中国移动通信集团新疆有限公司

ZGYDXJ-SC-2021

一体化管理体系管理手册

（信息技术服务、信息安全一体化管理体系管理手册）

文件版本： A/0
编　　制：王 博
审　　核：王 博
批　　准：蒋文隆

受控状态：受控

2021 年 11 月 1 日发布　　2021 年 11 月 1 日实施

颁布令

为提高中国移动通信集团新疆有限公司的信息安全管理水平，保障我公司业务活动的正常进行，防止由于信息系统的中断、数据的丢失、敏感信息的泄密所导致的公司和客户的损失，以及规范我公司IT信息技术服务管理，提供满足顾客要求的信息技术服务，我公司开展贯彻GB/T22080-2016/ISO27001:2013《信息技术-安全技术-信息安全管理体系-要求》、ISO/IEC20000-1:2018《信息技术-服务管理-服务管理体系要求》国际标准工作，建立、实施和持续改进文件化的信息安全&信息技术服务管理体系，制定了《信息安全&信息技术服务管理》。

《信息安全&信息技术服务管理手册》是企业的法规性文件，是指导企业建立并实施信息安全&信息技术服务管理管理体系的纲领和行动准则,用于贯彻企业的信息安全&信息技术服务管理方针、目标，实现信息安全管理体系有效运行、持续改进，体现企业对社会的承诺。

《信息安全&信息技术服务管理手册》符合有关信息安全法律、法规要求及GB/T22080-2016/ISO27001:2013《信息技术-安全技术-信息安全管理体系-要求》、ISO/IEC20000-1:2018《信息技术-服务管理-服务管理体系要求》标准和企业实际情况，现正式批准发布，自2020年7月15日起实施，企业全体员工必须遵照执行。

全体员工必须严格按照《信息安全&信息技术服务管理手册》的要求，自觉遵循信息安全管理方针，贯彻实施本手册的各项要求，努力实现公司信息安全&信息技术服务管方针和目标。

中国移动通信集团新疆有限公司

总经理：蒋文隆

2021年11月1日

中国移动通信集团新疆有限公司文件

关于印发《中国移动通信集团新疆有限公司一体化管理体系管理手册》的通知

公司各部门：

为了适应行业发展的需要，强化企业管理、合理配置资源，公司从实现企业整体战略目标出发，统一策划、优化过程，按照系统化的原则，整合信息技术服务和信息安全管理体系标准要求，构建集约化、规范化、系统化和文件化的“二合一”的一体化管理体系（Integrated Management System，缩写 IMS）。在这一指导思想下，公司依据 GB/T 22080-2016《信息技术 安全技术 信息安全管理体系 要求》和 ISO/IEC 20000-1：2018《信息技术 服务管理 第 1 部分 服务管理体系 要求》标准要求，组织编写了《中国移动通信集团新疆有限公司一体化管理体系管理手册》（以下简称《一体化管理手册》），并经公司总经理常务会议审议通过，现予以发布。

《一体化管理手册》阐述了公司一体化管理体系工作的总体要求，明确了公司管理层及各部门的管理职责，是指导全公司实施一体化管理体系工作的纲领性文件。公司通过推行一体化标准化管理，力求公司服务管理、信息安全管理工作规范化、科学化、系统化和法制化。体系内各部门及员工必须以《一体化管理手册》为指导，各司其职、各尽其责、同心协力，认真贯彻落实公司管理方针、稳步推进一体化管理的各项工作，并为公司全面、协调、可持续发展作出贡献。

2021 年 11 月 1 日

文件控制页

文件编号	ZGYDXJ-SC-2021		
文件名称	《中国移动通信集团新疆有限公司一体化管理体系管理手册》（简称《一体化管理手册》）		
版 本 号	第 A 版第 0 次（2021 年版）		
受控状态	受控	受控编号	001
编　　制		日　　期	2021 年 11 月 1 日
审　　核		日　　期	2021 年 11 月 1 日
批　　准		日　　期	2021 年 11 月 1 日

更改情况

序号	章节/条款	修改内容	更改人/日期	批准人/日期
	全文	《一体化管理手册》首次发布	王 博 2021.11.1	蒋文隆 2021.11.1
备注				

目　录

前言

采用信息技术服务和信息安全管理体系等标准建设“二合一”一体化管理体系（Integrated Management System，缩写 IMS）是公司重要的战略决策，目的是按照系统化的原则，整合信息技术服务和信息安全管理要求、形成统一而又相互协调、相互兼容、相互补充的有机整体。构建“二合一”一体化管理体系的优势在于能合理配置资源、优化过程、协调目标、规范管理、提升效率，并追求系统整体有效性，以实现公司总的方针目标。

本手册及公司一体化管理体系的其他文件在遵守法律法规要求的基础上，结合了本公司的具体管理特点，并依据 GB/T 22080-2016《信息技术 安全技术 信息安全管理体系 要求》和 ISO/IEC 20000-1：2018《信息技术 服务管理 第 1 部分 服务管理体系 要求》等标准编制。

本手册是公司一体化管理体系实施运行的依据，是本公司信息技术服务管理、信息安全管理工作的纲领性文件。

引言

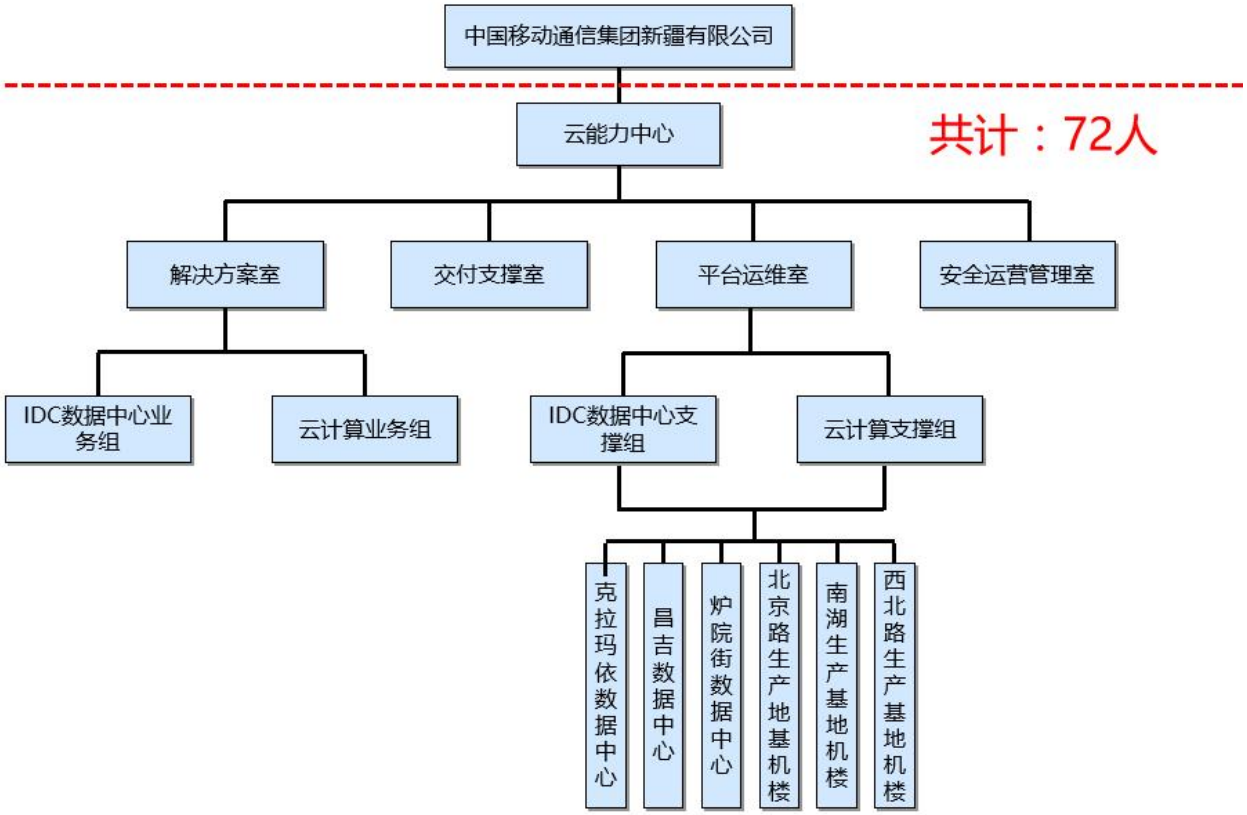
0.1 公司简介

中国移动通信集团新疆有限公司（以下简称“新疆移动”）成立于 2004 年 2 月 3 日，注册资金 25 亿人民币。新疆移动主要经营移动语音、数据、IP 电话和多媒体业务，并具有计算机互联网国际联网单位经营权和国际出入口局业务经营权。除提供基本话音业务外，还提供信息系统集成、安防工程、IT 运维服务、传真、数据、IP 电话等多种增值业务，拥有"全球通"、"神州行"、"移动梦网"、"动感地带"、"神州行天山通"等知名品牌。公司秉承"沟通从心开始"的企业服务理念、"追求客户满意服务"的企业经营宗旨，努力为客户提供一体化的优质服务，极大地满足了客户多样化的通信需求。

新疆移动作为疆内惟一专注移动通信发展的通信运营公司，在网络建设与业务发展方面始终保持领先地位，经过不断地发展与建设，建成了质量一流、覆盖完善、技术领先、通达全国、连接世界的精品网络。移动网络规模和客户数量在疆内遥遥领先。截止 2004 年 8 月，网络已全面覆盖全疆 88 个的地、州、市县，主要交通干线已实现连续覆盖，对高速公路覆盖达 95%，对乡镇团场和主要国道覆盖达 90%。网络总容量达到 410 万门，客户总数达到 320 万户。截至 2005 年 9 月底 ，中国移动与 201 个国家和地区的 250 个运营公司开通了 GSM 国际漫游业务，并与 90 个国家和地区的 71 个运营商开通了 GPRS 国际漫游，国际短信共通达 106 个国家和地区的 214 家运营商，彩信通达 4 个国家和地区的 14 家运营商。

公司内强素质，外塑形象，守法经营，持续发展，先后获得了多项国家级和自治区级荣誉。连续 6 年被中国消费者协会评为"诚信单位"，被自治区授予"突出贡献企业";2004 年被国家交通战备办公室评为全国"交通战备正规化建设先进单位";2005 年获得"全国级青年文明号";2005 年被自治区精神文明建设指导委员会命名为"自治区文明行业"，所有 15 个地州分公司均成功创建成"自治区级文明单位"。

面向未来，中国移动通信确立了"做世界一流企业，实现从优秀到卓越的新跨越"的发展战略目标。围绕这一目标，中国移动新疆公司将秉承"正德厚生，臻于至善"的企业核心价值观，深入贯彻科学发展观，努力提升核心竞争力，通过打造卓越的运营体系，建设卓越的组织，培育卓越的人才，努力成为移动信息专家和卓越品质的创造者，积极推进自治区国民经济和社会信息化发展进程，努力为新疆的繁荣昌盛和稳定做出自己应有的贡献。


中国移动通信集团新疆有限公司
云能力中心
共计：72人
解决方案室
交付支撑室
平台运维室
安全运营管理室
IDC数据中心业务组
云计算业务组
IDC数据中心支撑组
云计算支撑组
克拉玛依数据中心
昌吉数据中心
炉院街数据中心
北京路生产地基机楼
南湖生产基地机楼
西北路生产基地机楼

0.2 管理方针与目标

0.2.1 信息技术服务方针

规划卓越、运行顺畅、服务优质、顾客满意

信息技术服务管理的总体目标包括：

客户服务满意率≥90%

重大变更成功率≥95%

事件解决率≥96%

全年无重大事件发生

客户协定的 SLA 指标达成率 98%以上

信息技术服务管理目标的考核计算方法如下：

	目标	计算方法	考核频次
1	客户满意度达到 90%以上	客户满意度 =（∑客户所打分数/打分客户人数）*100%，客户满意度调查分析表、客户服务报告	半年一次
2	事件解决率达 96%以上	事件解决率=（已解决事件数/受理事件总数）*100%	半年一次
3	客户协定的 SLA 指标达成率 98%以上	SLA 指标达成率=（完成的客户 SLA 指标数量/客户 SLA 指标总数量）*100%	半年一次
4	重大变更成功率达到 95%	重大变更成功率=（成功的重大变更成功数目/重大变更总数目）*100%	半年一次
5	全年无重大事件发生	对发生的重大事件的统计	半年一次

0.2.2 信息安全方针

合法合规、数据保密 、信息完整、 控制风险、 持续改进、 全员参与、 提高绩效、客户满意。

(1) 合法合规。遵循国家相关法律、法规和政策，遵守国家有关信息安全的相关法令、法规及其他规范；遵从中国移动集团数据中心下发的各种标准和规范；遵从内蒙移动数据中心制定的相关制度和规范。

(2) 风险管理。信息安全建设与风险管理紧密相关，信息安全管理控制点应以风险出现的可能性及风险的影响作为对象而展开；建立有效的风险评估机制，通过风险评估识别风险，并采取适当的控制目标与控制方式对风险进行控制，使信息风险被避免、转移或降低到一个可以被接受的水平。

(3) 全员参与。数据中心信息安全工作应全员参与，做到人人有责；形成信息安全的文化，融入到数据中心整体企业文化之中，梳理全员的信息安全意识，并贯穿信息安全工作的始终。

(4) 持续改进。信息安全工作的关键是持续改进。构建信息安全保障体系绝非一日之功，要坚持不懈、持续改进；制定信息安全整体规划，并采用分步实施的方式，集中有限资源，分阶段实现目标；定期进行风险评估，并根据风险评估的结果以及信息安全工作中出现的问题，及时对信息安全工作进行适当调整并不断完善。

公司信息安全总目标如下：

(1) 总体目标

1) 建立科学、完善、有效的信息安全体系，实现动态的、规范的、制度化的信息安全管理，提高数据中心信息安全管理能力，保障数据中心业务持续稳定发展；
2) 构建完善的信息安全组织体系，实现信息安全工作在各个层面的有效衔接，为信息安全决策的制定和落实提供保障。
3) 建立持续有效的信息安全风险管理和响应机制，实现“早预防、严监控、精计量、快反应”和规范化、流程化的风险管理，提高数据中心的安全风险防范能力。

(2) 具体目标

1） 初步建立融合多种标准和监管要求（包括 ISO/IEC 27001、ISO/IEC 20000）的信息化综合保障体系，将相关标准制度规范和监管要求真正落到实处，并与日常的工作流程以及应采取的风险防范措施相结合；

2） 重大信息安全事件（事故）为零；

3） 顾客保密性抱怨/投诉次数≦1 起/年；

4） 机密信息泄露的事态不得发生；

5） 各类信息设施的可用性达到 90%以上；

6） 年度信息安全培训人员覆盖率 100%；有效性测量。

信息安全管理目标的考核计算方法如下：

	目标	计算方法	考核频次
1	重大信息安全事件（事故）为零	期间重大信息安全事件发生数量统计	一年一次
2	顾客保密性抱怨/投诉次数≦1 起/年	顾客保密性抱怨数统计	一年一次
3	机密信息泄露的事态不得发生	机密信息泄露事态发生个数统计	一年一次
4	各类信息设施的可用性达到 90%以上	可用性=（可用信息设备数目/信息设备总数目）*100%	一年一次
5	年度信息安全培训人员覆盖率 100%	覆盖率=被培训人员数目/人员总数目）*100%	一年一次

0.3 管理承诺

我代表中国移动通信集团新疆有限公司郑重向全体员工和社会作出以下承诺：

1、以守法合规为前提，遵守法律规定、履行社会责任；
2、以顾客满意为焦点，追求精益求精，创造精品工程；
3、以安全环保为使命，坚持以人为本，实现和谐发展；
4、致力于满足 IT 服务要求和提供价值；
5、致力于信息安全建设，提升信息安全管理水平；
6、承担一体化管理的最终责任，对公司一体化管理体系的有效性负责；
7、理解相关方的需求和期望，自觉接受顾客和相关方的监督，努力提升管理水平；
8、培育公司特色的企业文化，促进公司可持续性发展；
9、制定公司管理方针，提供资源保障，保证管理目标实现；
10、确保管理体系标准要求融入本公司的经营管理活动和业务过程；
11、支持各级管理人员发挥领导作用，督促和指导员工履行职责；
12、搭建全员参与平台，表彰奖励先进，充分发挥员工的积极性和创造性；
13、确保一体化管理体系实现其预期结果，推动持续改进，提高管理绩效。

总经理：蒋文隆

2021 年 11 月 1 日

0.4 管理者代表

公司各部门：

经公司总经理常务会议研究决定，任命 王 博 同志为中国移动通信集团新疆有限公司一体化管理体系的管理者代表，负责公司信息技术服务和信息安全一体化管理体系的建立、实施、检查和改进。其职责为：

1、协助总经理实现其信息技术服务和信息安全管理职责；

2、代表总经理协调一体化管理体系的相关活动，按照管理体系标准要求建立、完善本公司信息技术服务和信息安全一体化管理体系；

3、负责提高满足顾客要求的意识、持续强化全员安全环保意识；

4、负责组织公司信息安全管理方面的资产识别与评价、风险识别与评价、确定不可接受风险；

5、负责公司风险处置计划的策划、实施；负责公司信息安全策略的策划与实施，确保公司信息安全管理工作的有效开展；

6、负责组织信息技术服务管理体系服务目录的建立、监督服务计划的制定与实现、服务级别协议的达成，确保信息技术服务工作的连续性与有效性。

7、配合总经理配置、调度一体化管理体系建立和运行所需的资源和人员；

8、向总经理报告一体化管理体系的运作情况、绩效和改进的需求；

9、代表总经理落实一体化管理体系有关事宜的外部联络。

总经理：蒋文隆

2021 年 11 月 1 日

0.5 信息安全小组暨信息技术服务小组任命书

公司各部门：

为满足 GB/T 22080-2016《信息技术 安全技术 信息安全管理体系 要求》和 ISO/IEC 20000-1：2018《信息技术 服务管理 第 1 部分 服务管理体系 要求》标准的要求，确保公司一体化管理体系的信息安全和信息技术服务管理工作的策划、实施、保持和改进得到有效开展，确保信息安全管理工作满足顾客和相关方需求，信息技术服务工作由优质走向卓越，公司特此设立信息安全小组，名单如下。信息安全小组成员同时也是信息技术服务小组成员。

特此任命。

信息安全小组暨信息技术服务小组成员名单：

组　长：总经理

副组长：公司领导班子成员

组　员：各部门负责人

总经理：蒋文隆

2021 年 11 月 1 日

0.6 过程方法

0.5.1 总则

公司按照相关管理体系标准的要求、采用过程方法，确定管理体系所需的过程及各过程的相关要求。过程方法结合了“策划、实施、检查、处置”（PDCA）循环和基于风险的思维。

0.5.2 过程方法

公司一体化管理体系在建立、实施、改进时采用过程方法，包括按照公司的管理方针和战略方向，对公司各管理活动、生产服务等过程及其相互作用，系统地进行规定和管理，从而实现预期结果：

——确定一体化管理目标和实现这些目标所需的过程；

——识别顾客和其它相关方的要求和期望，以确定公司期望的过程输出；

——确定每个过程的输入和输出，并建立每个过程运行的准则和方法；

——为管理过程确定职责、权限和义务；

——确定和提供必需的资源和信息；

——确定过程相互依赖的关系，分析个别过程的变更对整个体系的影响；

——管理可能影响过程输出和一体化管理体系整体绩效的风险；

——建立和应用对每个过程实施监视和/或测量及分析的方法；

——将过程及其相互关系作为一个体系进行管理，以有效和高效地实现一体化管理目标；

——运行和改进过程并监视、分析和评价整个体系的绩效。

0.5.3 PDCA 循环

公司一体化管理体系基于策划、实施、检查与改进（PDCA）的运行模式，该模式可应用于公司一体化管理体系及其每个单独的过程。该模式可简述如下：

PDCA 循环可以简要描述如下：

——策划（Plan）：建立管理体系的方针、目标，识别过程和其作用以及管理体系风险变化情况，确定要形成的文件或记录，以达到规定的要求。

——实施（Do）：在资源支持下，依据策划安排，实施并控制管理体系所涉及的过程或活动，在不断运行中优化管理体系。

——检查（Check）：根据规定要求，对过程或活动以及管理绩效进行监视、测量、分析，并记录其结果。

——改进（Action）：建立改进机制，实施管理评审，寻求和采取积极措施，持续改进管理体系和整体业绩。

0.5.4 基于风险的思维

基于风险的思维的是实现一体化管理体系有效性的基础。

基于风险的思维体现在本手册的相关条款（章节）的要求中，通过落实相关要求、确保风险管理工作与其他管理工作紧密结合，并把风险管理的各项要求融入经营管理和业务流程中：

——条款：“4 组织环境”：识别组织环境中的风险和机遇；

——条款：“5 领导作用”：承诺促进“基于风险的思维”的落实，成为员工思想方法和工作习惯；

——条款：“6 策划”：确定一体化管理活动中需应对的风险和机遇，并策划风险和机遇的管理措

施；

——条款：“7 支持”：为管理体系有效运行提供必要的资源，并符合风险现状及风险控制的需要；

——条款：“8 运行”：实施应对风险和机遇的措施，并关注运行过程中的风险和机遇；

——条款：“9 绩效评价”：通过监视、测量、分析和评价活动，评价风险控制措施的有效性；

——条款：“10 持续改进”：识别改进机会，采取措施避免或减少不良影响，提高一体化管理绩效。

0.7 手册的管理

本手册采用 ISO 制定的管理体系标准框架并规定了以下内容：

——一体化管理体系的范围：覆盖的产品、活动及服务的范围；

——一体化管理方针、目标、管理职责、权限；

——一体化管理体系的过程、过程活动顺序及相互作用；

——对管理体系各活动过程的基本要求及对应的程序文件；

——对一体化管理手册编制、审批、发放、更改等过程的管理。

本手册旨在通过对管理体系标准的应用达到以下目的，并通过持续改进，自我完善、追求卓越：

——防范经营风险、履行合规义务；

——理解相关方需求和期望、充分满足顾客要求，增强顾客满意；

——应用风险管理过程，保持信息的保密性、完整性和可用性，为相关方树立风险得到充分管理的信心；

——支持服务生命周期的管理，满足约定的要求并为客户、用户和组织提供价值。

本手册可通过以下方式证实符合管理体系标准的要求：

——公开管理承诺、进行内部审核、实施管理评审；

——接受顾客或相关方的检查与审核，对其符合性进行确认；

——通过认证机构进行认证审核并取得一体化管理体系认证证书。

本手册由安全运营管理室负责组织编制，经管理者代表审核，由总经理批准颁布后实施。

本手册属受控文本，由安全运营管理室统一管理，未经管理者代表批准，任何人不得将管理手册提供给本公司以外人员。本手册持有者负责对手册进行妥善保管，防止丢失、损坏。

1 范围

1.1 公司一体化管理体系覆盖范围(认证范围)

1.1.1 信息技术服务管理体系(IT-SMS)：向客户提供 IDC 数据中心业务、云计算 IaaS 业务（弹性计算、云存储、云网络、云安全、管理与监控）、PaaS 业务及 SaaS 业务(开放云市场业务)运营和运行维护的信息技术服务

1.1.2 信息安全管理体系(ISMS)：向客户提供 IDC 数据中心业务、云计算 IaaS 业务（弹性计算、云存储、云网络、云安全、管理与监控）、PaaS 业务及 SaaS 业务(开放云市场业务)运营和运行维护相关活动的信息安全管理活动。（信息安全适用性声明 1.0）

1.2 公司一体化管理体系覆盖的边界信息

注册地址：新疆维吾尔自治区乌鲁木齐市水磨沟区红光山路 1966 号

办公地址：新疆维吾尔自治区乌鲁木齐市水磨沟区红光山路 1966 号

组织范围：公司云能力服务中心（附录组织机构图）及相关员工。

活动场所：公司的经营管理活动及作业活动所涉及的办公场所、数据中心等。

其他与本公司生产经营管理有关的活动（包括计划的和正在实施的），以及公司可以控制的或在公司影响范围内的可能影响公司一体化管理绩效的活动及所涉及的人员和场所。

1.3 管理体系标准的适用性

本手册及相应的管理体系文件涵盖了 GB/T22080-2016、ISO/IEC20000-1:2018 标准的全部要求。

1.4 一体化管理手册的适用性

本手册适用于公司依据信息技术服务和信息安全等管理体系标准建立的信息技术服务和信息安全一体化管理体系（IMS）。

本手册也适用于第二方或第三方审核本公司信息技术服务、信息安全管理能力的依据之一。

2 规范性引用文件

公司一体化管理体系建立、实施和改进主要依据以下标准和要求：

ISO/IEC 20000-1：2018《信息技术 服务管理 第 1 部分 服务管理体系 要求》；

GB/T22080-2016/ISO/IEC 27001:2013《信息技术 安全技术 信息安全管理体系 要求》；

公司的一体化管理活动，除应满足以上管理体系标准的要求外，还应符合国家、行业现行有关法律法规要求的规定。

3 术语和定义

3.1

本手册及相应的管理体系文件在充分理解相关管理体系标准所规定的术语和定义的基础上，优先使用本公司生产经营活动所涉及的行业术语和本公司的习惯用语。

3.2

本手册及相应的管理体系文件中的“归口管理”是指公司管理层或部门对某一方面的活动制定政

策、对活动情况进行监督检查，并进行联络和协调。

3.3

以下简称用于本手册和本公司其他一体化管理体系文件：

公司、本公司：中国移动通信集团新疆有限公司的简称、自称。

信息技术服务和信息安全一体化管理体系：公司依据 GB/T22080 和 ISO/IEC 20000-1 等标准建立的整合型管理体系。

一体化管理体系/管理体系：公司建立的信息技术服务和信息安全一体化管理体系的简称。

IMS（Integrated Management System）：本公司一体化管理体系的英文简称。

IT-SMS（IT Service Management System）：信息技术服务管理体系的英文简称。

ISMS（Information Security Management System）：信息安全管理体系的英文简称。

4 组织环境

4.1 理解组织及其环境

4.1.0 职责

1、总经理和管理层依据所面临的组织环境进行经营决策。

2、管理者代表依据所面临的组织环境对一体化管理体系进行策划、调整。

3、公司各级管理人员及各部门监视其职责范围内的组织环境信息。

4、安全运营管理室组织、协调各部门对组织环境进行识别、监视和评审。

4.1.1 组织环境包括外部市场经营环境和公司内部经营条件。组织环境一般包括如下内容：

1、市场经营环境（外部因素）：与公司生产经营活动有关的政治、经济因素、社会因素、技术因素、市场因素和自然因素等。

2、公司经营条件（内部因素）：影响公司经营的企业战略、文化与运营模式、资源状况、技术能力、施工能力、市场管理能力等。

4.1.2 公司管理层依据所面临的组织环境策划一体化管理体系、并进行经营决策。组织环境的分析结果为以下事项提供依据：

1、确定或调整一体化管理体系的范围、策划和建立一体化管理体系；

2、识别组织环境中可能存在的风险和机遇、确定应对措施；

3、制定发展战略、确定方针、目标；

4、进行经营决策；

5、管理评审；

6、市场调查与预测、市场开发等。

4.1.3 公司各级管理人员及各部门监视其职责范围内的组织环境信息，当组织环境发生较大变化时应及时向主管领导汇报或及时提交会议进行讨论。

4.1.4 在公司调整发展战略、举办管理评审及组织环境发生重大变化时，总经理应组织召开会议对公司所面临的组织环境进行讨论分析，必要时制定相应措施、确保与内外部环境相适应。

4.2 理解相关方的需求和期望

4.2.0 职责

1、公司管理层及各部门持续关注相关方需求的变化，采取措施理解、满足相关方的需求和期望。

2、安全运营管理室组织、协调各部门对相关方的需求和期望进行识别、监视和评审。

4.2.1 公司秉承“共生”的企业理念，与相关方进行广泛交流与沟通，促进公司可持续发展。识别相关方需求和期望的工作步骤和内容包括：

1、识别相关方；

2、客观认识相关方需求，并采用可行的方式回应他们的关注；

3、承认相关方在关注公司一体化管理体系方面的利益和合法权利；

4、认识到某些相关方能对公司的一体化管理产生重大影响；

5、评估并考虑相关方接触、参与以及影响本公司的相应能力。

4.2.2 公司相关方包括：股东、员工、业主、供方、勘察、设计、施工方、合作伙伴、政府主管部门、社区等。相关方对公司经营管理产生不同的影响，公司需分层次考虑不同的相关方的需求，公司依据以下情况，确定相关方的关注程度：

1、相关方可能对公司经营绩效或决策产生的影响；

2、相关方带来风险和机遇的能力；

3、相关方可能对业务开展产生的影响或冲击；

4、相关方决策或活动对公司经营管理的影响能力。

4.2.3 公司管理层组织各部门持续关注相关方需求，采取措施理解、满足相关方的需求和期望。各部门对相关方需求和期望进行识别、获取、分析，协商解决相关方关注的问题。

4.2.4 必须遵守的要求包括：

1、法律法规标准，监管机构、行政机关的要求；

2、服务要求，如服务级别目标、信息安全性或可用性要求等；

3、合同义务，包括对客户、供应商、合作伙伴的合同义务。

4.3 确定管理体系的范围

4.3.0 职责

管理者代表对管理体系进行策划，明确管理体系的边界和适用性，并确定范围。

4.3.1 公司在策划一体化管理体系时，应依据以下内容确定管理体系的范围：

1、公司面临的组织环境；

2、相关方的需求和期望；

3、必需履行的合规义务；

4、公司经营服务范围及所涉及行业的特点；

5、公司交付的服务；

6、公司各过程、生产经营活动之间，以及与其他组织之间的接口和依赖关系。

4.4 管理体系及其过程

4.4.0 职责

总经理授权管理者代表按照相关标准的要求，建立、实施、保持和持续改进一体化管理体系。

4.4.1 公司按照相关管理体系标准（条款 2）的要求、采用过程方法确定一体化管理体系的过程及各过程的相关要求，并根据行业的特点，制定目标、明确职责，确定公司产品和服务实现过程（过程

示意图见附录），配置必须的资源、并建立必要的成文信息支持各管理过程的运行和项目的实施，保留过程运行记录证实所有过程按照要求实施。公司通过监视、测量、分析和评价，发现问题并采取措施、改进过程或管理体系。

4.4.2 公司采用过程方法，确定一体化管理体系各过程的如下内容：

1、过程的输入和输出；

2、过程的顺序和过程之间的相互作用；

3、过程的顾客与利益相关方（包括内部顾客，即下一过程的接收者）及其要求；

4、过程运行的准则和方法（包括检查、检测、测量和相关绩效指标等）；

5、过程运作中潜在的风险和机遇及其应对措施；

6、过程所需的资源、过程的职责和权限。

4.4.3 公司对外包过程进行识别并加以控制，依据外包过程影响公司产品和服务的重要程度以及双方在外包过程中所承担的责任，对承包商进行调查、评价，确定控制类型和程度并采取适当的控制措施，确保产品和服务提供过程及成果满足要求。本公司外包过程主要为数据中心机房的运维服务。

4.4.4 从实现公司整体战略目标出发，以及经营管理集成化的实施需求，总经理及管理者代表在策划信息技术服务和信息安全一体化管理体系时，应考虑经营管理、社会责任、成本控制等与一体化管理体系进行系统融合。

5 领导作用

5.1 领导作用和承诺

5.1.0 职责

1、总经理是公司一体化管理体系的最高管理者，推动管理体系的整合，并承担一体化管理的最终责任。

2、管理者代表组织、协调公司管理体系的相关活动，承担公司一体化管理体系建设的直接责任。

3、公司各级领导落实管理职责，在一体化管理体系实施、保持和改进过程中发挥领导作用。

5.1.1 领导作用是一体化管理体系建立、实施、检查和改进的基本必要条件。总经理应：

1、指挥和控制一体化管理体系的策划，承担一体化管理的最终责任；

2、确定组织架构和职责，建立合理的机制，确保各级管理者和员工在管理体系运行中发挥作用；

3、制定与组织环境相适应、与战略方向相一致的管理方针、管理目标，以及确保方针目标实现的管理方案、服务管理计划和信息安全策略等；

4、确保管理体系标准要求融入公司的业务过程；

5、确保提供一体化管理体系所需的资源；

6、建立沟通机制、消除障碍，传达一体化管理的重要性；

7、授权管理者代表按照管理体系标准的要求，建立、实施、保持和持续改进一体化管理体系。

8、确保一体化管理体系实现其预期结果，推动持续改进，提高一体化管理绩效。

5.1.2 公司各级领导带头遵守法律法规要求、做出明确具体的一体化承诺、通过落实管理职责，以身作则、在各项工作和活动中使员工感受到自己对一体化管理的重视和态度，产生引领示范的作用。

5.2 方针

5.2.0 职责

1、总经理组织制定、批准管理方针，并确保方针在公司内部得到宣传和贯彻。

2、安全运营管理室负责初步拟定管理方针，并负责管理方针的宣传、贯彻、实施。

5.2.1 制定管理方针

5.2.1.1 公司根据法律法规要求，考虑顾客、相关方、员工的需求，结合公司的战略和管理现状，制定一体化管理方针。公司管理方针应符合以下要求：

1、符合公司的组织环境、行业特点和经营管理需要；

2、为公司信息技术服务、信息安全目标的制定提供框架；

3、包括对适用的信息技术服务、信息安全要求的承诺；

4、持续改进一体化管理体系的承诺。

5.2.1.2 总经理组织制定管理方针，为管理目标的制定提供框架，通过管理目标的支撑来实现管理方针，并定期对管理方针进行评审。

5.2.1.3 管理方针的制定应得到员工广泛的参与和认同。

5.2.2 沟通管理方针

管理方针的沟通应满足以下要求：

1、管理方针由总经理签署发布，并通过管理手册、宣传手册或在宣传标语中表述。

2、公司通过会议、培训、宣传等方式使全体员工准确理解方针的含义并在工作中贯彻落实。

3、公司通过招投标活动或文字声明等方式，向相关方说明公司的管理方针，表明公司一体化管理的决心和态度，展示公司形象。

5.3 组织的岗位、职责和权限

5.3.0 职责

1、总经理负责完善的组织机构，明确各部门的作用、责任和权限。确保体系符合相关标准的要求。

2、解决方案室汇总编制部门/岗位职责。

3、管理者代表负责向最高管理者报告体系和服务的绩效。

5.3.1 公司建立与公司业务范围和经营规模相适应的组织管理机构，公司组织机构层级包括：

1、总经理。

2、管理者代表及管理层等。

3、公司相关职能部门。

5.3.2 公司管理层和相关职能部门应对公司产品和服务实施有效的管理，检查、技术支持，并定期进行工作成效的考核。

5.3.3 公司依据经营管理实际情况，在满足国家法律法规要求的前提下，确定各部门、岗位的作用、职责和权限，相关要求如下：

1、公司确保岗位、职责和权限的制订，并通过会议、文件传阅和培训等方式确保全体人员对其职责、权限的了解和理解，让员工都清楚自己岗位的职责与权限，并自觉履行职责。

2、各部门和全体人员，承担其工作内容相应的部门和岗位责任，贯彻执行公司一体化管理体系的规定和要求，做好职责范围内相关的工作。

3、公司建立责任考核机制，对各级管理人员及员工职责履行情况进行定期考核。

4、公司组织机构或岗位设置发生变化时，需同时对职能、职责及有关制度作相应调整，保证公司部门的管理职能和岗位的工作职责的完整性、连续性。

6 策划

6.1 应对风险和机遇的措施

6.1.1 总则

6.1.1.0 职责

总经理组织管理层对应对风险和机遇的措施进行策划，明确风险和机遇的分类和管理要求。

6.1.1.1 公司考虑组织环境和相关方需求，确定需要应对的风险和机遇。根据公司经营管理实际，将风险和机遇分为：

1、经营风险与信息技术服务风险（6.1.2）；

2、信息安全风险（6.1.3）；

6.1.1.2 公司制定相应的控制过程分别对经营风险（包括信息技术服务风险）、信息安全风险、合规风险等进行控制，策划相应的应对措施，并在过程中及其他业务过程中融入并实施这些措施，进而消除、规避或减少风险所造成的负面影响，确保一体化管理体系实现预期结果。

6.1.1.3 应对风险和机遇措施的策划应与变更的策划（6.3）结合，并考虑变更带来的风险。

6.1.1.4 风险控制措施应与可能产生的后果的严重程度相适应，并考虑技术、财务和实施的要求及限制。公司通过监视、测量、分析和评价活动定期分析和评价措施的可行性和有效性，必要时对控制措施进行调整。

6.1.2 经营风险与信息技术服务风险

6.1.2.0 职责

1、安全运营管理室归口经营风险管理，负责协调公司经营风险的管理工作。

2、平台运维室负责公司产品服务管理风险控制工作的组织、协调。

6.1.2.1 经营风险指未来的不确定性对企业实现其经营目标的影响。经营风险一般可分为战略风险、财务风险、市场风险、运营风险、法律风险等，包括公司信息技术服务的服务风险；也可以能否为公司带来盈利等机会为标志，将风险分为纯粹风险（只有带来损失一种可能性）和机遇（带来损失和盈利的可能性并存）。

6.1.2.2 公司风险管理工作应与其他管理工作紧密结合，把风险管理的各项要求融入企业管理和业务流程中。策划管理体系及其过程时，应组织各部门识别各过程以及信息技术服务过程中可能存在的风险，并针对性地确定控制过程和制定控制要求。

6.1.2.3 风险信息报告是加强风险管理的重要举措，根据公司风险管理工作的有关要求，按照“早发现、早预警、早处置”的原则，公司各部门应及时获取、识别本部门职责范围内的风险信息，通过报告、提交公司会议讨论等形式对风险信息进行讨论。

6.1.2.4 公司结合办公例会与管理评审等活动，采用会议讨论、专家咨询、案例比较等风险评估方法，定期开展经营风险与服务风险评估。在组织环境发生重大变化以及需要对重大事项进行决策时，应增加风险评估的频率。

6.1.2.5 风险评估应综合考虑风险发生的可能性、风险发生后可能造成的影响程度以及可能持续的时间，采取适当风险控制策略（包括：风险规避、风险降低、风险分担、风险承受），确保消除、降低或减缓风险，充分利用可能的发展机遇，保证实现企业效益和管理体系预期结果。

6.1.3 信息安全风险评估与处置

6.1.3.0 职责

安全运营管理室统筹协调公司信息安全风险管理工作，对各部门信息安全风险管理情况进行监督检查。

6.1.3.1 信息安全风险即对信息安全目标的不确定性影响，公司制订并维护信息安全风险策略，识别、分析、评价信息安全风险,并进行信息安全风险处置，确保信息安全风险为风险所有者所知悉，并被处置至可接受的水平。

6.1.3.2 信息安全风险评估即信息安全风险的识别、分析和评价。公司建立的信息安全风险评估过程包括：

1、确定信息安全风险准则，包括：信息安全风险定义与范围、风险接受准则和信息安全风险评估的实施准则；信息安全风险准则的制定，应能保证重复的信息安全风险评估产生一致的、有效的和可比较的结果。

2、识别信息安全风险及风险责任人，尤其是识别公司确定的信息安全管理体系(ISMS)覆盖范围内的、与信息的机密性、完整性和可用性损失相关的风险。

3、分析信息安全风险，评估风险发生的可能性及可能导致的后果、并确定风险等级。

4、根据风险分析结果、评价信息安全风险、确定风险等级。

6.1.3.3 公司根据信息安全风险评估结果，选择风险处置选项、确定适当的控制去实施这些选项、制定风险处置计划，对信息安全风险进行处置，并保留相应的文件化信息。

6.1.3.4 公司对信息安全适用性进行声明，声明所列的控制目标和控制措施直接源于 ISO/IEC 27001 标准的要求，以保证公司信息安全管理体系(ISMS)的有效性及适用性。

6.2 目标及其实现的策划

6.2.0 职责

1、总经理负责目标管理的领导工作，组织制定公司管理目标，批准目标及其实施计划和方案。

2、安全运营管理室负责组织一体化管理目标的分解、贯彻实施和相关考核工作。

6.2.1 管理目标的制定

6.2.1.1 为实现公司的管理方针，总经理依据管理方针提供的框架和公司的发展战略，组织制定管理目标。

6.2.1.2 管理目标的制定原则：

1、与管理方针一致；

2、可测量，具体明确、追求改进；

3、考虑信息安全及适用法律法规和其他要求，考虑风险评估和风险处置的结果；

6.2.1.3 管理目标包括信息技术服务目标和信息安全目标。公司每年依据战略目标和经营目标，结合上一年度目标完成情况制定年度管理目标，并在在组织内外部得到沟通。

6.2.2 目标实现的策划

为确保公司目标、指标的实现，应制定目标实施计划（管理方案），并明确以下要求：

1、目标、指标以及实施的措施及方法。

2、所需的资源(经费等)配置内容。

3、完成的时间和进度要求。

4、检查、考核的要求以及实施检查/考核的部门或检查/考核者。

6.3 策划服务管理体系

为确保公司一体化管理体系中信息技术服务管理体系(IT-SMS)的有效性和适宜性，公司应建立、实施和维护服务管理计划，并确保公司其他策划活动与服务管理计划保持一致。服务管理计划包含以下内容：

1、服务清单；

2、可能影响 IT-SMS 和服务的已知限制；

3、义务（如策略、标准、法律、法规或合同要求）及其适用于 IT-SMS 和服务的程度；

4、IT-SMS 和服务的职责和权限；

5、IT-SMS 和服务所需人员、技术、信息和财务资源；

6、与服务生命周期内其他参与方合作时应采取的方法；

7、用于支持 IT-SMS 的技术；

8、如何测量、审核、报告和改进 IT-SMS 和服务有效性的方法。

7 支持

7.1 资源

7.1.1 职责

1、总经理确保一体化管理体系有效运行的相关资源的提供。

2、管理者代表统筹协调资源配置工作，为管理体系的有效运行提供必要的资源。

7.1.1.1 公司为管理体系的运行提供必要的资源，这些资源包括：生产条件、财务资源、人力资源、基础设施、工作环境、技术资源、信息资源等。资源的配置应符合以下要求：

1、满足国家、行业法律法规要求。依法取得和保持相关资质或行业许可，接受各级管理部门的监督，并在能力范围内承揽业务。

2、考虑各级管理者、员工及相关方的需求，符合公司性质、规模、发展规划的需要，并保障一体化管理的资源投入，确保一体化管理体系有效运行。

3、满足产品和服务实施的需要，和预防污染、节能降耗、安全生产、信息安全控制的需要。

4、能够为员工的技能提升、个人发展和公司的团队建设、企业文化培育等投入资源。

5、通过分析与评价、管理评审，定期评审资源的适宜性。

7.1.1.2 由于受到企业规模、资源基础等的限制，公司应考虑现有内部资源的能力和局限性。为了确保满足管理体系运行的需求，公司通常还需要从外部供方获得资源，例如：外聘人员、运维服务等。外部资源的管理需要通过对供方实施有效管理来进行管控。

7.2 能力

7.2.0 职责

安全运营管理室负责公司教育培训工作的组织实施和公司人员的考核、能力评价。

7.2.1 公司基于各岗位的职责权限或工作内容，确定相关人员必备的能力要求。人员能力的管理应涵盖公司全体员工及临时聘用人员等，公司应保留相应记录作为人员能力的证据，如教育、培训和经验等方面的记录、面试记录、工作绩效考核有关的记录等。

7.2.2 公司所制定的人员能力要求（岗位任职条件）必要符合公司经营管理需要和法律法规的要求，包括学历、从业资格、工作经历、知识要求、技能要求及其他关键素质要求等。

7.2.3 公司从外部环境的需要（如法律法规要求）和内部条件的现状（人员能力、管理现状等）识别培训需求，制定员工培训计划。培训计划应对培训对象、内容、方式及时间做出安排，并从以下三个方面评价培训的有效性：

1、培训计划是否完成，是否满足需求；

2、培训后通过测验、考试、抽查等方式评价培训效果；

3、在培训后的实际工作中考察接受培训的人员是否提升了能力水平，胜任了岗位要求。

7.2.4 公司定期对公司人员实施考核，对达不到岗位能力要求的人员，采取相应的培训、转岗、淘汰等措施。

7.3 意识

7.3.0 职责

安全运营管理室组织各部门开展培训、宣传活动，引导员工的行为和态度。

7.3.1 公司通过沟通、培训和组织多种形式的企业文化活动，引导员工的行为和态度，确保员工：

1、提高一体化管理意识，使员工知晓公司的管理方针和管理目标。

2、知晓公司的管理方针和管理目标；

3、充分认识到所从事工作对公司一体化管理的重要性；

4、清楚不符合管理体系要求带来的影响。

7.4 沟通

7.4.0 职责

1、总经理及管理者代表统筹协调公司相关方沟通管理，并组织、落实员工参与和协商等活动。

2、安全运营管理室负责公司会议管理和文件信息的接收、传递与处理。

3、各部门负责本部门职能范围内的内、外部信息交流与沟通和本部门内的信息反馈、传达，并按规定落实有关信息的处理措施。

7.4.1 总则

公司确定与管理体系相关的内部和外部沟通，建立相关方沟通机制，明确沟通“五要素”，即：内容、时机、对象、方式和人员，采用可行的方式与相关方进行沟通和交流。

7.4.2 沟通的分类与要求

7.4.2.1 根据沟通对象不同，沟通包括：

1、内部沟通：包括公司内部的上下级之间的纵向沟通或各部门之间的横向沟通。

2、外部沟通：与外部相关方的沟通，沟通过程中需识别公司必须遵守的法律法规要求。

7.4.2.2 根据沟通的意愿，沟通包括：

1、主动沟通：沟通涉及各管理过程和项目实施过程，各管理程序和规章制度应对各过程输入、输出以及管理活动过程中有需要协调、协商的事项作出相应规定，公司定期组织办公会议以及部门例会等方式，就工作事项与存在问题进行分析、讨论，并提出相应的对策，对取得的成绩进行表扬、鼓励。

2、被动沟通：应特别重视不合格、不符合，质量、环境、安全事故、事件，相关方抱怨、投诉等沟通处理。

7.5 成文信息

7.5.0 职责

安全运营管理室负责公司文件和记录的管理和管理手册、程序文件的编制、修订工作。

7.5.1 总则

公司建立、完善与各项一体化管理活动相关的文件和记录。公司文件和记录包括手册、程序文件、管理制度、作业文件和记录表格、合同、图表等。

7.5.2 创建和更新

文件和记录的编制和修订遵循规定的格式，并经过评审和批准后以电子版或纸质版的形式向各、员工发布。批准后的文件应采用清晰的文件标识（受控、非受控、现行、作废）和说明（如：标题、日期、发文部门、文件编号等）。

7.5.3 成文信息的控制

公司明确文件和记录管理过程，规定文件编制、审批、发布、更改、回收、评审与修订、归档和记录填写、标识、收集、保管、检索、保存期限和处置要求。成文信息管理应符合下列规定：

1、成文信息需进行会签，听取相关部门的意见，确保制度的适宜性，并经审批后方可发布。

2、应根据法律法规的变化、公司发展的需求定期对文件进行评审，必要时修订并重新审批；

3、应识别并获取相关法律法规标准及其他外来文件，外来文件经识别后纳入公司文件管理；

4、应确保在使用场所获得所需文件的适用版本；

5、应建立公司文件制度清单，并明确查询路径；

6、应保证向员工提供作业活动所依据的文件；

7、应将作废文件撤出使用场所或加以标识。

7.5.4 服务管理体系文档管理

服务管理体系的文档信息应包括：

1、服务管理体系范围；

2、服务管理方针和目标；

3、服务管理计划；

4、变更管理方针、信息阿沁方针和服务连续性计划；

5、组织服务管理体系过程；

6、服务要求；

7、服务目录；

8、服务级别协议；

9、与外部供应商签订的合同；

10、与内部供应商或作为供应商的客户签订的协议；

11、服务管理体系标准要求的程序

12、证明符合服务管理体系标准和公司服务管理体系要求所需的记录。

7.6 知识

7.6.0 职责

安全运营管理室负责统筹协调和组织公司知识管理工作的开展。

7.1.6.1 公司获取有利于产品实施和经营管理活动开展的知识，并进行分享、应用和创新，公司通过知识的应用不断提高管理水平。

7.1.6.2 知识管理围绕人员、过程、技术和信息四个要素进行管控。知识包括：

1、与人有关的经验诀窍、口口相传的知识和经验；

2、与过程相关的经营和工程施工过程中的积累、成功案例、事故教训；

3、与技术有关的专利技术、科研成果、典型质量问题等。

7.1.6.3 公司通过经验分享、工作总结、会议讨论、培训学习等方式和活动，将各类最佳做法（知识，经验）进行识别、汇总，形成记录、文件或对相应的文件进行修订，并通过知识的保存和分享防止由于人员更换或分享不畅而导致的知识流失。

7.1.6.4 公司建立监理知识库和案例库，以保证公司内共享所积累的监理技术知识和信息。

7.1.6.5 公司领导和全体员工都应参加经验分享、学习、培训，参与沟通、交流，获取经营、管理、技术、操作等各方面的知识。公司做好知识的传承与保密界定工作，确保在人员脱离本岗位后公司的知识不会受到遗失与泄密。

8 运行

8.1 服务运行的策划和控制

8.1.1 运行的规划和控制

平台运维室负责信息技术服务的运行控制。

为确保信息技术服务管理体系有效实施，本公司开展以下活动：

1、公司应针对满足信息技术服务要求及实施确定的控制措施制定相关的程序和规则制度，所需的过程予以策划、实施和控制。也应实施计划以实现确定的信息技术服务目标；

2、公司应保持与信息技术服务管理体系运行过程中的各种信息数据，以确保信息技术服务管理体系是否按照计划有效运行；

3、当与信息技术服务方针、目标、工作计划和程序、控制措施等发生变更时，应进行管理，计划的变更应按照计划进行控制，非预期的变更要评审变更的影响，确保变更皆有负面的影响，必要时采取措施减轻负面影响；

8.1.2 服务组合

8.1.2.1 服务交付

各相关部门应按照手册运行服务管理体系，确保协作活动和资源，应执行服务所需要的活动。服

务组合通常管理服务生命周期中的所有服务，包括提议的，开发中的，服务目录中的在线服务和即将停止的服务。服务组合管理确保服务提供者有正确的服务构成，服务组合管理活动中包括服务策划，控制服务生命周期的相关方，服务目录管理，资产管理和配置管理。

8.1.2.2 策划服务

应确定和记录现有服务、新服务和服务变更的要求。根据公司、客户、用户和其他相关的需求确定服务的紧急程度。公司确定和管理服务之间的依赖性和重复性。根据需要提出变更，以便服务与服务管理方针、服务管理目标和服务要求保持一致。同时考虑已知的限制和风险。优先考虑服务变更请求或变更服务的提议，以在考虑可用资源的情况下与业务需求和服务管理目标保持一致。

8.1.2.3 服务生命周期内各参与方的控制

1、公司对服务管理体系标准的要求和交付的服务负责。

2、公司确定评价和选择服务生命周期内其他参与方的准则，并实施选择和评价，并形成以下文件：

——其他方提供或运行的服务；

——其他方提供或运行的服务组件；

——其他方运行的公司服务管理体系范围内的过程或部分过程；

3、集成公司自身或其他方提供和运行的服务管理体系范围内的服务、服务组件和过程，以满足服务要求。公司协调与服务生命周期内其他参与方的活动，包括服务策划、设计、转换、交付和改进服务。

4、公司对其他各方过程绩效进行测量测量和评价。

8.1.2.4 服务目录管理

应创建并维护服务目录。服务目录包括公司、客户、用户和其他相关方的信息，以描述服务，服务的预期结果和服务之间的依从关系。服务目录应允许客户、用户和其他相关方访问服务目录的有关部分。

8.1.2.5 资产管理

公司对交付服务的资产进行管理，以满足服务要求个和规定的义务。当资产也是配置项时，见配置管理要求。

8.1.2.6 配置管理

1、定义配置项的类型。应将服务归类为配置项。

2、按服务的紧急程度和类型适当的细节级别记录配置信息。应控制对配置信息的访问。每个配置项的配置信息应包括：

——唯一标识；

——配置项类型；

——配置项描述；

——与其他配置项的关系；

——状态。

3、对配置项实施控制。配置项的变更应可追溯、可审计，以保持配置信息的完整性。配置项变更部署后，应更新配置信息。

4、按策划的时间间隔验证配置信息的准确性。如果发现缺陷，公司采取必要的措施。

5、适当时，应将配置信息用于其他服务管理活动。

8.1.3 关系与协议

8.1.3.1 总则

公司可以使用供应商完成以下工作：

1、提供或运行服务；

2、提供或运行服务组件；

3、运行公司服务管理体系范围内的过程或部分过程。

8.1.3.2 业务关系管理

1、公司识别并记录服务的客户、用户和其他相关方。公司指定专人负责管理客户关系和维护顾客满意度。

2、公司建立与客户和其他相关方沟通的机制。沟通机制应促进对服务运行的业务环境和新的或变更的服务要求的理解，并使公司能够对新的或变更的服务要求做出响应。

3、公司按计划的时间间隔评审服务的绩效趋势和服务的结果。

4、公司按计划的时间间隔，根据客户的代表性样本测量对服务的满意度。公司对测量结果进行分析和评审，识别改进机会并报告顾客满足度。

5、公司当记录服务投诉，管理客户的服务投诉，调查和采取措施直至投诉关闭，报告服务投诉。当服务投诉无法通过正常渠道解决时，应向顾客提供投诉升级渠道。

8.1.3.3 服务级别管理

1、公司和客户应就交付的服务达成一致。对于交付的各项服务，公司根据成文的服务要求建立一个或多个服务级别协议。服务级别协议应包括服务级别目标、工作量限值和期望。

2、公司按计划的时间间隔监视、评审并报告：

——服务级别目标的完成情况；

——与级别协议规定的工作量限值相比较，工作量的实际和周期性变化。

3、如果服务级别目标未达成的，公司识别改进机会。

8.1.3.4 供应商管理

1、外部供应商管理

公司指定专人负责管理与外部供应商的关系、合同和绩效。

公司和每一个外部供应商签订书面合同。合同应包含：

——外部供应商提供或运行的服务、服务组件、过程或部分过程；

——外部供应商应满足的要求；

——服务级别目标或其他合同义务；

——公司对外部供应商的权限和责任。

公司与客户共同评价外部供应商服务级别目标或其他合同义务与服务级别协议的一致性，并管理已识别出的风险。

公司定义和管理与外部供应商的接口。

公司按计划的时间间隔监视外部供应商的绩效。如果服务级别目标未达成或其他合同义务未履行的，公司确保识别改进机会。

公司按计划的时间间隔，根据当前服务的要求评审合同。在批准变更前，应针对确定的合同变更评价其对服务管理体系和服务的影响。

公司记录并管理公司与外部供应商间的争议，直至争议关闭。

2、管理内部供应商或作为供应商的客户

对于每个内部供应商或作为供应商的客户，公司制定、达成并维护书面协议，以定义服务级别目标、其他承诺、各方的活动和接口。

公司按计划的时间间隔监视内部供应商或作为供应商的客户的绩效。如果服务级别目标未达成或其他约定义务未履行的，公司确保识别改进机会。

8.1.4 供给与需求

8.1.4.1 服务的预算与核算

公司根据其财务管理策略和流程对服务或服务组进行预算和核算。

应编制成本预算，以便对服务进行有效的财务控制和决策。

公司按计划的时间间隔，根据预算监控并报告实际成本，评审财务预测并管理成本支出。

8.1.4.2 需求管理

公司按计划的时间间隔：

1、确定目前和未来的服务需求；

2、监视并报告服务的需求和使用量。

需求管理用于理解客户现在和未来的服务的需求。能力管理与需求管理共同作用于提供满足需求的充足的能力。

8.1.4.3 能力管理

1、公司考虑服务和绩效要求，确定人员、技术、信息和财务资源的能力要求，形成文件，予以维护。

2、公司制定能力计划，包括：

——根据服务需求得出的当前和未来的能力；

——约定的服务级别目标、服务可用性和服务连续性要求对能力的影响；

——服务能力升级的时间段和阈值。

3、公司提供足够的能力，来满足约定的能力和绩效要求。公司监视能力使用情况，分析能力和绩效数据，识别改进绩效的机会。

8.1.5 服务设计、创建和转换

8.1.5.1 变更管理

1、变更管理方针

公司制定变更管理方针并形成文件，定义以下内容：

——纳入变更管理控制的服务组件和其他项目；

——变更类型，（包括紧急变更）以及管理变更的方法；

——对客户或服务有潜在重大影响的变更的判定准则。

2、变更管理启动

应对所有变更请求实施记录和分类，包括增加、撤销或转换服务的提议。

公司使用服务设计和转换以实施以下活动：

——依照变更管理方针确定的可能对顾客或其他服务造成重大影响的新服务；

——对依照变更管理方针确定的可能对客户或其他服务造成重大影响的服务变更；

——根据变更管理方针，由服务的设计和转换管理的变更类别；

——撤销某一服务；

——公司将现有服务转让给客户或其他方；

——客户或其他方将现有服务转让给公司。

应通过变更管理活动管理范围内的新的或变更的服务的评估、批准、计划和评审。

3、变更管理活动

公司和相关方应就变更请求是否批准和变更优先顺序做出决策。决策时应考虑风险、商业利益、可行性和财务影响，还应考虑变更对以下各项的潜在影响：

——现有服务；

——客户、用户和其他相关方；

——本标准要求的策略和计划；

——能力、服务可用性、服务连续性和信息安全；

——其他变更请求、发布和部署计划。

应对批准的变更进行准备、验证并尽可能进行测试。应向相关方通知已批准变更的拟部署日期及部署详情。

应策划回退或补救不成功变更所需的活动，可能的话，进行测试，如果变更失败，应进行变更回退或补救。失败的变更应被调查并采取商定的措施。

在部署对配置项的更改后，应更新配置信息。

公司评审变更的有效性，并采取与相关方商定的措施。

应按计划的时间间隔分析变更请求记录以发现相关趋势。应记录并评审分析结果和结论，识别改进机会。

8.1.5.2 服务设计和转换

1、策划新的或变更的服务

策划时，应使用确定的新的或变更的服务要求，并包含括：

——设计、开发和转换活动的权限和职责；

——公司或其他方按时间表开展的活动;

——人员、技术、信息和财务资源；

——对其他服务的依赖；

——新服务或变更服务所需的测试；

——服务验收准则；

——以可测量指标表示交付的新服务或变更服务的预期结果；

——对服务管理体系、其他服务、计划变更、客户、用户和其他相关方的影响。

针对将要撤销的服务，策划还应包括服务撤销日期及数据、文档信息和服务组件的存档、处置或传送活动。

针对将要转让的服务，策划还应包括服务转让日期及数据、文档信息、知识和服务组件的存档、处置或传送活动。

应通过配置管理对受新服务或变更服务影响的配置项实施管理。

2、设计

应设计新服务或变更服务并形成文件，满足第 8.2.2 条确定的服务要求。设计应包括以下方面的项目：

——交付新服务或变更服务的各参与方的权限和职责；

——变更人员、技术、信息和财务资源的要求；

——对适当的教育、培训和经验的要求；

——新服务或变更服务级别协议、合同和为服务提供支持的其他成文协议；

——对服务管理体系的变更，包括新的或变更的策略、计划、过程、程序、措施和知识；

——对其他服务的影响；

——服务目录的更新。

3、创建和转换

公司开发并测试新服务或变更的服务，验证其是否满足服务要求，是否符合设计要求，是否达到商定的服务验收准则。如果未达到服务验收准则，公司和相关方应就必要的措施和部署作出决策。

应利用发布和部署管理将批准的新服务或变更的服务部署到运行环境中。

转换活动完成后，公司向相关方报告所取得的结果和与预期结果进行对比的结果。

8.1.5.3 发布和部署管理

公司定义发布的类型（包括紧急发布）、发布频率和管理发布的方法。

公司与顾客和相关方对新服务和变更的服务和服务组件部署到运行环境中进行策划。策划应与变更管理过程协调，并包含相关方的变更请求、已知错误和通过该发布所关闭问题的引用。策划应包括各项发布的部署日期、交付方式和部署方法。

应对照书面的验收准则对发布的内容实施验证，并应在部署前获得批准。未达到验收准则的，公司和相关方应就必要的措施和部署作出决策。

将一项发布部署到运行环境之前，应获取受影响的配置项的基线。

发布应部署到运行环境中，以维护服务和服务组件的完整性。

应监视和分析成功和失败的发布。测量内容应包括发布部署后一段时间内与发布有关的事件。应记录并评审分析结果和结论，识别改进机会。

适用时，应提供发布成败相关信息和未来发布日期，用于其他服务管理活动。

8.1.6 解决与实现

8.1.6.1 事件管理

对于事件，应采取以下措施：

——记录并分类；

——考虑到影响和紧急程度，分配优先顺序；

——必要时升级；

——解决；

——关闭。

应根据采取的措施更新事件记录。

公司确定识别重大事件的准则。重大事件应依照成文的程序进行分类和管理。应随时向最高管理层报告重大事件。公司分配管理每个重大事件的职责。事件解决后，应报告并评审重大事件，识别改进机会。

8.1.6.2 服务请求管理

对于服务请求，应采取以下措施：

——记录并分类；

——确定优先顺序；

——履行；

——关闭。

应根据采取的措施后应更新服务请求记录。

公司向服务请求实施人员发出履行服务请求的指示。

8.1.6.3 问题管理

公司分析事件数据和趋势以识别问题。公司分析根本原因，确定措施防止事件发生或再次发生。

对于问题，应采取以下措施：

——记录并分类；

——确定优先顺序；

——必要时升级；

——尽可能解决；

——关闭。

应根据采取的措施更新问题记录。解决问题所需的变更应根据变更管理策略进行管理。

如果识别了根源，但问题尚未彻底解决的，公司采取措施以减轻或消除问题对服务的影响。应记录已知错误。适用时，应为其他服务提供有关已知错误和问题解决的最新信息。

应按计划的时间间隔监视、评审和报告问题解决方案的有效性。

8.1.7 服务保证

8.1.7.1 服务可用性管理

公司按计划的时间间隔评估和记录服务可用性的风险。公司确定服务可用性要求和目标。商定服务可用性要求时应考虑相关业务要求、服务要求、服务级别协议和风险。

应记录和维护服务的可用性要求和目标。

应监视服务可用性，记录结果并与目标进行比较。并对非计划的不可用性进行调查，并采取必要措施。

8.1.7.2 服务可用性管理

服务连续性管理

公司按计划的时间间隔，评估和记录服务连续性的风险。公司确定服务连续性要求。商定服务连续性要求时应考虑相关业务要求、服务要求、服务级别协议和风险。

公司创建、实施并维护一个或多个服务连续性计划。服务连续性计划应包含以下内容：

——启动服务连续性的条件和职责；

——在发生重大服务缺失时执行的程序或引用的程序；

——服务连续性计划启用时的服务可用性目标；

——服务的恢复要求；

——恢复正常工作环境的程序。

当访问正常的服务位置被阻止时，应能访问到服务连续性计划和联系人名单。

应按计划的时间间隔，测试服务连续性计划并与服务连续性要求进行比较。在服务环境发生重大变更后，应重新测试服务连续性计划。并记录测试结果。每次测试和启用服务连续性计划后均应进行评审。如果发现缺陷，公司采取必要的措施并报告所采取的行动。

启用服务连续性计划时，公司报告原因、影响和恢复措施。

8.1.7.3 信息安全管理

应按计划的时间间隔评估服务管理体系和服务的信息安全风险并进行记录。应制定、实施和运行信息安全控制措施，落实信息安全方针，处理已确定的信息安全风险。应记录有关信息安全控制措施的决定。

公司商定并实施信息安全控制措施，处理与外部公司有关的信息安全风险。

公司监视并评审信息安全控制的有效性并采取必要措施。

对于信息安全事件，应采取以下措施：

——记录并分类；

——根据信息安全风险分配优先顺序；

——必要时升级；

——解决；

——关闭。

公司按类型、数量和对服务管理体系、服务和相关方的影响来分析信息安全事件。应报告并评审信息安全事件，识别改进机会。

8.2 信息安全运行控制

8.2.1 运行的规划和控制

安全运营管理室负责信息安全管理的运行控制。

8.7.1.1 为确保信息安全管理体系有效实施，对已识别的风险进行有效处理，本公司开展以下活动：

1、公司信息安全管理小组负责编制形成信息安全风险处理计划，以确定适当的管理措施、职责及安全保密控制措施的优先级，应特别注意公司外包过程的确定和控制；为实现已确定的安全保密目标、实施风险处理计划，明确各岗位的信息安全职责；

2、信息安全领导小组依据信息安全风险处置计划编制相应的控制措施，并要求各职能部门实施所选择的控制措施，以实现控制目标的要求；

3、安全运营管理室通过公司年度教育培训、各部门通过部门内部培训等方式组织相关人员进行信息安全培训教育，提高全员信息安全意识和能力；

4、信息安全管理小组成员负责完成信息安全管理体系运行时必须的任务；对信息安全管理体系的

运行情况和必要的改善措施向信息安全最高责任者报告。

5、各部门负责人作为本部门信息安全的主要责任人，信息安全内审员负责指导和监督本部门信息安全管理体系的运行与实施，并形成文件；全体员工都应按保密承诺的要求自觉履行信息安全义务。

6、各部门应按照《信息安全适用性声明》中规定的安全保密目标、控制措施（包括安全保密运行的各种控制程序）的要求实施信息安全控制措施。

7、信息安全管理小组应对满足信息安全要求及实施 6.1 中确定的措施所需的过程予以规划、实施和控制，同时应实施计划以实现 6.2 中确定的信息安全目标。

8、信息安全管理小组应保持文件化信息达到必要的程度，以确信过程按计划得到执行。

9、信息安全管理小组应控制计划内的变更并评审非预期变更的后果，必要时采取相应措施减轻负面影响。

10、各部门确定本部门业务过程中的外包活动，并对外包过程进行必要的控制。

8.7.1.2 本公司目前无外包过程。如后续信息安全管理范围内有外包过程则按照以下方面进行控制：

1、发生外包的项目部分过程需要外包时，需对外包方进行严格的评价和选择；

2、项目经理应在项目策划阶段识别所面临的信息安全风险，并在项目全过程中对信息安全风险进行实时监控和更新。

8.2.2 信息安全风险评估

公司按照信息安全风险评估的要求，每年定期或当重大变更提出或发生时，执行信息安全风险评估。每次风险评估的过程均需形成记录，并由信息安全管理小组保留每次风险评估的记录，如：风险评估报告、风险处理计划等。

8.2.3 信息安全风险处置

为确保信息安全管理体系有效实施，对已识别的风险进行有效处理，本公司开展以下活动：

1、形成信息安全风险处理计划，以确定适当的管理措施、职责及安全保密控制措施的优先级；

2、为实现已确定的安全保密目标、实施风险处理计划，明确各岗位的信息安全职责；

3、实施所选择的控制措施，以实现控制目标的要求；

4、进行信息安全培训，提高全员信息安全意识和能力；

5、对信息安全体系的运作进行管理；

6、对信息安全所需资源进行管理。

信息安全管理小组负责组织相关人员，定期检查风险处理计划的执行情况，并保留信息安全风险处置结果的文件化信息。

9 绩效评价

9.1 监视、测量、分析和评价

9.1.0 职责

管理者代表组织各部门对监视、测量、分析和评价过程进行策划。

9.1.1 公司策划并实施必要的监视、测量、分析和评价过程，编制、修订相关的文件制度，对监视、测量、分析和评价过程实施控制。监视、测量、分析和评价活动包括：

1、对经营管理活动、规章制度执行情况和各管理过程的实施情况的检查；

2、管理目标的考核；

3、采购物资的检验与验收；

4、运维服务质量的评定；

5、顾客满意度测量；

6、信息安全管理绩效的评定；

7、统计分析与管理绩效的评价；

8、内部审核；

9、管理评审；

10、外部检查、验收、评价活动等。

9.1.2 监视、测量、分析和评价过程的策划内容：

1、需要监视、测量、分析和评价的项目和内容；

2、监视、测量、分析和评价的方式。方式可以是：检验、检测、监测、监督、检查、审计、统计分析、审核、评审等。

3、监视、测量、分析和评价方法：如检查的方法和检查标准等；

4、时机和频次：如适宜的测量点、见证点、验收点的设置，检查的时机和次数；

5、职责和权限：确定责任部门或岗位，明确规定相应的职责和权限，包括人员的能力和资格。

6、需要填写和保存的记录：如顾客满意度调查记录、服务过程的检查记录、安全检查记录等。

9.1.3 监视、测量、分析和评价过程的策划，应充分考虑并确定包括统计技术在内的适用方法及其应用程度，采用现代信息技术和手段，提升一体化管理的有效性和效率。

9.2 内部审核

9.2.0 职责

1、管理者代表负责内部审核的领导工作，向总经理报告管理体系运行情况。

2、安全运营管理室负责内部审核的策划、组织实施与协调。

3、审核组长带领内审员根据审核计划实施审核。

9.2.1 为验证一体化管理活动和有关结果是否符合规定的要求、一体化管理体系的运行是否有效，公司应对内部审核活动进行策划、按照策划的时间间隔进行内部审核。

9.2.2 公司应每年至少进行 1 次覆盖全要素、全公司所有部门的审核，两次审核间隔不超过 12 个月，确保一体化管理体系规范运行。内部审核可采用集中式审核、滚动式审核等方式开展，也可根据需要进行专项审核，并可与常规的检查、考核等工作相结合。

9.2.3 审核组按照批准的审核计划对各部门进行审核，各部门及时对审核发现的问题采取纠正措施，并进行跟踪验证，确保问题的产生原因得到彻底消除。

9.2.4 审核完成后，应形成审核报告，经总经理审批后，形成文件，并按文件管理规定的要求保存。公司确保向员工、职工代表及有关的相关方报告相关的审核结果。

9.3 管理评审

9.3.0 职责

1、总经理主持管理评审活动。

2、安全运营管理室负责管理评审的组织实施与协调、改进措施实施的跟踪验证。

9.3.1 总则

为确保管理体系持续的适宜性、充分性和有效性，公司应对管理评审活动进行策划、按照策划的时间间隔进行管理评审，并确保每年至少进行一次覆盖公司一体化管理体系全部范围的年度管理评审活动。管理评审内容需满足公司管理改进的要求，以确保一体化管理体系持续的保持适宜性、充分性和有效性。

9.3.2 管理评审输入

管理评审输入可以以部门工作总结或专题汇报（如公司年度安全生产管理情况报告）等形式提交会议讨论。管理评审输入包括：

1、以往管理评审决议的贯彻、落实情况；

2、外部市场经营环境和公司内部经营条件的变化；

3、顾客满意和其他相关方的需求、期望和反馈；

4、资源配置（人员、技术、财力、基础设施等）的充分性；

5、服务管理方针、信息安全方针和标准要的其他策略的遵守情况和适宜性；

6、服务管理目标、信息安全目标的实现程度；

7、风险评估的结果，以及为应对风险和机遇而采取措施的有效性；

8、有关一体化管理体系绩效和有效性的信息等。

9.3.3 管理评审输出

9.3.3.1 管理评审的输出应包括：

1、公司管理体系运行的总体评价；

2、确定改进项目，如管理流程优化等，以及改进的相关措施或要求；

3、确定需要的变更，如对方针和目标的调整、对职责、权限及文件的更改等。

4、确定资源的投入，如对人力资源的补充调整、购置新的设备设施等。

9.3.3.2 各部门执行管理评审决定，采取改进措施，跟踪并验证改进措施的实施，并就改进的情况提交下次管理评审。

9.4 信息技术服务报告

管理评审的输出还包括利用信息技术服务管理体系(IT-SMS)的活动和交付服务产生的信息编制服务管理体系和服务绩效和有效性报告。服务报告应包括趋势。公司应根据服务报告的结果做出决策并采取措施，并向相关方传达商定的措施。

10 持续改进

10.1 总则

10.1.0 职责

管理者代表负责持续改进过程的策划。

10.1.1 公司确定并选择改进机会，采取必要措施，满足顾客、相关方要求，提高管理体系的绩效和有效性。改进的方式可以是被动地改进(如纠正措施 10.2)、渐进地改进(如持续改进 10.3)、创造性改进(如技术创新)或重组(如转型)等多种形式。

10.2 不符合和纠正措施

10.2.0 职责

1、安全运营管理室归口信息安全、信息技术服务不合格和质量问题以及一体化管理体系不符合的管理。

2、各部门负责归口管理过程不符合的识别、控制及相关纠正措施的实施。

10.2.1 总则

公司确保对不合格和不符合要求的管理活动进行识别和控制，并及时采取纠正措施，以消除不符合的原因，防止不符合的再发生。

10.2.2 不合格（不符合）

当出现不合格（不符合）时，公司应采取以下方面的行动：

1、对不合格（不符合）做出应对，首先应采取措施以控制和纠正发现的不合格（不符合），防止问题的蔓延和扩展，并对不合格（不符合）造成的后果予以及时处置。

2、在采取措施控制或纠正不合格（不符合）的同时，应对问题的原因进行调查，必要时，实施纠正措施（10.2.3）。

10.2.3 纠正措施

公司及时采取纠正措施，以消除不符合的原因，防止不符合的再发生，所采取的纠正措施应与所遇到问题的影响程度相适应。纠正措施的实施步骤如下：

1、通过监视、测量等活动发现不符合（不合格）；

2、对不符合（不合格）进行原因分析，并举一反三，是否还有类似的不符合（不合格），必要时调查核实；

3、针对原因采取纠正措施，重大纠正措施应提交主管领导审定；

4、有关责任部门或责任人组织实施纠正措施；

5、主管或监督部门到验证纠正措施实施的效果；

6、向与不符合（不合格）相关的内部和相关方沟通或通报不符合（不合格）及处理结果；

7、将纠正措施实施结果提交管理评审。

10.3 持续改进

10.3.0 职责

1、总经理批准每年的改进事项和管理改进计划，

2、管理者代表负责组织改进的实施和改进效果评价。

3、安全运营管理室汇总持续改进信息和事项，编制改进计划，组织实施并监督检查执行情况。

10.3.1 公司依据分析和评价和管理评审输出结果，确定改进的机会，实施改进措施，持续改进管理体系的效率与效益。

10.3.2 公司通过实施以下活动达到持续改进的目的：

1、在管理方针中作出持续改进的承诺，通过建立管理目标来设定具体的改进要求，从而确定公司的改进方向和目标，营造一个激励改进的氛围与环境；

2、通过分析和评价的结果来评价管理体系的改进机会，例如：顾客满意信息、信息技术服务质量问题统计信息、不良趋势方面的信息等等，从而确定改进的需求。

3、通过内部审核的结果来确定管理体系的薄弱环节，并采取相应的改进措施以实现持续改进；

4、针对已发生的不符合或潜在的不符合的原因，采取适宜的纠正措施和应对措施，达到防止不符合再发生或发生的目的；

5、关注外部环境、市场的变化作出快速灵活的反应，引入新材料、新技术、新设备、新工艺、新理念、新方法；

6、通过知识的获取、分享与应用进行改进和创新；

7、通过管理评审作出管理体系及其过程、服务质量、资源方面的改进决定或措施，并有针对性地采取相应的改进措施，以不断提高管理体系的充分性、适宜性、有效性；

8、通过员工参与和合理化建议不断寻找改进的机会，并做出适当的改进活动安排。

10.3.3 改进过程包括以下步骤：

1、识别改进的潜在机会；

2、分析并确认实施改进的合理性(成本/收益)；

3、确定资源的投入与配置；

4、做出实施改进的决定，确定改进目标；

5、研究实现目标所需的方法、措施和各种方案；

6、实施改进，并对实施过程进行监视和测量；

7、改进的影响和效果的验证；

8、在下一次管理评审中审议改进结果。

附录

附录 1 标准对照表

手册条款标题	ISO/IEC20000-1：2018	GB/T22080-2016
4 组织环境	4 组织的环境	4 组织的环境
4.1 理解组织及其环境	4.1 理解组织及其环境	4.1 理解组织及其环境
4.2 理解相关方的需求和期望	4.2 理解相关方的需求和期望	4.2 理解相关方的需求和期望
4.3 确定管理体系的范围	4.3 确定服务管理体系范围	4.3 确定信息安全管理体系范围
4.4 管理体系及其过程	4.4 服务管理体系	4.4 信息安全管理体系
5 领导作用	5 领导作用	5 领导
5.1 领导作用和承诺	5.1 领导作用和承诺	5.1 领导和承诺
5.2 方针	5.2 方针 5.2.1 制定服务管理方针 5.2.2 沟通服务管理方针	5.2 方针
5.3 组织的岗位、职责和权限	5.3 组织角色、职责和权限	5.3 组织的角色、责任和权限
6 策划	6 策划	6 规划
6.1 应对风险和机遇的措施	6.1 应对风险和机遇的措施	
6.1.1 总则		
6.1.2 经营风险与信息技术服务风险		
6.1.3 信息安全风险		6.1 应对风险和机会的措施
6.2 目标及其实现的策划	6.2 服务管理目标及其实现目标的策划 6.2.1 制定目标 6.2.2 实现目标的策划	6.2 信息安全目标及其实现目标的策划
6.3 策划服务管理体系	6.3 策划服务管理体系	
7 支持	7 服务管理体系的支持	7 支持
7.1 资源	7.1 资源	7.1 资源
7.2 能力	7.2 能力	7.2 能力
7.3 意识	7.3 意识	7.3 意识
7.4 沟通	7.4 沟通	7.4 沟通
7.5 成文信息	7.5 文档信息 7.5.1 总则	7.5 文件化信息

手册条款标题	ISO/IEC20000-1：2018	GB/T22080-2016
	7.5.2 创建和更新文档信息 7.5.3 文档信息的控制 7.5.4 服务管理体系文档信息	
7.6 知识	7.6 知识	
8 运行		
8.1 服务运行的策划和控制	8 服务管理体系的运行	
8.1.1 运行的策划与控制	8.1 运行的策划和控制	
8.1.2 服务组合	8.2 服务组合	
8.1.3 关系与协议	8.3 关系与协议	
8.1.4 供给与需求	8.4 供给与需求	
8.1.5 服务设计、创建和转换	8.5 服务设计、创建和转换	
8.1.6 解决与实现	8.6 解决与实现	
8.1.7 服务保证	8.7 服务保证	
8.2 信息安全运行控制		8 运行
8.2.1 运行规划和控制		8.1 运行规划和控制
8.2.2 信息安全风险评估		8.2 信息安全风险评估
8.2.3 信息安全风险处置		8.3 信息安全风险处置
9 绩效评价	9 绩效评价	9 绩效评价
9.1 监视、测量、分析和评价	9.1 监视、测量、分析和评价	9.1 监视、测量、分析和评价
9.2 内部审核	9.2 内部审核	9.2 内部审核
9.3 管理评审	9.3 管理评审	9.3 管理评审
9.4 信息技术服务报告	9.4 服务报告	
10 持续改进	10 改进	10 改进
10.1 总则		
10.2 不符合和纠正措施	10.1 不符合和纠正措施	10.1 不符合和纠正措施
10.3 持续改进	10.2 持续改进	10.2 持续改进

附录 2 手册条款职能分配表

符号释义：

●——主控⊙——部分职能主控○——参与

手册条款标题	管理层	解决方案室	交付支撑室	平台运维室	安全运营管理室
4 组织环境（仅标题）					
4.1 理解组织及其环境	●	○	○	○	○
4.2 理解工作人员和其他相关方的需求和期望	●	○	○	○	○
4.3 确定管理体系的范围	●	○	○	○	○
4.4 管理体系及其过程	●	○	○	○	○
5 领导作用（仅标题）					
5.1 领导作用和承诺	●	○	○	○	○
5.2 方针	●	○	○	○	○
5.3 组织的岗位、职责和权限	●	●	○	○	○
6 策划（仅标题）					
6.1 应对风险和机遇的措施（仅标题）					
6.1.1 总则	●	○	○	○	○
6.1.2 经营风险与信息技术服务风险	○	○	○	●	○
6.1.3 信息安全风险	○	○	○	○	●
6.2 目标及其实现的策划	○	○	○	○	●
6.3 策划服务管理体系	●	○	○	○	○
7 支持（仅标题）					
7.1 资源	●	○	○	○	○
7.2 能力	○	○	○	○	●
7.3 意识	○	○	○	○	●
7.4 沟通	●	○	○	○	●
7.5 成文信息	○	○	○	○	●
7.6 知识	○	○	○	○	●
8 运行（仅标题）					
8.1 服务运行策划和控制（仅标题）	○	○	○	○	○
8.1.1 运行策划和控制	○	○	●	○	○
8.1.2 服务组合	○	○	●	○	○
8.1.3 关系与协议	○	○	●	○	○
8.1.4 供给与需求	○	○	●	○	○
8.1.5 服务设计、创建和转换	○	○	●	○	○
8.1.6 解决与实现	○	○	●	○	○
8.1.7 服务保证	○	○	●	○	○
8.2 信息安全运行控制（仅标题）	○	○	○	○	○

手册条款标题	管理层	解决方案室	交付支撑室	平台运维室	安全运营管理室
8.2.1 运行的规划和控制	○	○	○	○	●
8.2.2 信息安全风险评估	○	○	○	○	●
8.2.3 信息安全风险处置	○	○	○	○	●
9 绩效评价（仅标题）					
9.1 监视、测量、分析和评价					
9.2 内部审核	○	○	○	○	●
9.3 管理评审	●	○	○	○	●
9.3 信息技术服务报告	○	○	○	●	○
10 持续改进（仅标题）					
10.1 总则	●	○	○	○	●
10.2 不符合和纠正措施	○	○	○	○	●
10.3 持续改进	●	○	○	○	●

附录 3 信息安全管理体系标准附录 A 职能分配表

符号释义：

●——主控⊙——部分职能主控○——参与

附录 A	管理层	解决方案室	交付支撑室	平台运维室	安全运营管理室
A5 信息安全策略					
A5.1 信息安全管理指导	○	○	○	○	●
A5.1.1 信息安全策略	○	○	○	○	●
A5.1.2 信息安全策略的评审	○	○	○	○	●
A6 信息安全组织					
A6.1 内部组织 6.1.1 信息安全的角色和责任 6.1.2 职责分类 6.1.3 与职能机构的联系 6.1.4 与特定相关方的联系 6.1.5 项目管理中的信息安全	○	○	○	○	●
A6.2 移动设备和远程工作	○	○	○	●	⊙
A6.2.1 移动设备策略	○	○	○	●	⊙
A6.2.2 远程工作	○	○	○	●	⊙
A7 人力资源安全					⊙
A7.1 任用前 7.1.1 审查 7.1.2 任用条款及条件	○	○	○	○	●
A7.2 任用中 7.2.1 管理责任 7.2.2 信息安全意识、教育和培训 7.2.3 违规处理过程	○	○	○	○	●
A7.3 任用的终止和变更 7.3.1 任用终止或变更的责任	○	○	○	○	●
A8 资产管理					
A8.1 有关资产的责任 8.1.1 资产清单 8.1.2 资产的所属关系 8.1.3 资产的可接受使用 8.1.4 资产归还	○	○	○	●	⊙
A8.2 信息分级 8.2.1 信息分级 8.2.2 信息的标记 8.2.3 资产的处理	○	○	○	●	⊙
A8.3 介质处理 8.3.1 移动介质的管理 8.3.2 介质的处置 8.3.3 物理介质的转移	○	○	○	●	⊙
A9 访问控制	○	○	○	●	⊙

附录 A	管理层	解决方案室	交付支撑室	平台运维室	安全运营管理室
A9.1 访问控制的业务要求 9.1.1 访问控制策略 9.1.2 网络和网络服务的访问	○	○	○	●	⊙
A9.2 用户访问管理 9.2.1 用户注册和注销 9.2.2 用户访问供给 9.2.3 特许访问权管理 9.2.4 用户的秘密鉴别信息管理 9.2.5 用户访问权的评审 9.2.6 访问权的移除或调整	○	○	○	●	⊙
A9.3 用户责任	○	○	○	●	⊙
A9.3.1 秘密鉴别信息的使用	○	○	○	●	⊙
A9.4 系统和应用访问控制 9.4.1 信息访问限值 9.4.2 安全登录规程 9.4.3 口令管理系统 9.4.4 特权实用程序的使用 9.4.5 程序源代码的访问控制	○	○	○	●	⊙
A10 密码 10.1 密码控制 10.1.1 密码控制的使用策略 10.1.2 密匙管理	○	○	○	●	⊙
A11 物理和环境安全	○	○	○	●	⊙
A11.1 物理和环境安全 11.1.1 物理安全边界 11.1.2 物理入口控制 11.1.3 办公室、房间和设施的安全保护 11.1.4 外包和环境威胁的安全防护 11.1.5 在安全区域工作 11.1.6 交接区	○	○	○	●	⊙
A11.2 设备 11.2.1 设备安置和保护 11.2.2 支持性设施 11.2.3 布缆安全 11.2.4 设备维护 11.2.5 资产的移动 11.2.6 组织场所外的设备资产安全 11.2.7 设备的安全处置或再利用 11.2.8 无人值守的用户设备 11.2.9 清理桌面和屏幕策略	○	○	○	●	⊙
A12 运行安全	○	○	○	●	⊙
A12.1 运行规程和责任 12.1.1 文件化的操作规程 12.1.2 变更管理 12.1.3 容量管理 12.1.4 开发、测试和运行环境的分离	○	○	○	●	⊙
A12.2 恶意软件防范 12.2.1 恶意软件的控制	○	○	○	●	⊙

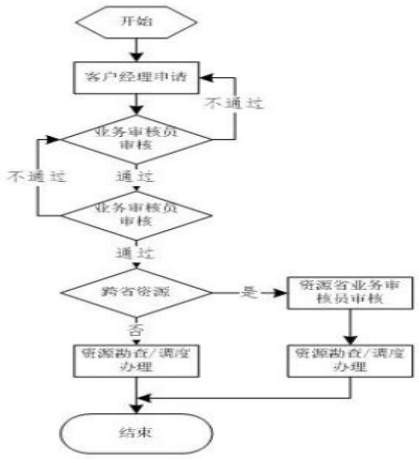
附录 A	管理层	解决方案室	交付支撑室	平台运维室	安全运营管理室
A12.3 备份 12.3.1 信息备份	○	○	○	●	⊙
A12.4 日志 12.4.1 事态日志 12.4.2 日志信息的保护 12.4.3 管理员和操作员日志 12.4.4 时钟同步	○	○	○	●	⊙
A12.5 运行软件的控制 12.5.1 运行系统的软件安装	○	○	○	●	⊙
A12.6 技术方面的脆弱性管理 12.6.1 技术方面脆弱性的管理 12.6.2 软件安装限制	○	○	○	●	⊙
A12.7 信息系统审计的考虑 12.7.1 信息系统审计的控制	○	○	○	●	⊙
A13 通信安全					
A13.1 网络安全管理 13.1.1 网络控制 13.1.2 网络服务的安全 13.1.3 网络中的隔离	○	○	○	●	⊙
A13.2 信息传输 13.2.1 信息传输策略和规程 13.2.2 信息传输协议 13.2.3 电子消息发送 13.2.4 保密或不泄露协议	○	○	○	●	⊙
A14 系统获取、开发和维护	○	○	○	●	⊙
A14.1 信息系统的安全要求 14.1.1 信息安全要求分析和说明 14.1.2 公共网络上应用服务的安全保护（删除） 14.1.3 应用服务事务的保护（删除）	○	○	○	●	⊙
A14.2 开发和支持过程中的安全 14.2.1 安全的开发策略 14.2.2 系统变更控制规程 14.2.3 运行平台变更后对应用技术评审 14.2.4 软件包变更的限制 14.2.5 系统安全工程原则 14.2.6 安全的开发环境 14.2.7 外包开发(删除) 14.2.8 系统安全测试 14.2.9 系统安全测试 14.2.9 系统验收测试	○	○	○	●	⊙
A14.3 测试数据 14.3.1 测试数据的保护	○	○	○	●	⊙
A15 供应商关系					
A15.1 供应商关系中的信息安全 15.1.1 供应商关系的信息安全策略 15.1.2 在供应商协议中强调安全 15.1.3 信息与通信技术供应链	○	●	○	○	⊙

附录 A	管理层	解决方案室	交付支撑室	平台运维室	安全运营管理室
A15.2 供应商服务交付管理 15.2.1 供应商服务的监视和评审 15.2.2 供应商服务的变革管理	○	●	○	○	⊙
A16 信息安全事件管理	○	○	○	●	⊙
A16.1 信息安全事件的管理和改进 16.1.1 责任和规程 16.1.2 报告信息安全事态 16.1.3 报告信息安全弱点 16.1.4 信息安全事态的评估和转换 16.1.5 信息安全事件的响应 16.1.6 从信息安全事件中学习 16.1.7 证据的收集	○	○	○	●	⊙
A17 业务连续性管理的信息安全方面					
A17.1 信息安全的连续性 17.1.1 规划信息安全连续性 17.1.2 实现信息安全连续性 17.1.3 验证、评审和评价信息安全连续性	○	○	○	●	⊙
A17.2 冗余	○	○	○	●	⊙
A17.2.1 信息处理设施的可用性	○	○	○	●	⊙
A18 符合性	○	○	○	●	⊙
A18.1 符合法律和合同要求 18.1.1 适用的法律和合同要求的识别 18.1.2 知识产权 18.1.3 记录的控制 18.1.4 隐私和个人可识别信息保护 18.1.5 密码控制规则	○	○	○	●	⊙
A18.2 信息安全评审 18.2.1 信息安全的独立评审 18.2.2 符合安全策略和标准 18.2.3 技术符合性评审	○	○	○	●	⊙

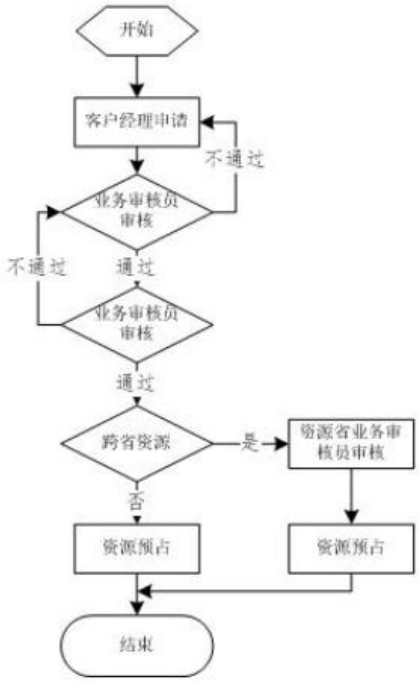
附录 4　业务流程

附录 4-1　IDC 数据中心业务

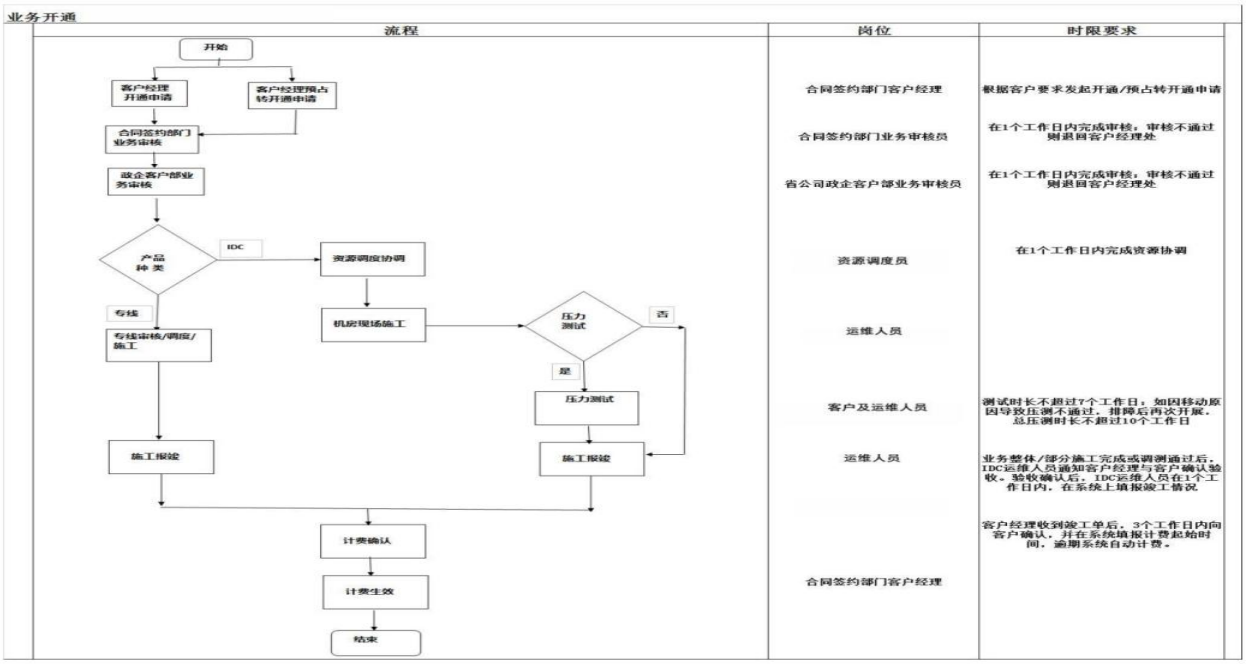
(1) IDC 资源勘查流程

资源勘察			
	流程	岗位	时限要求
		合同签约部门客户经理 合同签约部门业务审核员 省公司政企部业务审核员 涉及资源省业务审核员 数据中心资源调度员	根据客户需求发起资源勘查申请 在1个工作日内完成审核 在1个工作日内完成审核 在1个工作日内完成审核 在1个工作日内完成资源勘查，并反馈客户经理

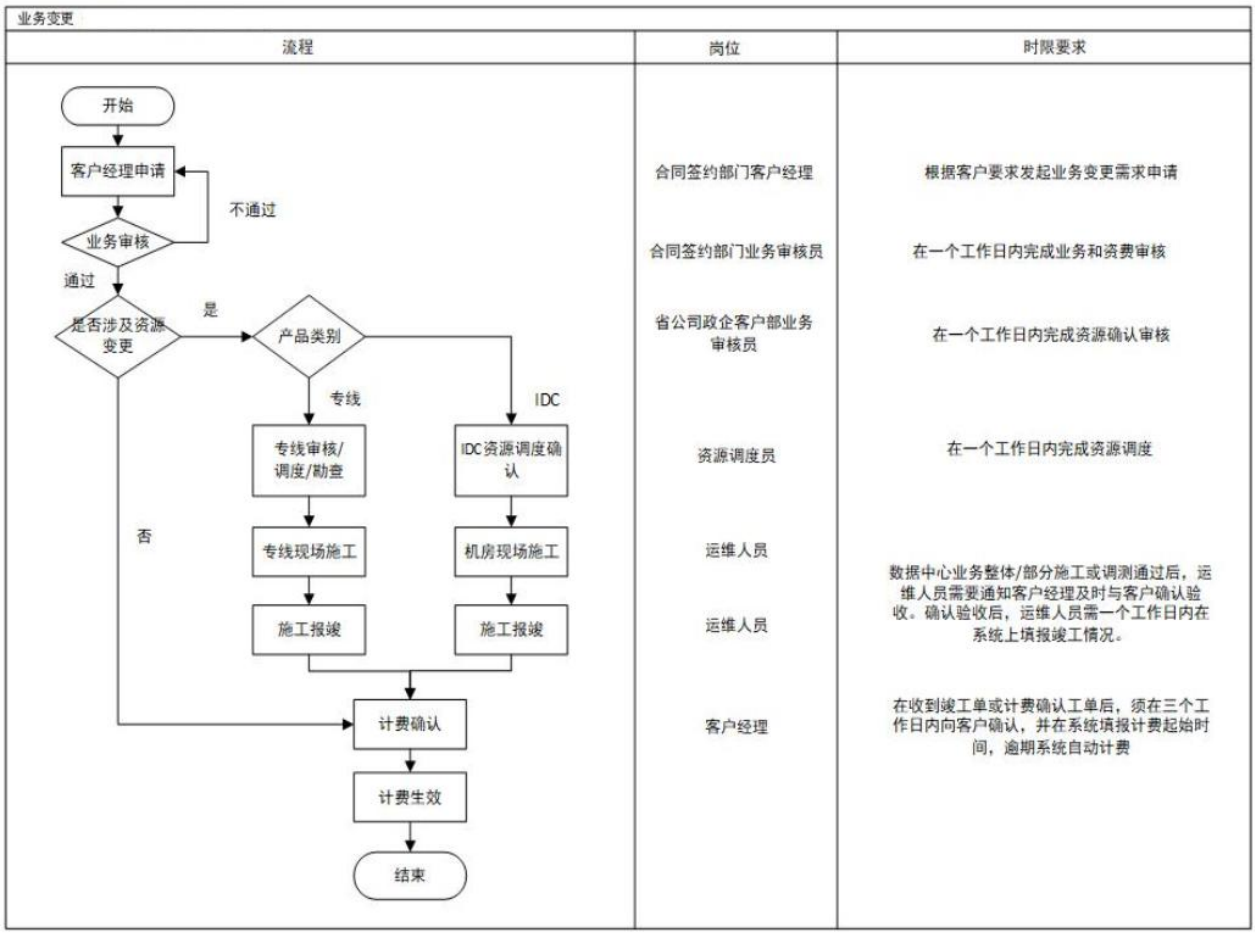
(2) IDC 资源预占流程

资源预占			
	流程	岗位	时限要求
		合同签约部门客户经理 合同签约部门业务审核员 省公司政企部业务审核员 涉及资源省业务审核员 数据中心资源调度员	根据客户需求发起资源预占申请 在1个工作日内完成审核 在1个工作日内完成审核 在1个工作日内完成审核 在2个工作日内完成资源电子预占，并反馈客户经理

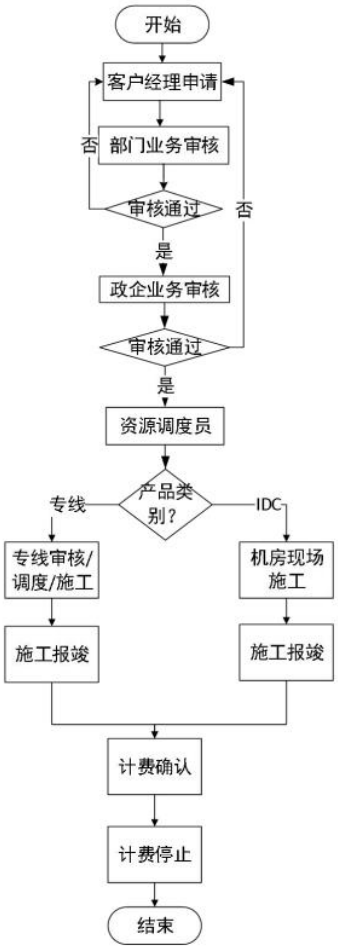
(3) IDC 业务开通流程



(4) IDC 业务变更流程

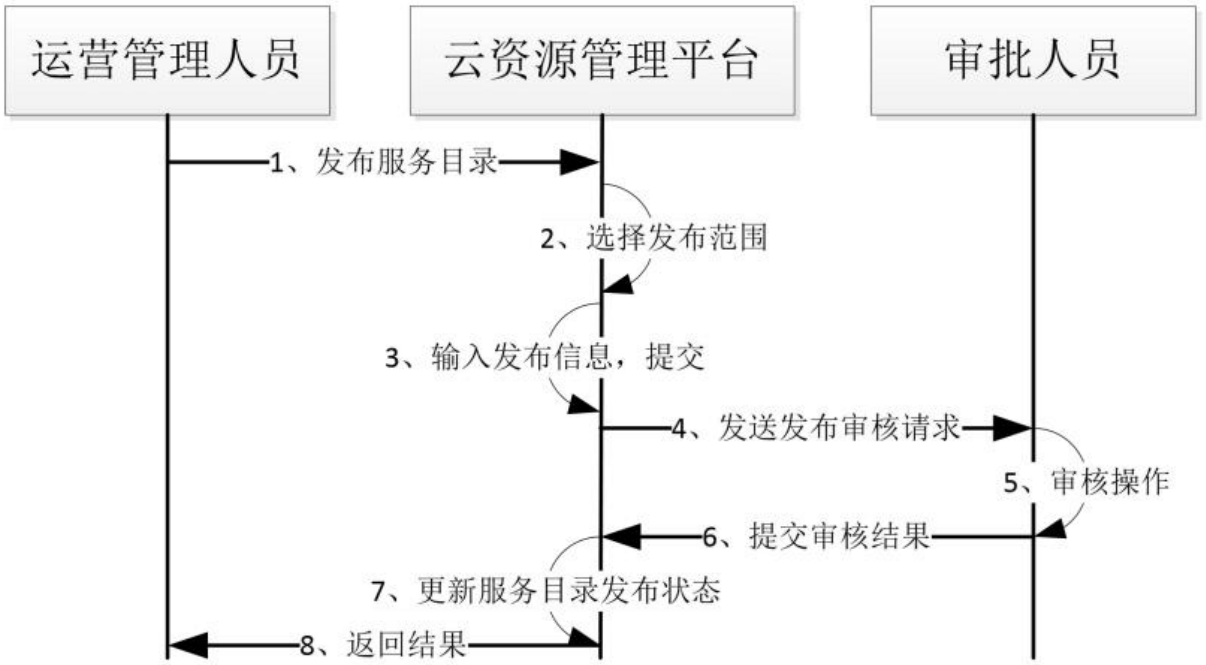


(5) IDC 业务注销流程

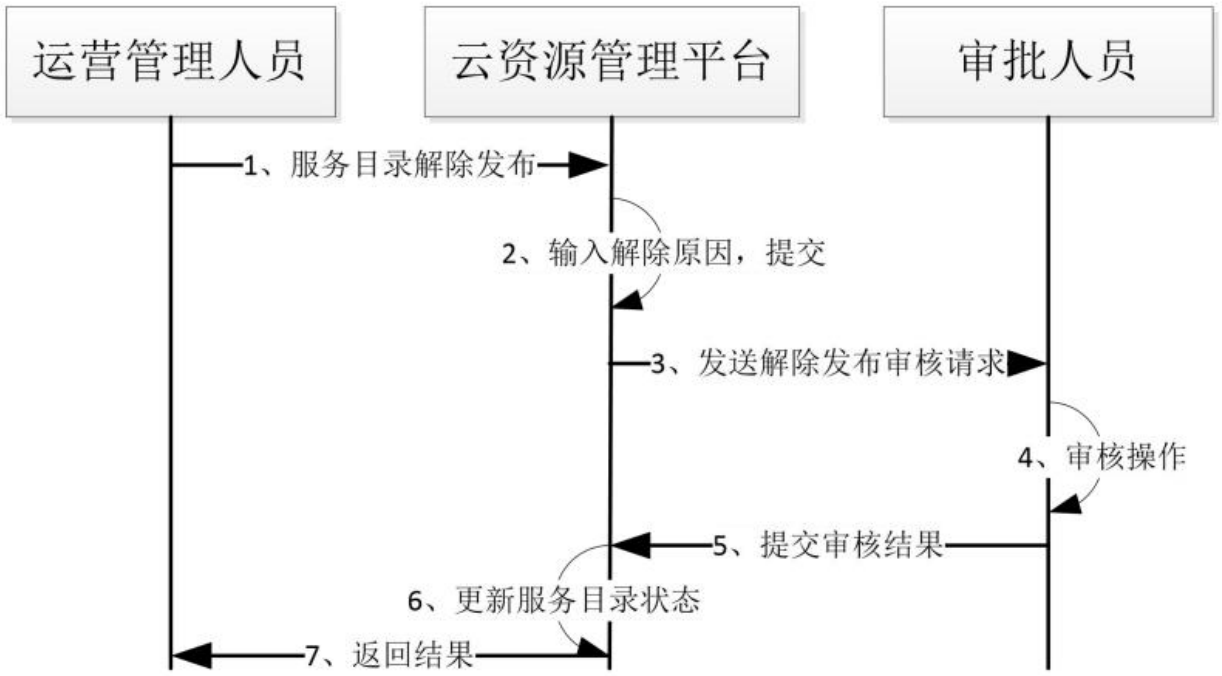
业务注销		
流程	岗位	时限要求
	合同签约部门客户经理 合同签约部门业务审核员 省公司政企客户部业务审核员 资源调度员 运维人员 客户及运维人员 运维人员 客户及合同签约部门客户经理 合同签约部门客户经理	根据客户要求发起退订申请 在1个工作日内完成审核 在1个工作日内完成审核 在1个工作日内完成资源调度 根据工单的注销时间，组织完成本地注销施工，在注销施工完成后1个工作日内在完成报竣。 客户经理在收到竣工单后，须在3个工作日内向客户确认，并在确认后1个工作日内在系统填报注销时间。

附录 4-2　云计算 IaaS 业务、PaaS 业务及 SaaS 业务

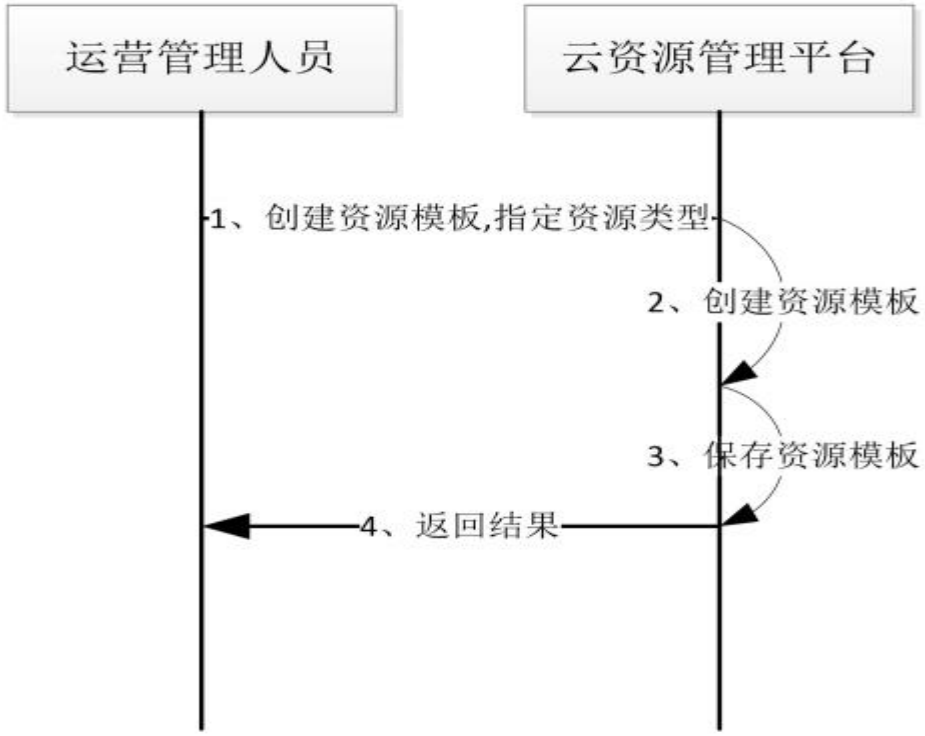
(1) 云产品服务目录发布流程



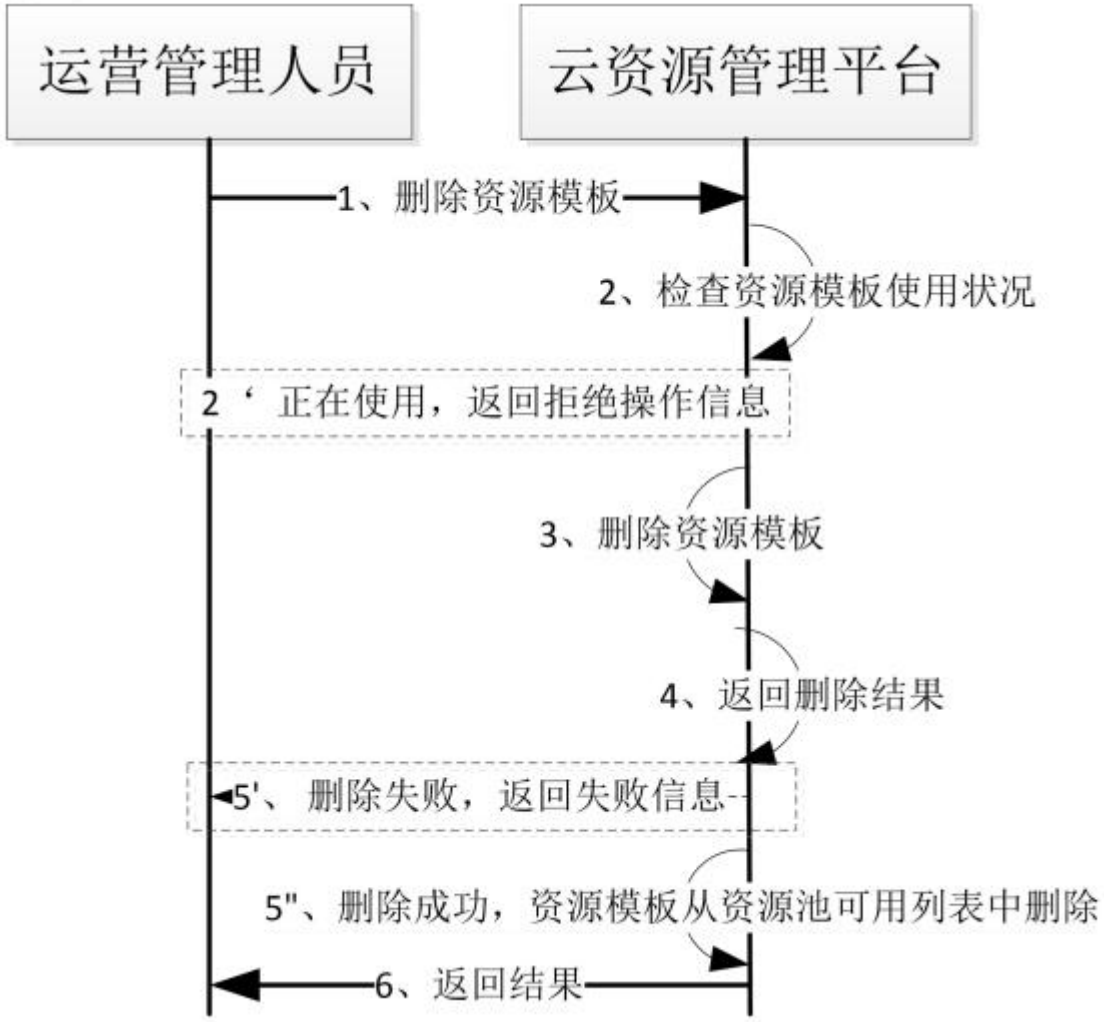
(2) 云产品服务目录解除流程



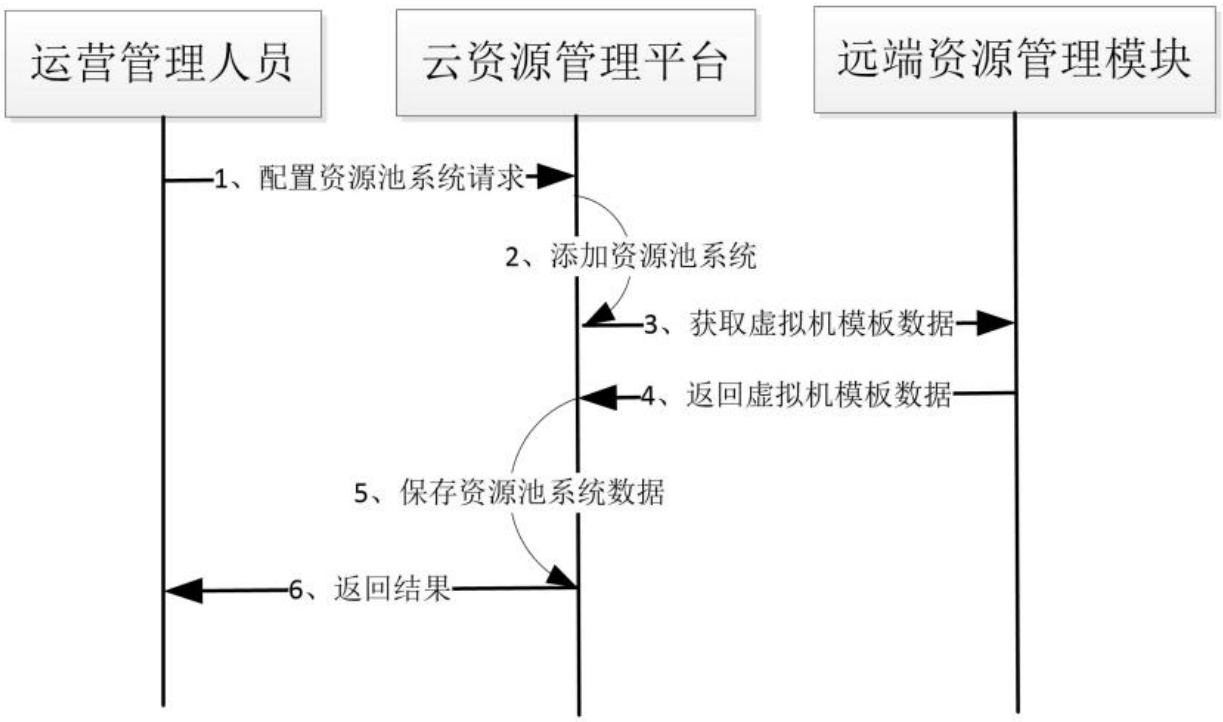
(3) 云主机资源模板创建流程



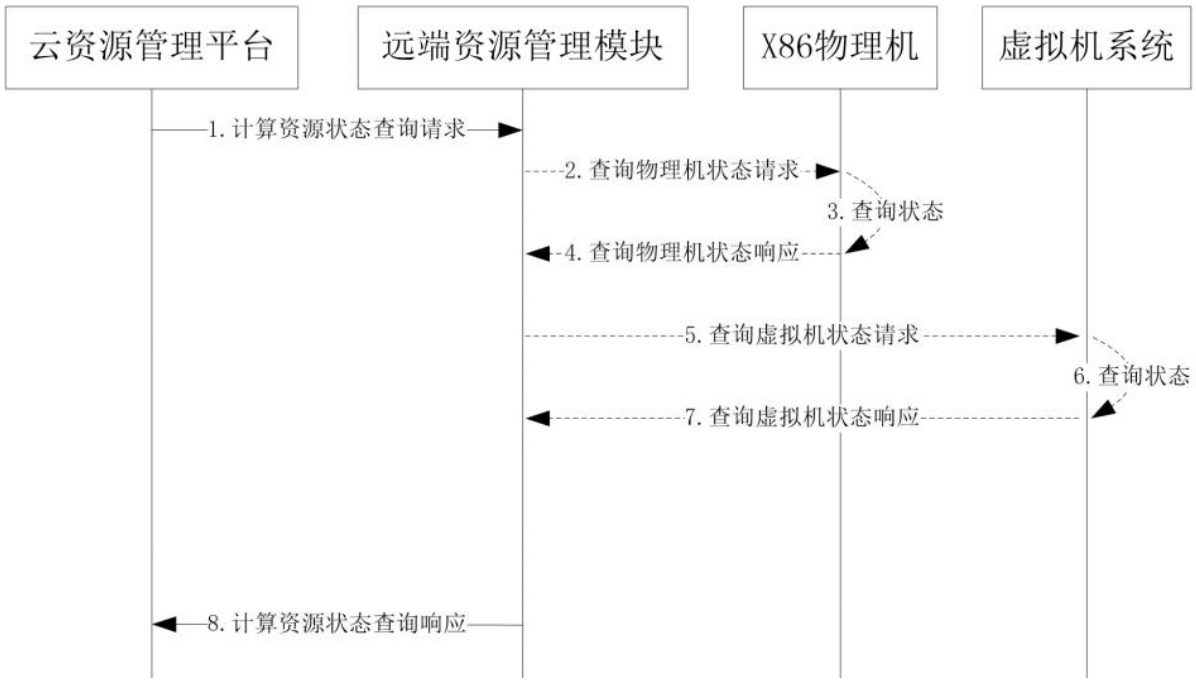
(4) 云主机资源模板删除流程



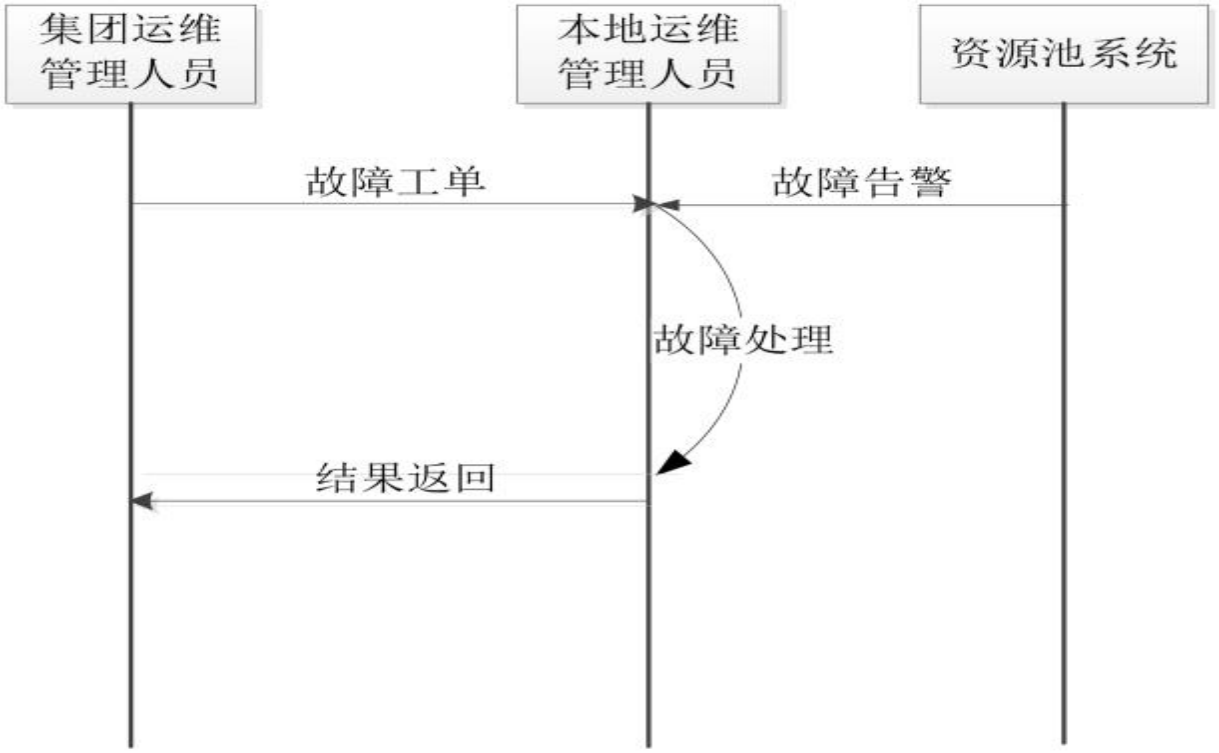
(5) 云资源添加/配置流程



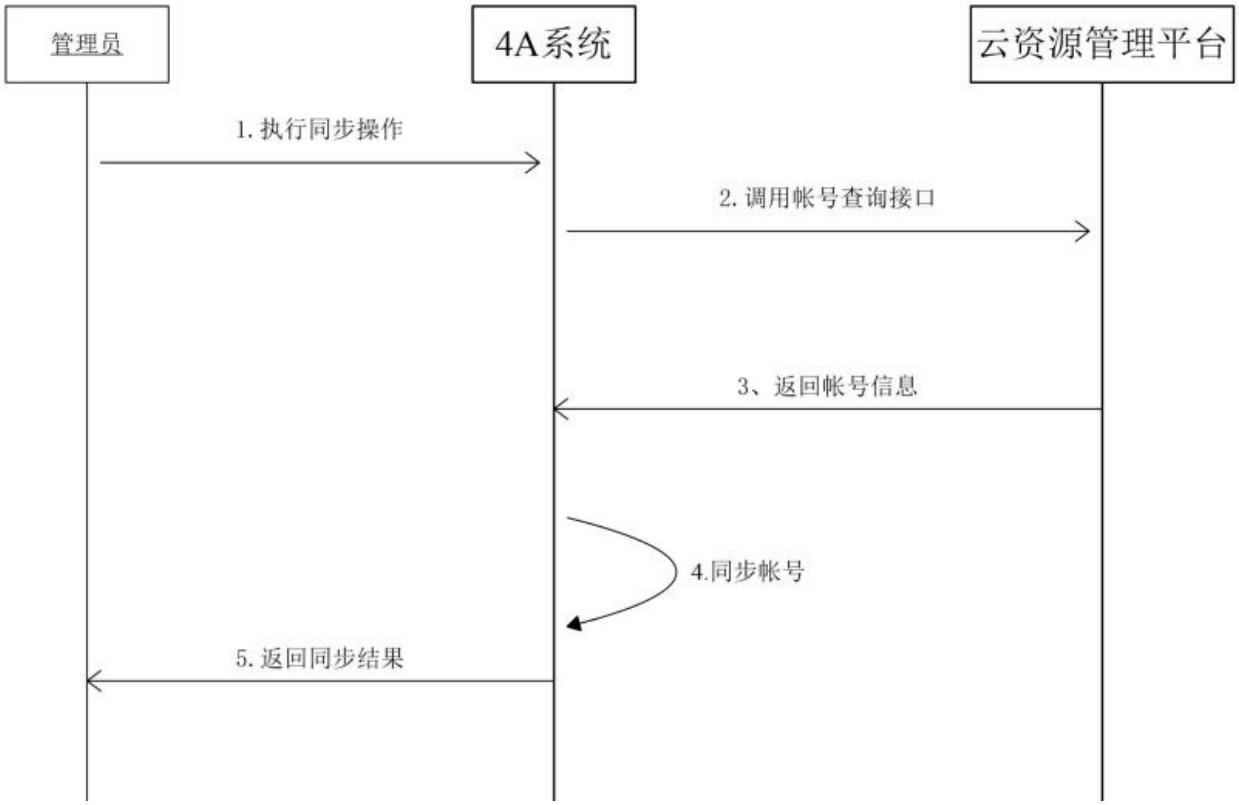
(6) 云资源状态查询流程



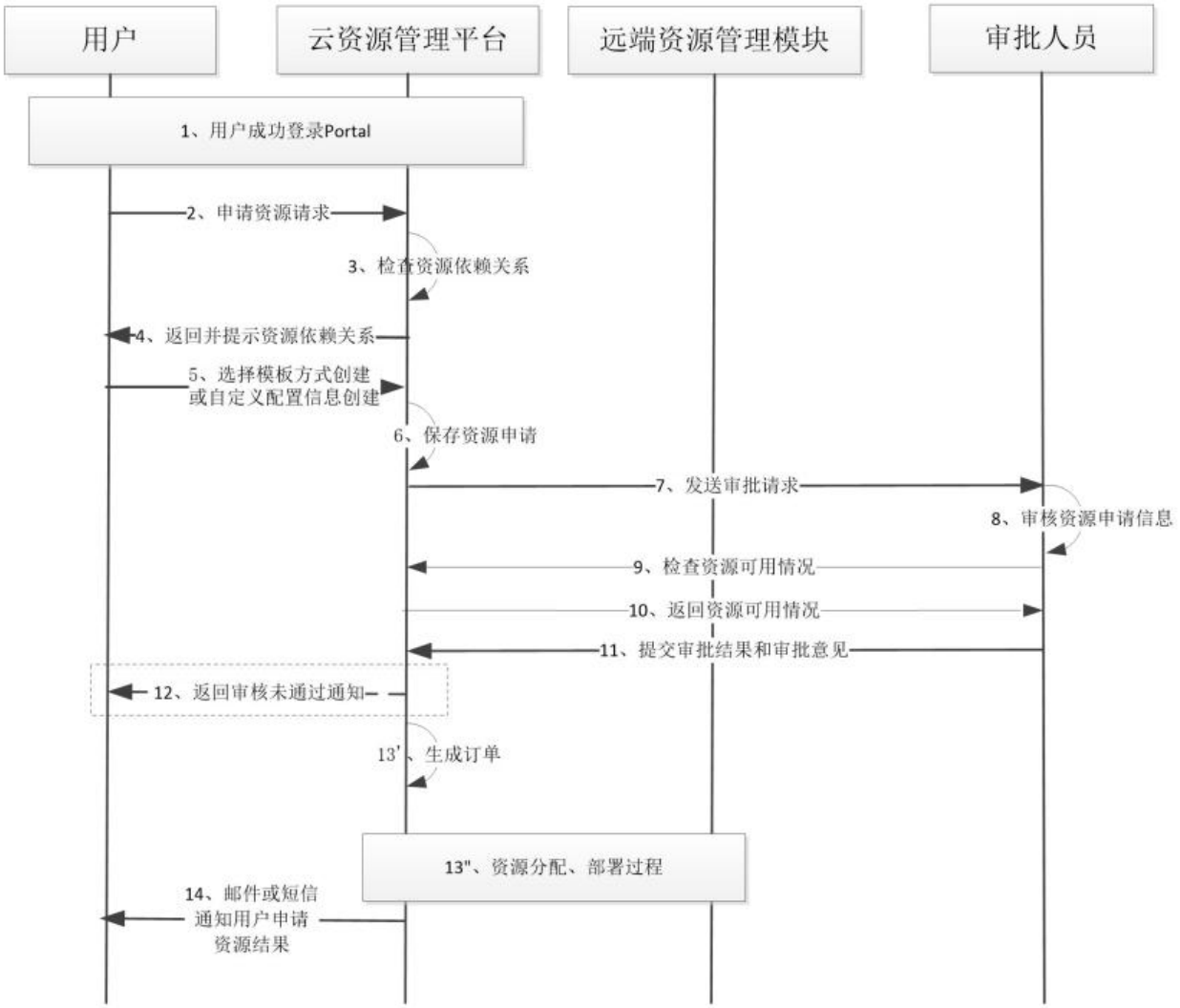
(7) 云资源事件处理流程



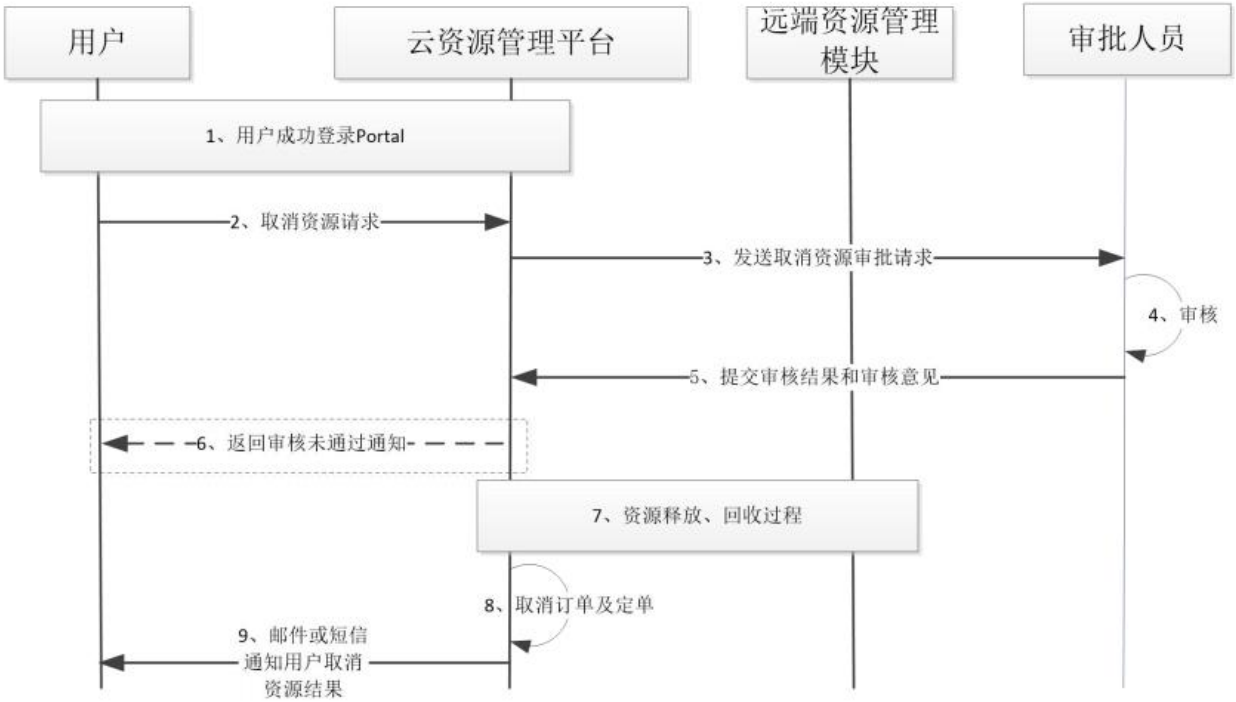
(8) 云平台用户创建流程



(9) 云资源申请开通流程



(10) 云资源释放流程



中国移动通信集团新疆有限公司

ZGYDXJ -SoA-01

信息安全适用性声明

依据： GB/T22080-2016/ISO/IEC 27001：2013 编制

文件版本：2.0

审　　核： 王 博

批　　准： 蒋文隆

受控状态： 受控

2021 年 11 月 1 日 发布　　2022 年 5 月 18 日 修订

文件控制页

文件编号	ZGYDXJ -SoA-01		
文件名称	**《信息安全适用性声明》**		
版 本 号	2.0		
受控状态	受控	受控编号	

更改情况

版本	章节/条款	修改内容	更改人/日期	批准人/日期
1.0		全文发布	王 博 2021.11.1	蒋文隆 2021.11.1
2.0		原 A10 为删减，现补充 A10 内容	王 博 2022.5.18	蒋文隆 2022.5.18

目 录

1 目的与范围

本声明描述了在 GB/T22080-2016/ISO/IEC 27001：2013 附录 A 中，适用于本公司信息安全管理体系的目标/控制、是否选择这些目标/控制的理由、公司现行的控制方式、以及实施这些控制所涉及的相关文件。

ISMS 的范围是：向客户提供 IDC 数据中心业务、云计算 IaaS 业务（弹性计算、云存储、云网络、云安全、管理与监控）、PaaS 业务及 SaaS 业务(开放云市场业务)运营和运行维护相关活动的信息安全管理活动。

公司地理位置： 新疆维吾尔自治区乌鲁木齐市水磨沟区红光山路 1966 号

涉及部门：公司云能力服务中心及相关员工。

资产范围：上述范围内涉及的所有信息资产，包括软件、数据、硬件、人员、文档、服务和其它资产。详见《资产清单》。

本公司《管理手册》采用了 GB/T22080-2016/ISO/IEC 27001：2013 标准正文的全部内容，对附录 A 的删减及理由如下：

适用性声明中删减了 A.9.4.5，A.10， A.14.2.7；

A.14.2.7 的删减理由：本公司不涉及软件外包开发， A.9.4.5 的删减理由：不涉及程序源代码。

2 相关文件

《管理手册》

《管理制度》

3 职责

《信息安全适用性声明》由安全运营管理室负责组织编制、修订，管理者代表审核、由总经理批准。

4 声明

本公司按 GB/T22080-2016/ISO/IEC 27001：2013 建立信息安全管理体系。

根据公司风险评估的结果和风险可接受水平，GB/T22080-2016/ISO/IEC 27001：2013 附录 A 部分条款被选择（或不选择）用于公司信息安全管理体系。

A.5 信息安全策略

标准条款号	标 题	目标/控制	是否选择	选择理由	控制描述	相关文件
A.5.1	信息安全管理指导	目标	YES	依据业务要求和相关的法律法规提供管理指导并支持信息安全。		
A.5.1.1	信息安全策略	控制	YES	信息安全管理实施的需要。	信息安全策略由公司制定，由公司总经理批准发布。通过培训、发放，等方式传达到每一员工。	信息安全策略
A.5.1.2	信息安全策略评审	控制	YES	确保策略的适宜性、充分性和有效性。	按照计划的时间间隔对信息安全策略进行评审。	信息安全策略

A.6 信息安全组织

标准条款号	标 题	目标/控制	是否选择	选择理由	控制描述	相关文件
A.6.1	内部组织	目标	YES	建立一个有效的信息安全管理组织机构。		
A.6.1.1	信息安全角色和职责	控制	YES	对于所有的安全职责都给与充分的定义和分配		
A.6.1.2	职责分离	控制	YES	保持特定资产和完成特定安全过程的职责需确定。	公司设立信息安全管理者代表，全面负责公司 ISMS 的建立、实施与保持工作。对每一项重要信息资产指定信息安全责任人。 与 ISMS 有关各部门的信息安全职责在《管理手册》中予以描述，关于具体的信息安全活动的职责在程序及作业文件中予以明确。	已规定了职能范围内所有人员的信息安全职责

A.6.1.3	与职能机构的联系	控制	YES	与法律实施部门、标准机构等组织保持适当的联系是必须的，以获得必要的安全管理、标准、法律法规方面的信息。	公司就电话/网络通讯系统的安全问题与市信息主管部门及标准制定部门保持联系，其他部门与相应的政府职能部门及社会服务机构保持联系，以便及时掌握信息安全的法律法规，及时获得安全事故的预防和纠正信息，并得到相应的支持。 信息安全交流时，确保本公司的敏感信息不传给未经授权的人。	相关方联系表
A.6.1.4	与特定相关方的联系	控制	YES	为更好掌握信息安全的新技术及安全方面的有益建议，需获得内外部信息安全专家的建议。	本公司设内部信息安全顾问，必要时聘请外部专家，与特定利益群体保持沟通，解答有关信息安全的问题。顾问与专家名单由本公司安全运营管理室提出，管理者代表批准。 内部信息安全顾问负责： a) 按照专业分工负责解答公司有关信息安全的问题并提供信息安全的建议； b) 收集与本公司信息安全有关的信息、新技术变化，经本部门负责人审核同意，利用本公司电子邮件系统或采用其它方式传递到相关部门和人员； c) 必要时，参与信息安全事故的调查工作。	相关方联系表
A.6.1.5	项目管理中的信息安全	控制	YES	无论何种类型的项目。宜将信息安全融入到项目管理中		
A.6.2	移动设备和远程工作	目标	YES	确保远程工作和移动设备使用的安全。		
A.6.2.1	移动设备策略	控制	YES	本公司有笔记本电脑移动设备，离开公司办公场所应进行控制，防止其被盗窃、未经授权的访问等危害的发生。	笔记本电脑在进入、离开规定的区域时，经过部门领导授权并对其进行严格控制，防止其丢失和未经授权的访问。	终端设备及介质使用管理规定
A.6.2.2	远程工作	控制	YES	宜实施策略和支持性安全措施来保护在远程站点访问，处理或存储的信息		网络访问控制策略

A.7 人力资源安全

标准条款号	标 题	目标/控制	是否选择	选择理由	控制描述	相关文件
A.7.1	任用之前	目标	YES	确保雇员、承包方人员理解其职责、考虑对其承担的角色是合适的		
A7.1.1	审查	控制	YES	通过人员考察，防止人员带来的信息安全风险。	负责对初始录用员工进行能力、信用考察，每年对关键信息安全岗位进行年度考察，对于不符合安全要求的不得录用或进行岗位调整。	人力资源管理制度
A.7.1.2	任用条款和条件	控制	YES	履行信息安全保密协议是雇佣人员的一个基本条件。	在《劳动合同》中明确规定保密的义务及违约的责任。	劳动合同 保密协议
A.7.2	任用中	控制	YES	确保所有的雇员和合同方意识到并履行其信息安全责任		
A.7.2.1	管理职责	控制	YES	缺乏管理职责，会使人员意识淡薄，从而对组织造成负面安全影响。	公司管理层要求员工、合作方以及第三方用户加强信息安全意识，依据建立的方针和程序来应用安全，服从公司管理，当有其他的管理制度与信息安全管理制度冲突时，首选信息安全管理制度执行。	人力资源管理制度
A.7.2.2	信息安全意识、教育和培训	控制	YES	安全意识及必要的信息系统操作技能培训是信息安全管理工作的前提。	与 ISMS 有关的所有员工，有关的物理访问者，应该接受安全意识、方针、程序的培训。方针、程序变更后应及时传达到全体员工。安全运营管理室通过组织实施《信息安全人员保密考察与审批管理程序》 ，确保员工安全意识的提高与有能力胜任所承担的信息安全工作。	人力资源管理制度
A.7.2.3	违规处理过程	控制	YES	对造成安全破坏的员工应该有一个正式的惩戒过程。	违背组织安全方针和程序的员工，公司将根据违反程度及造成的影响进行处罚，处罚在安全破坏经过证实的情况下进行。处罚的形式包括精神和物质两方面。	信息安全管理承诺
A.7.3	任用的终止或变化	目标	YES	宜将保护组织的利益融入到任用变化或终止的处理流程中。		
A.7.3.1	任用终止或变更的责任	控制	YES	执行工作终止或工作变化的职责应清晰的定义和分配。	在员工离职前和第三方用户完成合同时，应进行明确终止责任的沟通。再次沟通保密协议和重申是否有竞业禁止要求等。	劳动合同 网络访问控制策略 员工保密协议

A.8 资产管理

标准条款号	标 题	目标/控制	是否选择	选择理由	控制描述	相关文件
A.8.1	有关资产责任	目标	YES	实现和保持对组织资产的适当保护		
A.8.1.1	资产清单	控制	YES	公司需建立重要资产清单并实施保护。	组织各部门按业务流程识别所有信息资产。根据重要信息资产判断准则确定公司的重要信息资产，建立《重要信息资产清单》，并明确资产负责人。 当信息资产增添或报废时，组织资产使用部门对《重要信息资产清单》进行修订。	信息资产分级评定标准 信息资产清单
A.8.1.2	资产的所属关系	控制	YES	需要对所有的与信息处理设施有关的信息和资产指定责任人。	组织相关部门依据《信息安全风险管理程序》中的要求和方法识别资产并指定资产负责人，形成《信息资产清单》。	信息资产分级评定标准 信息资产清单
A.8.1.3	资产的可接受使用	控制	YES	识别与信息系统或服务相关的资产的合理使用规则，并将其文件化，予以实施。	制定相应的业务系统应用管理制度，重要设备有使用说明书，规定了资产的合理使用规则。使用或访问组织资产的员工、合作方以及第三方用户应该了解与信息处理设施和资源相关的信息和资产方面的限制。并对信息资源的使用，以及发生在其责任下的使用负责。 对于电子邮件和互联网的使用规则见本文件中的 A10.8 中的描述；	信息资产分级评定标准
A8.1.4	资产归还	目标	YES	所有员工、合作方以及第三方用户应该在聘用期限、合同或协议终止时归还所负责的所有资产。	员工离职或工作变动前，应办理资产归还手续，然后方能办理移交手续。	用户注册及注销规程
A.8.2	信息分级	目标	YES	确保信息受到与其对组织的重要性保持一致适当级别的保护		

A.8.2.1	信息分级	控制	YES	本公司的信息安全涉及信息的敏感性（包括来自顾客的要求），适当的分类控制是必要的。	不同密级事项的界定，由涉及秘密事项产生部门按照《信息分类及密级控制策略》规定的原则进行。	信息分类及密级控制策略
A.8.2.2	信息的标记	控制	YES	按分类方案进行标注	对于属于机密信息的文件（无论任何媒体），密级确定部门按《密级控制程序》里关于密级的要求进行适当的标注；公开信息不需要标注，其余均标注受控或机密。	信息分类及密级控制策略
A8.2.3	资产处理			规定信息处理的安全的要求。	信息的使用、传输、存储等处理活动按《信息分类及密级控制策略》等进行控制。	信息分类及密级控制策略
A.8.3	介质处置	目标	YES	防止存储在介质上的信息遭受未授权的泄露、修改、移动或销毁。		
A.8.3.1	移动介质的管理	控制	YES	本公司存在含有敏感信息的磁盘、磁带、光盘、打印报告等可移动媒体。	可移动计算媒体包括光盘、磁带、磁盘、盒式磁带和已经印刷好的报告，各部门按其管理权限并根据风险评估的结果对其实施有效的控制。 媒体移动的记录予以保持。	终端设备及介质使用管理规定
A.8.3.2	介质的处置	控制	YES	当介质不再需要时，必须对含有敏感信息的媒体（包括不良保密制品）采用安全的处置办法。	对于含有敏感信息或重要信息的介质在不需要或再使用时，介质处置部门按照的要求，采取安全可靠处置的方法将其信息清除。	终端设备及介质使用管理规定
A.8.3.3	物理介质转移	控制	YES	本公司存在如文件、技术资料等信息介质传送及保密制品的运输活动，确定安全的传送方法是必要的。	为避免被传送的介质在传送（运输）过程中发生丢失、未经授权的访问或毁坏，造成信息的泄露、不完整或不可用，负责介质（包括保密产品的运输）传送的部门采用以下方法进行控制： a) 选择适宜的安全传送方式，对保密产品运输供方进行选择与评价，并与之签订保密协议； b) 保持传送活动记录。	终端设备及介质使用管理规定

A.9 访问控制

A.9.1	访问控制的业务要求	目标	YES	限制信息与信息处理设施的访问		
A.9.1.1	访问控制策略	控制	YES	明确访问的业务要求，并符合信息安全方针的规定要求，对信息访问实施有效控制。	本公司基于以下原则制定文件化的访问控制策略，明确规定访问的控制要求，规定访问控制规则和每个用户或用户组的访问权力，访问规则的制定基于以下方面考虑： a) 每个业务应用的安全要求； b) 在不同系统与网络间，访问控制与信息分类策略要保持一致； c) 数据和服务访问符合有关法律和合同义务的要求； d) 对各种访问权限的实施管理。	网络访问控制策略
A9.1.2	网络和网络服务的访问	控制	YES	制定策略，明确用户访问网络和网络服务的范围，防止非授权的网络访问。	本公司建立并实施网络服务安全策略，以确保网络服务安全与服务质量。	网络访问控制策略
A．9.2	用户访问管理	目标	YES	确保授权用户访问系统和服务，并防止未授权的访问		
A.9.2.1	用户注册和注消	控制	YES	本公司存在多用户信息系统，应建立用户登记和解除登记程序。	根据访问控制策略确定的访问规则，访问权限管理部门对用户（包括第三方用户)进行书面访问授权，若发生以下情况，对其访问权将从系统中予以注销： a) 内部用户雇佣合同终止时； b) 内部用户因岗位调整不再需要此项访问服务时； c) 物理访问合同终止时； d) 其它情况必须注销时。	用户注册和注销规程
A9.2.2	用户访问提供	控制	YES	内部用户会发生岗位变化，或有的用户的访问权是有时限要求的，为防止非授权的访问，对用户访问的评审是必要的。	用户访问权限主管部门每半年对一般用户访问权进行评审，对特权用户每季度进行评审一次，注销非法用户或过期无效用户的访问权，评审结果应予以保持。	网络访问控制策略

A.9.2.3	特许访问权管理	控制	YES	本公司网络系统管理员拥有特权，特权不适当的使用会造成系统的破坏。	特权分配以“使用需要”（Need-to-use)和“事件紧跟”(Event-SK/event)为基础，即需要时仅以它们的功能角色的最低要求为据，有些特权在完成特定的任务后将被收回，确保特权拥有者的特权是工作所需要的且不存在多余的特权（最小特权原则)。 系统管理员，只有经过书面授权，其特权才被认可。 当特权拥有者因公出差或其它原因暂时离开工作岗位时，特权部门负责人应对特权实行紧急安排，将特权临时转交可靠人员，以保证系统正常运行；当特权拥有者返回工作岗位时，及时收回特权；特权的交接应有可靠安全的方法。	网络访问控制策略
A．9.2.4	用户的秘密鉴别信息管理	控制	YES	用户访问信息系统和服务是按授权的范围进行访问的，并拥有口令，因此建立正式的管理过程对口令进行分配并控制是必须的。	系统管理员按以下过程对被授权访问该系统的用户口令予以分配： a) 管理员根据入职员工的工作岗位分配相关临时口令。 b) 当用户忘记口令时，可由系统管理员帮其找回或重新分配安全的口令。 c) 禁止将口令以无保护的形式存储在计算机系统内。	网络访问控制策略
A.9.2.5	用户访问权的评审	控制	YES	内部用户会发生岗位变化，或有的用户的访问权是有时限要求的，为防止非授权的访问，对用户访问的评审是必要的。	用户访问权限主管部门每半年对一般用户访问权进行评审，对特权用户每季度进行评审一次，注销非法用户或过期无效用户的访问权，评审结果应予以保持。	网络访问控制策略
A9.2.6	访问权的移除或调整	控制	YES	所有是雇员和第三方人员对信息安全和信息处理设施的访问权应在任用、合同或协议终止时删除，或在变化时调整		
A.9.3	用户职责	目标	YES	确保用户对保护他们的鉴别信息负有责任		
A.9.3.1	秘密鉴别信息的使用	控制	YES	使用户遵循口令使用规则，防止口令泄密或被解密。	本公司明确规定了口令安全选择与使用要求，所有用户须严格遵守。 实施口令定期变更策略。	网络访问控制策略
A．9.4	系统和应用访问控制	目标	YES	防止对系统和应用的非授权访问。		

A．9.4.1	信息访问限制	控制	YES	为减少非授权访问的机会，对信息服务系统的访问采用安全登录过程。	本公司通过域登录等技术手段提供安全的系统登录过程。	网络访问控制策略
A.9.4.2	安全登陆规程	控制	YES	为追溯行为的个人责任，对连接到网络终端应有唯一的用户 ID。	用户有唯一的识别符（USER ID），以便用户单独使用时，能追溯行为的个人责任。用户 ID 由系统管理员根据授权的规定予以设置，用户识别符（USER ID）不在多个用户之间共享。 用户识别符（USER ID）可以由用户名称加口令或其它适宜方式组成。	网络访问控制策略
A.9.4.3	口令管理系统	控制	YES	为减少非法访问操作系统的机会，应建立口令管理系统。	公司部署实施口令管理，通过技术手段提供有效的、互动的设施以确保口令质量。除非一次性的口令系统，通过操作系统的强制措施要求用户定期变更口令。	《网络访问策略》 《口令控制策略》
A.9.4.4	特权实用程序的使用	控制	YES	对系统工具程序的使用应控制，防止恶意破坏系统安全。	应对系统工具程序（System Utility Program）的使用进行限制和严格控制，只有经过授权的系统管理员才可以使用系统工具程序，如漏洞扫描工具等。	《第三方访问策略》 《特权访问策略》
A9.4.5	程序源代码的访问控制	无	NO	无此项业务		不适用，删减

A.10 密码

标准条款号	标 题	目标/控制	是否选择	选择理由	控制描述	相关文件
A.10.1	密码控制	目标	YES	确保适当并有效的密码的使用来保护信息的保密性，真是性或完整性		
A.10.1.1	密码控制的使用策略	控制	YES	与外部信息交换过程需要有加密控制措施来保护信息的安全	识别需要采用加密保护的信息以及保护的手段，本公司在与外部信息交换过程中涉及的需用加密控制的信息有：客户从外部远程输送数据 ，针对此类信息与外部交换的过程应使用加密控制。	《口令控制策略》
A.10.1.2	秘钥管理	控制	YES	使用密钥来支持组织使用的加密技术	公司对识别的需要使用加密控制技术的信息，若在采用加密手段时要对密钥的使用进行管理	《口令控制策略》

A.11 物理和环境安全

标准条款号	标 题	目标/控制	是否选择	选择理由	控制描述	相关文件
A.11.1	安全区域	目标	YES	防止对组织信息和信息处理设施的未授权物料访问、损坏和干扰		
A.11.1.1	物理安全边界	控制	YES	定义物理安全边界来保护包含敏感或关键信息和信息处理设施的区域。	定义物理安全边界来保护包含敏感或关键信息和信息处理设施的区域。	物理访问策略
A.11.1.2	物理入口控制	控制	YES	安全区域进入应经过授权，未经授权的非法访问会对信息安全构成威胁。	外来人员进入公司区域要在前台进行登记。 第三方人员进入特别安全区域须被授权，进出有记录。 员工加班也需登记。	物理访问策略
A.11.1.3	办公室/房间和设施的安全保	控制	YES	对安全区域内的后勤管理部、房间和设施应有特殊	本公司为避免出现对办公室、房间和设施的未授权访问。对特别安全区域内的计算机和设施进行必要的控制，以防止火灾、	物理访问策略

	护			的安全要求。 当有紧急自然灾害发生，则需要提前示警。	盗窃或其它形式的危害，这些控制措施包括： a) 大楼配备有一定数量的消防设施； b) 房间装修符合消防安全的要求； c) 易燃、易爆物品严禁存放在安全区域内，并与安全区域保持一定的安全距离； d)房间无人时，应关紧窗户，锁好门；	
A.11.1.4	外部和环境威胁的安全保护	控制	YES	加强公司物理安全控制，防范火灾、水灾、地震，以及其它形式的自然或人为灾害。	公司设备具有防范火灾、水灾、雷击等自然、人为灾害的安全控制措施。	物理访问策略
A.11.1.5	在安全区域工作	控制	YES	在安全区域工作的人员只有严格遵守安全规则，才能保证安全区域安全。	处理敏感信息的设备不易被窥视。公司范围内禁止吸烟。 明确规定员工在有关安全区域工作的基本安全要求，并要求员工严格遵守。	物理访问策略
A.11.1.6	交接区	控制	YES	对特别安全区域，禁止外来人员直接进入传送物资是必要的。	公司外的送水人员、邮件快件投递人员、送货人员在送水、投递、送货送餐过程中，未经允许不得进入前台接待区以外的安全区域。	物理访问策略
A.11.2	设备	目标	YES	防止资产的损失、损坏、失窃或危机资产安全以组织的运营		
A.11.2.1	设备的安置和保护	控制	YES	设备存在火灾、吸烟、油污、未经授权访问等威胁。	设备使用部门负责对设备进行定置管理和保护。为降低来自环境威胁和危害的风险，减少未经授权的访问机会，特采取以下措施： a) 设备的定置，要考虑到尽可能减少对工作区不必要的访问； b) 对需要特别保护的设备加以隔离； c) 采取措施，以尽量降低盗窃、火灾、爆炸、吸烟、灰尘、震动、化学影响、电源干忧、电磁辐射等威胁造成的潜在的风险； d) 禁止在信息处理设施附近饮食、吸烟。	数据库安全策略
A.11.2.2	支持性设施	控制	YES	供电中断或异常会给信息系统造成影响，甚至影响正常的生产作业。	针对重要服务器及设备提供 ups，确保不间断供电，其他办公电脑和网络连接设备经风险评估可以接受供电中断的风险。	数据库安全策略

A.11.2.3	布缆的安全	控制	YES	通信电缆、光缆需要进行正常的维护，以防止侦听和损坏。	对传输线路进行维护，防止线路故障。 通信电缆与电力电缆分开铺设，防止干扰。	数据库安全策略
A.11.2.4	设备维护	控制	YES	设备保持良好的运行状态是保持信息的完整性及可用性的基础。	计算机信息网络系统设备及用户计算机终端（包括笔记本电脑）、各信息系统由工程部进行维护。	数据库安全策略
A.11.2.5	资产的移动	控制	YES	设备、信息、软件等重要信息资产未经授权的迁移会造成其丢失或非法访问的危害。	重要信息设备、保密信息的迁移应被授权，迁移活动应被记录。信息处理设施（网络设备及计算机终端）的迁移控制执行《网络和计算机策略》。	数据库安全策略
A.11.2.6	组织场所外的设备和资产安全	控制	YES	本公司有笔记本电脑移动设备，离开公司办公场所应进行控制，防止其被盗窃、未经授权的访问等危害的发生。	笔记本电脑在进入、离开规定的区域时，经过部门领导授权并对其进行严格控制，防止其丢失和未经授权的访问。	数据库安全策略
A.11.2.7	设备的安全处置或再利用	控制	YES	对本公司储存有关敏感信息的设备，如系统集成部的源代码，对其处置和再利用应将其信息清除。	含有敏感信息的设备在报废或改作他用时，由使用部门用安全的处置方法，将设备中存储的敏感信息清除并保存清除记录。	数据库安全策略
A.11.2.8	无人值守的用户设备	控制	YES	设备、信息、软件等重要信息资产未经授权的迁移会造成其丢失或非法访问的危害。	重要信息设备、保密信息的迁移应被授权，迁移活动应被记录。信息处理设施（网络设备及计算机终端）的迁移控制执行《网络和计算机策略》。	数据库安全策略
A.11.2.9	清空桌面和屏幕策略	控制	YES	不实行清除桌面或清除屏幕策略，会受到资产丢失、失窃或遭到非法访问的威胁。	本公司制定清除桌面、清除屏幕的策略并实施，各部门负责人负责监督。 各部门员工自觉履行该策略的日常实施。	信息安全策略

A.12 运行安全

标准 条款号	标 题	目标/ 控制	是否 选择	选择理由	控制描述	相关文件
A.12.1	运行规程和责任	目标	YES	确保正确、安全的操作信息处理设施。		
A.12.1.1	文件化操作程序	控制	YES	标准规定的文件化程序要求必须予以满足。	本公司按照信息安全方针的要求，建立并实施文件化的作业程序，文件化程序的控制执行《文件化信息管理制度》。	网络安全管理规定
A.12.1.2	变更管理	控制	YES	未加以控制的系统更改会造成系统故障和安全故障。	对信息处理设施、软件等方面的更改实施严格控制。在更改前评估更改所带来的潜在影响，正式更改前履行更改审批手续，并采取必要的措施确保不成功更改的恢复。	网络安全管理规定
A.12.1.3	容量管理	控制	YES	为避免因系统容量不足导致系统故障，必须监控容量需求并规划将来容量。	公司负责对信息网络系统的容量（CPU 利用率、内存和硬盘空间大小、传输线路带宽）需求进行监控，并对将来容量需求进行策划，适当时机进行容量扩充。	网络安全管理规定
A.12.1.4	开发、测试和运行设施分离	控制	YES	如果具有应用软件和测试程序的开发能力，开发与业务设施必须进行分离，以防止意外的系统的更改或未授权的访问。	在一个独立的测试环境中测试软件，并与业务设施分离。 操作系统管理员与用户分离。	网络安全管理规定
A.12.2	防范恶意软件	目标	YES	确保对信息和信息处理设施的保护，防止恶意软件		
A.12.2.1	控制恶意软件	控制	YES	恶意软件的威胁是客观存在的，特别是本公司许多电脑终端可以访问 Internet 互联网。	防范恶意软件宜基于恶意软件检测和修复软件、信息安全意识、适当的系统访问和变更管理控制。	网络安全管理规定

A.12.3	备份	目标	YES	防止数据丢失		
A.12.3.1	信息备份	控制	YES	必须对重要信息和软件定期备份，以防止信息和软件的丢失和不可用，及支持业务可持续性。		网络安全管理规定
A．12.4	日志和监视	目标	YES	记录事件并生成证据		
A.12.4.1	事态日志	控制	YES	为访问监测提供帮助，建立事件记录（审核日志）是必须		事件记录
A.12.4.2	日志信息的保护	控制	YES	日志记录设施以及日志信息应该被保护，防止被篡改和未经授权的访问。		事件记录
A.12.4.3	管理员和操作员日志	控制	YES	应记录系统管理员和系统操作员的活动。		事件记录
A.12.4.4	时钟同步	控制	YES	采取适当的措施实施时钟同步，是日常经营与获取客观证据的需要。		事件记录
A12.5	运行软件的控制	目标	YES	确保运行系统的完整性		
A12.5.1	运行系统软件安装	控制	YES	对软件在作业系统中的执行应予以控制，否则易受到未经授权的软件安装和更改的影响，导致系统及数据完整性丢失。	应对软件在作业系统的执行进行严格控制，在新软件安装或软件升级之前，应经主管部门负责人审核同意后方可进行。计算机终端用户除非授权，否则严禁私自安装任何软件。	网络安全管理规定
A12.6	技术脆弱性管理	目标	YES	防止技术脆弱性被利用		
A12.6.1	技术脆弱性管理	控制	YES	及时获得正在使用信息系统的技术脆弱性的相关信息，应评估对这些脆弱性的暴露程度，并采取适当的方法处理相关风险。	对技术脆弱性应进行风险评估，进行专项分析，制订风险处理计划，根据风险处理计划采取对应的技术和管理措施。	网络安全管理规定
A12.6.2	软件安装的限	控制	YES	应建立并实施用户安装软件控制的规则		

	制			
A12.7	信息系统审计考虑	目标	YES	将审计活动对运行系统的影响最小化
A12.7.2	信息系统审计控制	控制	YES	涉及对运行系统核查的审计要求和活动，应谨慎地加以规划并取得批准，以便最小化造成业务过程中断的风险

A.13 通信安全

标准条款号	标 题	目标/控制	是否选择	选择理由	控制描述	相关文件
A13	网络安全管理	目标	YES	确保对网络及信息处理设施中信息收到保护		
A13.1.1	网络控制	控制	YES	本公司已建立设计、制造应用系统和各种管理应用系统，网络结构简单，实施网络控制是必须的。	本公司网络安全控制措施包括： a)内外网物理隔离； b)专用网络与生产网络隔离；特定项目网络隔离； c)对网络设备定期维护； d)对防火墙、交换机等实施安全配置管理； e)对用户访问网络实施授权管理； f)实施有效的安全策略； g)对系统的变更进行严格控制； h)对网络的运行情况进行监控； i)对网络设备的变更进行控制； j)对网络系统管理与操作人员的管理。	网络安全管理规定
A13.1.2	网络服务的安全	控制	YES	明确规定网络服务安全属性是实施网络安全管理的需要。	公司根据组织的安全策略，识别现有的网络服务，由授权的系统管理员进行参数配置与维护管理。 选择资源良好的多家网络接入供应商。	网络安全管理规定
A13.1.3	网络的隔离	控制	YES	涉密网络（如研发）应予以隔离。	为确保本公司网络安全，采用物理和逻辑两种方式进行网络隔离：	网络安全管理规定

					a)通过防火墙将内部网络与外部网络实施逻辑隔离； b)专用网络与其他网络物理隔离。	
A13.2	信息传输	目标	YES	保持组织内以及与组织外信息传输的安全		
A13.2.1	信息交换策略和规程	控制	YES	应有正式的交换策略、规程和控制措施，以保护通过使用各类型通信设施的信息交换	可通过使用多种不同类型的通信设施进行信息传输，例如电子邮件、声音、传真和视频。 可通过多种不同类型的介质进行软件传输，包括从互联网下载和从出售现货的供应商处获得。 宜考虑与电子数据交换、电子商务、电子通信和控制要求相关的业务、法律和安全的含义。	通讯安全策略
A13.2.2	信息传输协议	控制	YES	应建立组织和外部各方之间的业务信息的安全传输协议	协议可以是电子的或手写的，并可采取正式合同或任用条款的形式。对保密信息而言，信息传输使用的特定机制对于所有组织和各种协议宜是一致的。	通讯安全策略
A13.2.3	电子消息发送	控制	YES	包含在电子消息发送中的信息应给予适当的保护	存在多种类型的电子消息发送，例如电子邮件、电子数据交换以及社交网络，在业务通信中扮演了一个角色。	通讯安全策略
A13.2.4	保密或不泄露协议	控制	YES	应识别、定期评审反应组织信息保护需要的保密性或不可泄露协议的要求，并将其形成文档	保密性和不泄密协议保护组织信息，并告知签署者以授权、负责的方式来保护、使用和披露信息的责任。 对于一个组织来说，可能需要在不同环境中使用保密性或不泄密协议的不同形式。	保密协议

A.14 信息系统获取、开发和维护

标准 条款号	标 题	目标/ 控制	是否 选择	选择理由	控制描述	相关文件
A.14.1	信息系统安全要求	目标	YES	确保信息安全成为信息系统生命周期的组成部份，包括向公共网络提供服务的信息系统的特定安全要求		

A.14.1.1	安全要求分析和说明	控制	YES	为确保系统具有一定的安全功能及规避开发过程的安全风险，增加新系统或扩大原有系统，应确定控制要求。	在进行新系统开发或系统更新时，首先对系统进行分析，根据业务功能要求及信息安全要求明确规定控制要求，包括： a) 系统的安全特性； b) 对现有的系统安全影响； c) 设计过程中的安全控制要求。 系统（软件）本身的功能及安全特性在设计开发输入时明确提出，并进行评审。	
A.14.1.2	公共网络上应用服务的安全保护	控制	YES	应保护在公共网络上的应用服务中的信息。	防止公共网上应用服务的信息未经收取的泄露和修改。	网络安全管理规程
A14.1.3	应用服务事务的保护	控制	YES	应用服务中的信息应受保护，以防止不完全传输、错误路由、未授权的信息篡改、未授权的泄露、未授权的信息复制或重放	为保护应用服务交易，对可能存在的应用服务进行控制。	网络安全管理规程
A14.2	开发和支持过程中的安全	目标	YES	确保应用系统软件和信息的安全。		信息安全策略
A.14.2.1	安全开发策略	控制	YES	对服务提供的更改进行管理，包括保持和改进现有的信息安全方针、程序和控制，要考虑业务系统的关键程度、所涉及的过程以及风险的再评估。	对第三方服务更改的管理过程需要考虑： a) 组织的更改，包括加强当前提供的服务，开发新应用程序和系统，修改和更新方针及程序，解决信息安全事件，提高安全性的新控制。 b) 第三方服务的更改，包括更改和加强网络，使用新技术，更改服务设施的物理位置，更改供应商。	信息安全策略
A.14.2.2	系统变更控制规程	控制	YES	为防止未授权或不充分的更改，避免系统故障与中断，需要实施严格更改控制。	为使信息系统的损害降至最小，对应用系统软件在开发过程中的任何更改，须进行适当的测试与评审，经开发软件负责人批准后予以实施。 操作系统（OS）及应用系统的升级须经过系统主管部门测试、评审与批准后方可进行。	信息安全策略
A.14.2.3	运行平台变更	控制	YES	操作系统的不充分更改对	当操作系统（OS）发生更改时，操作系统更改对应用系统的	信息安全策略

	后对应用技术的评审			应用系统会造成严重的影响。	影响应由工程部进行评审，确保对应用程序的作业或安全措施无不利影响。	
A.14.2.4	软件包变更限制	控制	YES	软件包的更改会引入脆弱性，导致内部控制故障，应进行严格限制。	本公司不鼓励修改软件包，如果有必要进行更改，更改部门在实施前进行风险评估，确定必须的控制措施，保留原始软件，并在完全一样的复制软件上进行更改，更改实施前须得到系统主管部门的授权。	
A.14.2.5	系统安全工程原则	控制	YES	工程安全系统原则被建立。形成文档，并应用到任何信息系统开发工作中	应用开发规程宜适用于具有输入输出接口的应用开发中的安全工程技术。安全工程技术提供了用户鉴别技术、安全会话控制和数据确认、调试代码的净化和消除方面的指南。	新安全策略
A.14.2.6	安全的开发环境	控制	YES	应在整个系统开发生命周期的系统开发和集成工作中，建立并适当保护开发环境的安全	安全的开发环境包括与系统开发和集成相关的人员、过程和技术。	信息安全策略
A.14.2.7	外包开发	删减				
A.14.2.8	系统安全测试	控制	YES	应进行安全功能测试		检查数据的检测与保护策略
A.14.2.9	系统验收测试	控制	YES	本公司存在建立新的信息系统、系统升级或使用新版本的活动，建立接受标准和在接受之前进行系统测试是必须的。	新系统、系统升级接收前，系统验收部门明确接收准则 ，经测试合格后方可正式运行，并保存测试记录及验收报告。	检查数据的检测与保护策略
A.14.3	测试数据	目标	YES	确保测试数据的安全		
A.14.3.1	测试数据的保护	控制	YES	对包括敏感作业数据的测试数据不适当的保护会涉及到保密性的破坏。	当系统测试数据使用作业数据，并且包含敏感信息时，测试部门按以下要求对测试数据进行保护： a) 对测试应用系统的活动进行授权； b) 作业信息每一次复制到测试应用系统，须被系统主管部门授权； c) 测试完成之后，立即从测试应用系统中消除作业信息。	检查数据的检测与保护策略

A.15 供应关系

标准条款号	标 题	目标/控制	是否选择	选择理由	控制描述	相关文件
A.15.1	供应商关系	目标	YES	确保组织中被供求商访问信息的安全		
A.15.1.1	供应商关系的信息安全策略	控制	YES	用于减轻供应商访问组织的资产相关风险的信息安全要求应形成文档并与供应商达成一致	信息安全管理不充分的供应商可使信息处于风险中。宜识别并应用控制来管理供应商对信息处理设施的访问。例如，如对信息的保密性有特殊需求，则可以使用非披露协议。另一个例子是当供应商协议涉及到跨国界的信息传送或访问时的数据保护风险，此时组织需要意识到其仍负有信息保护的法律或合同责任。	服务和供应品采购制度
A.15.1.2	在供应商协议中强调安全	控制	YES	应与每个可能访问、处理、存储组织信息，与组织进行通信或为组织提供 IT 基础设施组件的供应商建立并协商所有信息安全相关要求	不同组织和不同类型供应商的协议可能有很大不同。因此，宜注意包含所有相关的信息安全风险和要求。供应商协议也可能涉及其他方（如分包商）。 在协议中需要考虑当供应商不能提供产品或服务时的连续处理规程，以避免拖延安排替代产品或服务。	服务和供应品采购制度
A.15.1.3	信息和通信技术供应链	控制	YES	供应商协议应包括信息。通信技术服务和产品供应链的相关信息安全风险	特定的信息与通信技术供应链风险管理实践是建立一般的信息安全、质量、项目管理和系统工程实践之上，而不是替代它们。 建议组织与供应商合作，以知晓信息与通信技术供应链及对所提供产品和服务有重要影响的任何事宜。组织通过在与供应商的协议中明确在信息与通信技术供应链中宜由其他供应商解决的问题，可影响信息与通信技术供应链的信息安全实践。	服务和供应品采购制度
A.15.2	供应商服务交付管理	目标	YES	确保信息安全和服务交付水平与供应商协议保持一致 《第三方服务管理程序》		

A.15.2.1	供应商服务的监视和评审	控制	YES	组织应定期监视、评审、审计供应商服务交付	组织宜对供应商访问、处理或管理的敏感或关键信息或信息处理设施的所有安全方面保持充分的、全面的控制和可见性。组织宜保持安全活动的可见性，诸如管理变更、脆弱性识别、按照规定的报告过程进行的信息安全事件报告和响应等。	服务和供应品采购制度
A.15.2.2	供应商服务的变更管理	控制	YES	应管理供应商提供服务的变更，包括保持和改进现有的信息安全策略、规程和控制措施，并考虑到业务系统和涉及过程的关键程度及风险的再评估	供应商协议的变更； 组织做出的变更以实现： 供应商服务做出的变更以实现：	服务和供应品采购制度

A.16 信息安全事件管理

标准条款号	标 题	目标/控制	是否选择	选择理由	控制描述	相关文件
A.16.1	信息安全事件的管理和改进	目标	YES	确保对信息安全事件进行持续、有效地管理、包括信息安全事态和弱点的沟通		
A.16.1.1	责任和规程	控制	YES	建立管理责任和程序以保证对信息安全事件快速、有效和有序地做出响应。	安全运营管理室接到报告以后，应立即进行迅速、有效和有序的反应。	信息安全事件管理制度
A.16.1.2	报告信息安全事态	控制	YES	安全事件、事故有可能发生，一旦发生必须报告。	安全事情、事故一经发生，事情、事故发现者、事情、事故责任者应立即向安全运营管理室报告，责任部门应及时对事情、事故进行反应处理。所有员工有报告安全事情、事故的义务。	信息安全事件管理制度

A.16.1.3	报告信息安全弱点	控制	YES	安全脆弱性是不可避免的,建立报告制度是预防发生的最好途径之一。	各部门及全体员工应按照要求及时识别安全脆弱性及可能的安全威胁，一旦发现应及时向有关人员或部门报告并记录，信息小组或安全管理负责人应采取有效的预防措施，防止威胁的发生。	信息安全事件管理制度
A.16.1.4	信息安全事态评估与决策	目标	YES	保证应用于信息安全事件管理的方法的一致和有效。		
A.16.1.5	信息安全事件的响应	目标	YES	对信息安全事件进行响应。		
A.16.1.6	从信息安全事件中学习	控制	YES	只有对事故进行有效鉴定，才能从中吸取教训，防止再发生。	事故发生后，对事故发生的原因、类型、损失进行鉴定，提出防止此类事故再次发生的措施或建议，形成事故调查分析及处理报告，责成有关部门实施纠正措施。 事故和处理过程结果应予以记录，重大事故应提交安全运营管理室评审。	信息安全事件管理制度
A.16.1.7	证据的收集	控制	YES	当信息安全事件发生后对个人或组织的后续行为涉及到法律行为时，所提供的证据应符合相关的证据法规。	公司负责发生法律纠纷与诉讼的证据收集，并确保证据收集应符合以下要求： a) 所呈证据应符合国家有关的证据法规； b) 符合用于提供可接受证据的任何已发布的标准或法规； c) 对已收集到的证据进行安全的保管，防止未经授权的更改或破坏； d) 收集到的证据符合法庭所要求的形式。	信息安全事件管理制度

A.17 信息安全方面的业务连续性管理

标准条款号	标 题	目标/控制	是否选择	选择理由	控制描述	相关文件
A.17.1	信息安全连续	目标	YES	信息安全到的连续性应嵌入组织的业务连续性管理体系		

	性					
A.17.1.1	规划信息安全连续性	控制	YES	不同的业务持续性计划之间应保持一致性。	应保持独立的业务持续性计划的框架，以确定各种计划的一致性并确定检测和维护的优先权。	连续性管理办法
A.17.1.2	实现信息安全连续性	控制	YES	为确保本公司与设计、制造、销售、测试等关键业务中断能及时恢复，应编写并实施业务持续性计划。	组织各相关部门编制《业务持续性管理计划》，由信息安全管理者代表批准，以便在储存数据、培训、测试等关键业务发生中断或故障后，实施持续性管理计划，以保证公司关键业务中断的及时恢复。 持续性计划应对应急措施和有关部门与人员的职责给予明确规定。	连续性管理办法
A.17.1.3	验证/评审和评价信息安全连续性	控制	YES	为保持业务持续性计划的时效和有效性，应定期试验、维护和评审。	每年组织有关部门采取适宜的测试方法对《业务持续性管理计划》进行测试，并保持测试记录；每次测试后，工程部组织与计划有关的部门对计划的时效和有效性进行评审，必要时，对业务持续性计划进行修改。	连续性管理办法
A.17.2	冗余	目标	YES	确保信息处理设施的可用性		
A.17.2.1	信息处理设施的可用性	控制	YES	信息处理设施应具备足够的冗余，以满足可用性要求	组织宜识别信息系统可用性的业务要求。当使用现有系统架构不能保证可用性时，宜考虑冗余组件或架构。 如可能，宜测试冗余信息系统以确保从一个组件到另一个组件的故障切换按预期执行。	

A.18 符合性

标准条款号	标 题	目标/控制	是否选择	选择理由	控制描述	相关文件
A.18.1	符合法律与合	目标	YES	避免违反任何信息安全相关的法律、法令、法规或合同义务以及任何安全要素		

	同要求					
A.18.1.1	适用法律与合同的要求的识别	控制	YES	为遵守适用的相关法律法规，应对其进行识别并将其要求文件化。	组织收集与信息安全有关的法律法规并对适用性评价，确定其实用范围和具体适用条款，形成适用的法律法规清单，将法律法规一起通过网络传达给有关部门并予以执行。 每年应对法律法规的有效性进行重新评价，保持适用的法律、法规的有效最新版本。每年对法律法规的符合性进行评价。	合规义务和合规性评价管理制度
A.18.1.2	知识产权	控制	YES	软件的使用与复制涉及知识产权问题（软件著作权），应使用正版软件。	本公司严格执行国家有关知识产权方面的法律法规，保证使用合法的正版软件，并通过以下方法进行控制： a) 确定获得合法软件的途径； b) 每年进行一次软件资产清查，确保正在使用的软件已经被适当的授权； c) 保留许可证、手册等拥有者的证明和证件； d) 确保用户数不超过所允许的上限； e) 只允许安装认可的软件和特许的产品； f) 严禁员工私自安装任何软件。	合规义务和合规性评价管理制度
A.18.1.3	保护记录	控制	YES	记录的保持应符合法律法规要求。	各部门应按照有关法律、法规要求，明确规定重要记录的保存期限并提供适当的保护，防止丢失、损坏和伪造。	文件化信息管理制度
A.18.1.4	隐私和个人可识别信息的保护	控制	YES	应按国家有关法规或规章对员工的个人档案、养老基金账户等数据或信息进行管理与保护。	对处理与个人数据与信息有关的部门应按照国家有关规定对个人信息进行妥善管理与保护，防止丢失或泄露个人秘密。	公司管理制度
A.18.1.5	密码控制规则	控制	YES	与外部信息交换过程使用到加密控制措施	使用符合相关协议、法律和法规的要求和限制的加密控制措施	
A.18.2	信息安全的评审	目标	YES	确保信息安全依照组织策略和规程进行实施并运行		

A.18.2.1	信息安全的独立评审	控制	YES	对作业系统的审核应事先策划，避免对作业系统造成不良影响。	正式审核之前，审核组应明确技术性审核的项目与要求，防止审核活动本身造成不必要的安全风险。	内部审核管理制度
A.18.2.2	符合安全策略和标准	控制	YES	确保体系有效实施，定期评审是必须的。	每年安全运营管理室组织至少一次信息安全管理体系内部审核，每次审核的范围覆盖与信息安全管理体系有关的所有部门与安全区域，确保职责范围内的所有安全程序正确完成，符合安全方针和标准。	内部审核管理制度
A.18.2.3	技术符合性检查	控制	YES	为验证信息系统保证符合安全技术标准，必要的技术检查是需要的。	内部审核活动应包括对各信息系统的技术性审核，内部审核组至少拥有一名具有一定信息安全技术的内部专家，技术性审核应在被监督的情况下进行。 但不鼓励利用漏洞扫描等工具对网络系统进行定期技术性检查，鼓励用管理软件和自身的日志进行监督。	内部审核管理制度