日期，验证过程（可能有多次验证），验证结论，遗留的问题等）

2017 年 10 月 23 日收到纠正和纠正措施材料，对 3 项需要书面验证的材料进行了验证，问题已关闭，可以接受；下次监督审核时对纠正和纠正措施有效性进行进一步验证。

验证人员：[illegible]　　日期：2017 年 10 月 23 日