



中国通信服务
CHINA COMSERVICE

2018年公司质量、环境、职业健康 安全、信息安全、信息技术服务 管理体系培训

项目管理部



公诚管理咨询有限公司
Gongcheng Management Consulting Co., Ltd.

一

公司管理体系介绍

二

新版三标一体化管理体系介绍

三

信息安全程序文件介绍

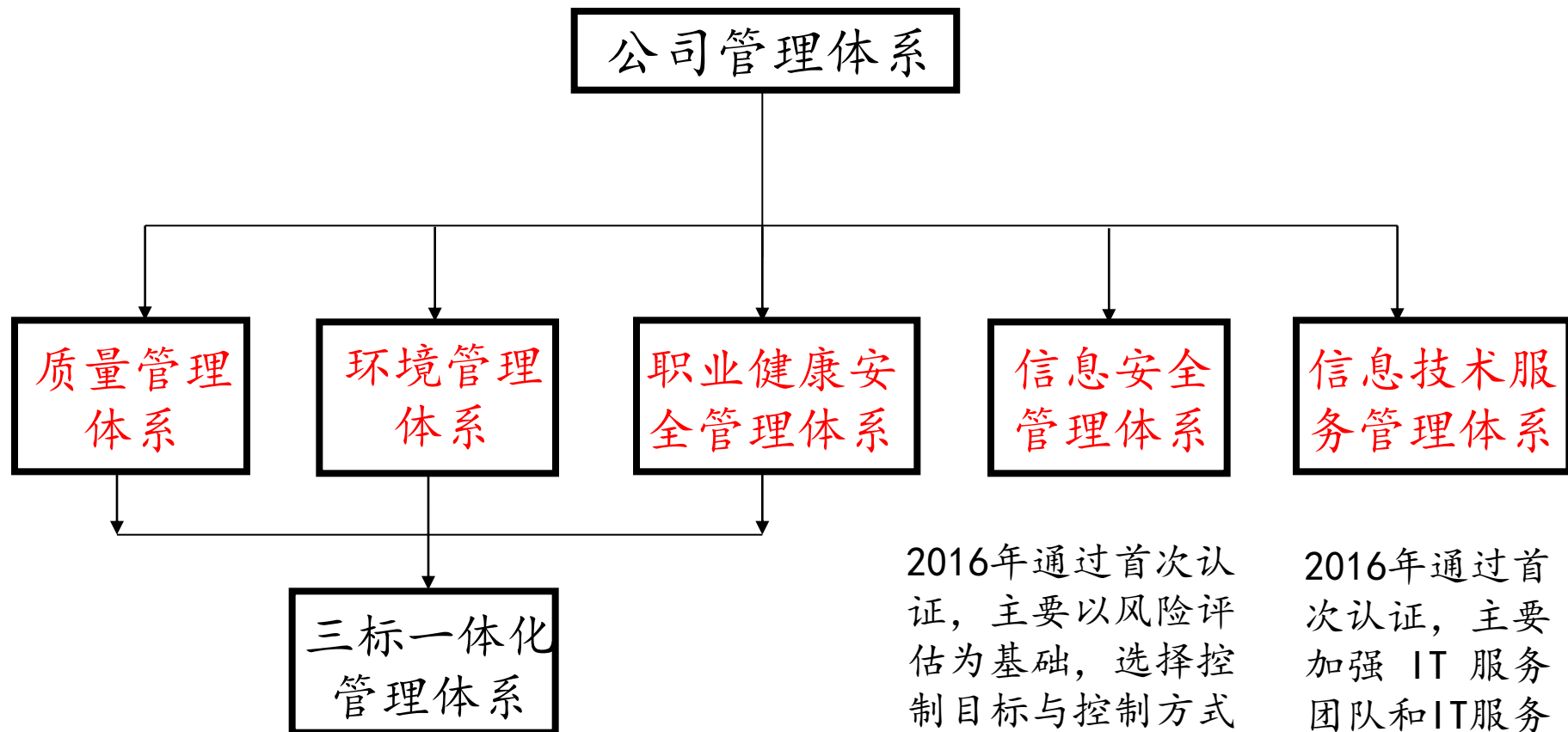
四

信息技术服务程序文件介绍

五

下阶段工作介绍

一、公司管理体系介绍



2012年合并并通过首次认证，体系主要针对企业对质量、环境和员工健康、安全方面的标准要求管理。

2016年通过首次认证，主要以风险评估为基础，选择控制目标与控制方式的信息安全管理体系。

2016年通过首次认证，主要加强 IT 服务团队和IT服务管理的管理体系。

一、公司管理体系介绍



质量管理体系
证书编号：
公诚管理

注册地址：广东省广州市天河区五山路246、
天河区天河北路423号远晖大厦9层F

根据贵组织的申请，本公
(GB/T19001-2016/ISO9001:2015)
特此发证，质量管理体系覆盖：

资质等级许可范围
工程造价咨询、招

首次发证日期：2010.4
证书换证日期：2017.4
证书有效期：2016.4

广东质检中
地址：中国广东省广州市海珠区
电话：020-8929233
网址：



环境管理体系
证书编号：
公诚管理

注册地址：广东省广州市天河区五山路246、
天河区天河北路423号远晖大厦9层F

根据贵组织的申请，本公
(GB/T24001-2016/ISO14001:2015)
特此发证，环境管理体系覆盖：

关于资质等级许可范围内
咨询、招标代理、企业管理
区域、作业

首次发证日期：2012.4
证书换证日期：2017.4
证书有效期：2015.4

广东质检中
地址：中国广东省广州市海珠区
电话：020-8929233
网址：



职业健康安全
证书编号：
公诚管理

注册地址：广东省广州市天河区五山路246、
天河区天河北路423号远晖大厦9层F

根据贵组织的申请，本公
(GB/T28001-2011) 规定实施
业健康安全管理体系覆盖范围：

关于资质等级许可范围内
咨询、招标代理、企业管理
区域、作业场所

首次发证日期：2012.4
证书换证日期：2017.4
证书有效期：2015.4

广东质检中
地址：中国广东省广州市海珠区
电话：020-8929233
网址：



信息安全

(正本)
兹证明

公诚管理咨询
统一社会信用代码：91440
注册地址：广州市天河区3
已按照
ISO/IEC 27001:201
标准要求建立并实施了信息安全
管理体系适用于

资质范围内的工程
招标代理、企业管
(适用性声明版本
涉及的场所及相关活动)

场所地址
广东省广州市天河区天
河北路105号远晖大厦
六楼、九楼(总部)
广东省广州市天河区天
河北路远晖大厦15-17
号附楼六楼二座

注册号：01217ISM0045R01
颁证日期：2017.01.13
有效期至：2020.01.12

广东质检中
地址：中国广东省广州市海珠区
电话：020-8929233
网址：



信息安全

(正本)
兹证明


公诚管理咨询
统一社会信用代码：91440
注册地址：广州市天河区3
已按照
ISO/IEC 27001:201
标准要求建立并实施了信息安全
管理体系适用于

资质范围内的工程
招标代理、企业管
(适用性声明版本
涉及的场所及相关活动)

场所地址
广东省广州市天河区天
河北路105号远晖大厦
六楼、九楼(总部)
广东省广州市天河区天
河北路远晖大厦15-17
号附楼六楼二座

注册号：0122017ISM008R0AIN
颁证日期：2017.01.16
有效期至：2020.01.15
换证日期：2017.04.28

广东质检中
地址：中国广东省广州市海珠区
电话：020-8929233
网址：



IT 服务管理体系认证证书

(正本)
兹证明

公诚管理咨询有限公司
统一社会信用代码：91440000721197608E
注册地址：广州市天河区五山路246、248、250号金山大厦801 自前807

已按照
ISO/IEC 20000-1:2011
标准要求建立并实施了IT 服务管理体系，
该管理体系适用于

信息系统工程监理、信息系统工程咨询、企业管理软件的运维服务

涉及的场所及相关活动：

场所地址	场所邮编	场所主要活动
广东省广州市天河区 天河北路105号远晖大厦 六楼、九楼(总部)	510610	企业管理软件的运维服务
广东省广州市天河区 天河东路广城街 15-17号附楼六楼二座	510620	信息系统工程监理、信息 系统工程咨询

广东质检中
地址：中国广东省广州市海珠区
电话：020-8929233
网址：



IT 服务管理体系认证证书

(正本)
兹证明

公诚管理咨询有限公司
统一社会信用代码：91440000721197608E
注册地址：广州市天河区五山路246、248、250号金山大厦801 自前807

已按照
ISO/IEC 20000-1:2011
标准要求建立并实施了IT 服务管理体系，
该管理体系适用于

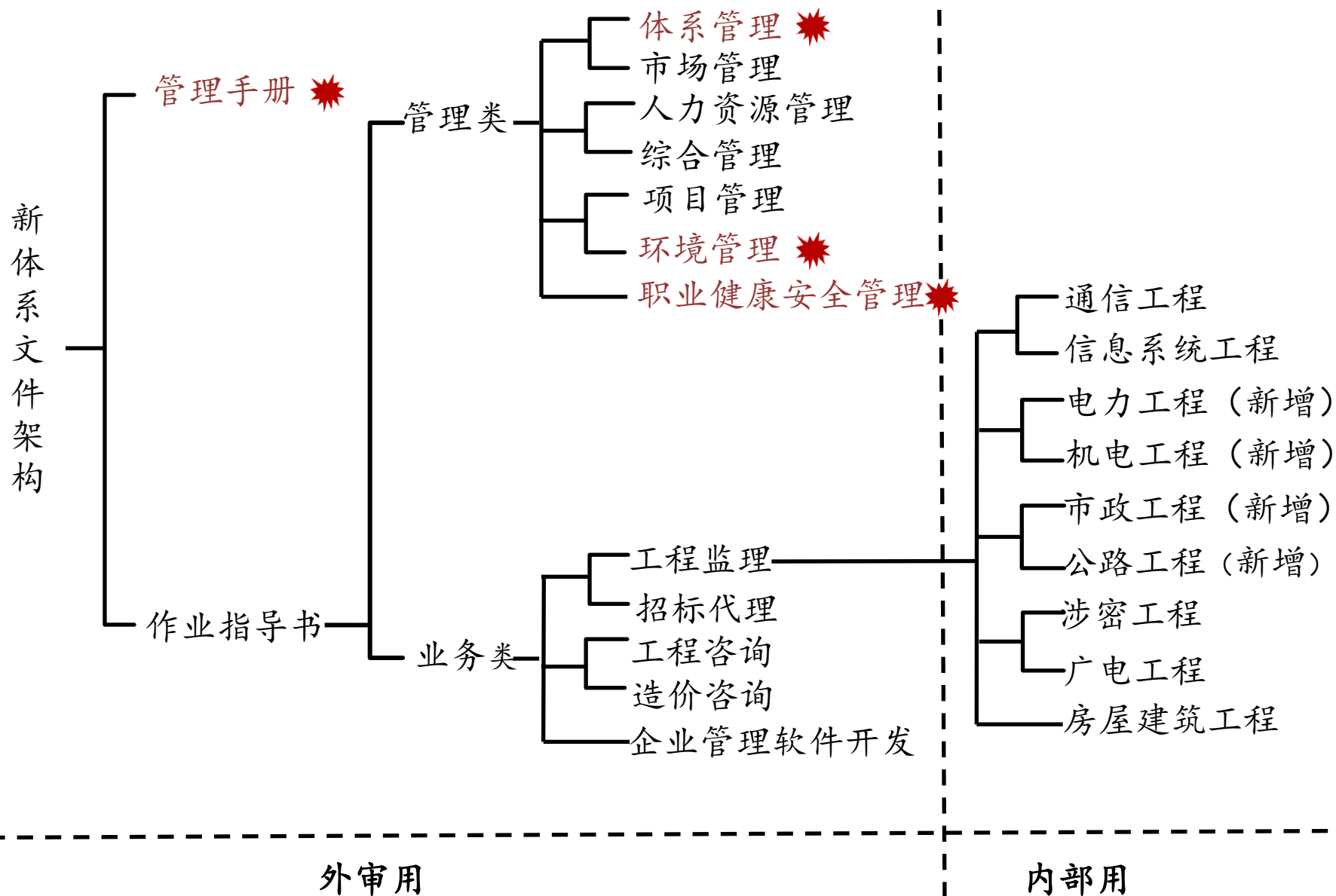
信息系统工程监理、信息系统工程咨询、企业管理软件的运维服务

涉及的场所及相关活动：

场所地址	场所邮编	场所主要活动
广东省广州市天河区 天河北路105号远晖大厦 六楼、九楼(总部)	510610	企业管理软件的运维服务
广东省广州市天河区 天河东路广城街 15-17号附楼六楼二座	510620	信息系统工程监理、信息 系统工程咨询

广东质检中
地址：中国广东省广州市海珠区
电话：020-8929233
网址：

二、新三标一体化管理体系介绍



二、新三标一体化管理体系介绍

第一层文件 管理手册

00

《管理手册》颁布令、任命书

《管理手册》颁布令和管理者代表的任命书。

03

策划

三点内容，分为风险与机遇的应对措施，目标及其实现的策划，管理体系变更策划。

06

监视、测量、分析和评价

三点内容，分为监视、测量、分析和评价，内部审核，管理评审。

01

管理体系概述

十点内容，分为体系适用范围，引用文件，术语和定语，文件组成，文件控制，记录控制，公司所处环境，相关方需求与期望，管理体系及其过程，法律法规及其他要求。

04

支持

五点内容，分为资源，能力，意识，沟通，形成文件的信息。

07

改进

两点内容，分为不合格和纠正措施，持续改进。

02

领导作用与员工的参与协商

五点内容，分为领导作用及其承诺，管理方针和目标，组织架构、岗位责任和权限，以顾客为关注焦点，信息交流、协商、参与和沟通。

05

运行

九点内容，分为运行的策划和控制，产品和服务的要求，设计和开发，外部提供的过程、产品和服务的控制，生产和服务的提供，产品和服务的放行，不合格输出的控制，环境与职业健康安全体系的运行策划与控制应急准备和响应。

08

职能分配表

对照表，针对体系中各组织机构对应规范的标准条款、公司管理手册中条款，按照责任部门和执行部门标识，便于对照。

二、新三标一体化管理体系介绍

认证覆盖范围

资质范围内工程监理、招标代理、工程咨询、造价咨询和企业管理软件开发。

覆盖人数：4160人。

覆盖组织机构：不包含分公司

体系文件架构

二级结构，一级管理手册、二级作业指导书，原程序文件已融入管理类作业指导书中。

管理手册

管理方针：精于执行、勤于改进、节能降耗、以人为本、打造和谐幸福企业；

质量目标：客户满意率：95%；

环境目标：办公和服务环境符合国家尘、毒、噪环境因素（源）保护标准要求；

杜绝重大环境污染。

职业健康安全目标：杜绝员工因公死亡、重伤事故。

二、新三标一体化管理体系介绍

第二层文件 体系管理作业指导书

附表《E-TX-01公司目标、指标、方案》
、《E-TX-02内审报告》
》、《E-TX-03管理评审报告》、
《E-TX-04事故、事件统计表》

第3章 体系运行管理

为了建立、健全符合公司运行和管理的
体系文件，保证公司体系运行健康，项
目管理部负责整个公司体系的运行管理

第1章 体系管理工作概述：

包括：公司标准体系认证有关的文件控制、监
督执行、内审组织等有关工作

第2章 目标、指标、方案管理：

为实现公司的管理方针，控制企业的重大危险源和重
要环境因素，制定职业健康安全和环境目标、指标，
为完成目标、指标而制定与实施相应的管理方案

二、新三标一体化管理体系介绍

归纳

第二层文件 体系管理作业指导书

- ◆ 建立符合标准条款、公司运行和管理的体系文件，每年维护体系文件在各组织机构内部的运行情况，每年采取内审、管理评审、第三方审核等措施监督体系的实施情况，不断改进；
- ◆ 各单位要按照体系文件规定的要求，根据工作职责，制定工作目标、指标和管理方案；
- ◆ 规定公司知识管理程序和要求。

二、新三标一体化管理体系介绍

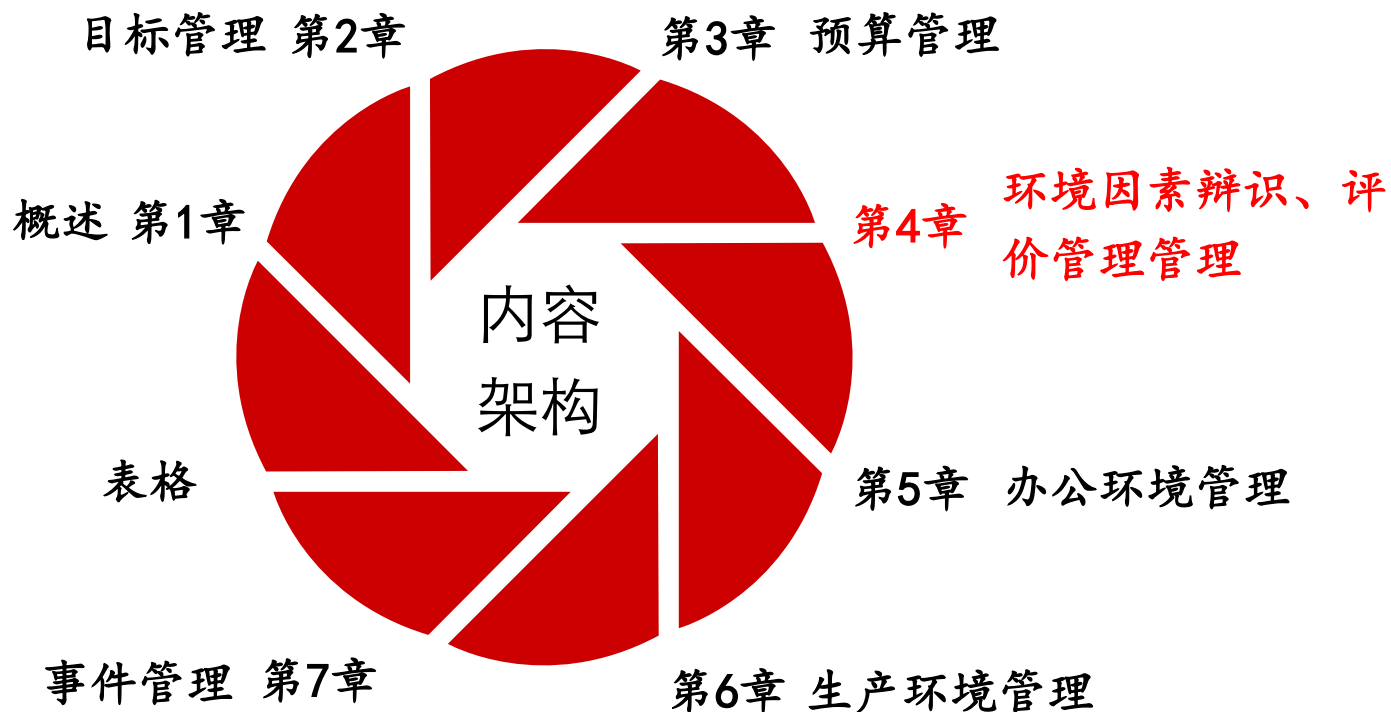
归纳

第二层文件 体系管理作业指导书

- ◆ 下发的纸质文件都是盖有“受控副本”印章，编号唯一。电子文件都是有单位水印的，文件的发放管理需要记录、受控；
- ◆ 所有体系文件中有编号的记录都受控，记录应及时填写(包括：名称、标识、编号、形成时间、记录内容、记录人、审核人等，电子或纸质 不强制要求)，做好归档；
- ◆ 各单位负责工作范围内的法律法规收集、合规性评价、绩效监测、测量、不合格控制、纠正和预防措施控制，知识管理等。

二、新三标一体化管理体系介绍

第二层文件 环境管理作业指导书



二、新三标一体化管理体系介绍

归纳

第二层文件 环境管理作业指导书

- ◆ 确定企业所在的环境范围，识别办公环境、生产环境，评价和确定重要环境因素，策划相应的控制措施，进行环境管控，做好环境保护；
- ◆ 对各种环境事件，制定应急预案和措施；
- ◆ 重要环境因素主要有固体废弃物、噪声、扬尘，污水、能源浪费，公司目前识别的环境重要因素有：

序号	环境因素	环境影响	涉及部门	控制方式
1	潜在火灾	产生大气污染	所有办公室职能部门和监理办公场所	专项应急预案、管理方案，定期开展应急演练管理
2	固体废弃物（含危废）的排放	产生大气污染	所有办公室职能部门和监理办公场所	管理方案

二、新三标一体化管理体系介绍

归纳

第二层文件 环境管理作业指导书

步骤一：如何识别环境因素

固体废物分类：

1、可回收利用无毒无害废弃物：废木材、废钢材、废弃的纸、箱、废金属等；

2、不可回收利用无毒无害废弃物：混凝土碎块、碎砖头瓦块、碎石材、生活垃圾、办公垃圾、生产垃圾等；

3、可回收有毒有害废弃物如：废油桶、废灭火器罐、废玻璃丝布、废铝箔纸。

4、不可回收有毒有害废弃物如：废打印墨盒、废磁盘、灭火器、日光灯管、计算器、废电池、废涂改液、变质过期的化学烯料、废涂料。

噪声排放指标未达到国标《声环境质量标准》和《社会生活环境噪声》要求的；
排放粉尘及有毒有害气体等污染物，排放的指标未达到《大气污染物综合排放标准》要求。

二、新三标一体化管理体系介绍

归纳

第二层文件 环境管理作业指导书

步骤二：如何评价环境因素

（一）识别环境因素时，采用以下两种方式：

- 1、过程分析法
- 2、现场观察法

（二）识别环境因素

各单位填写“环境因素调查表”，在识别环境因素时，应考虑环境因素的三种时态、三种状态和七种表现形式。

环境因素的三种时态：过去、现在、将来

环境因素的三种状态：

- 1、正常状态——正常的生活、生产、经营活动产生的环境影响；
- 2、异常状态——非例行作业状态，如设备的开机、停机、检修产生的环境影响；
- 3、紧急状态——可能发生的突发事件或事故，如火灾、洪水、地震、爆炸、环保设施突然失效等产生的环境影响。

二、新三标一体化管理体系介绍

归纳

第二层文件 环境管理作业指导书

步骤二：如何评价环境因素

（二）识别环境因素

环境因素的四种类别：

- 1、大气排放主要包括：粉尘、烟尘、有毒有害气体等；
- 2、废弃物主要包括：生产废物、生活垃圾、建筑垃圾和危险固体废弃物等；
- 3、噪声排放主要包括：机械设备、车辆等产生噪声对环境的影响；
- 4、能源、自然资源和原材料的消耗主要包括：生产中原材料和能源、自然资源（煤、电、油、气、水）的使用和消耗等；

（四）环境因素的评价方法

各单位汇总“环境因素调查表”，对环境因素逐项进行评价，填写“环境因素评价表”，对于环境因素类型（粉尘、噪声、废弃物、能资源等），可根据以下公式进行评价： $\Sigma = a+b+c+d+e$ （ Σ —环境因素总分） a —合规性、 b —发生频率、 c —影响范围、 d —影响程度、 e —社区关注程度

二、新三标一体化管理体系介绍

归纳

第二层文件 环境管理作业指导书

步骤三：确定重要环境因素和优先等级

根据环境因素评价等值 Σ ，判断重要环境因素优先等级，填写“重要环境因素清单”。

分 数 值	重要环境因素优先等级
$\Sigma > 20$	高度优先
$\Sigma = 18$	中度优先
$\Sigma = 15$	低度优先

步骤四：对公司自身产生的重要环境因素，应根据其程度策划相应的控制措施。

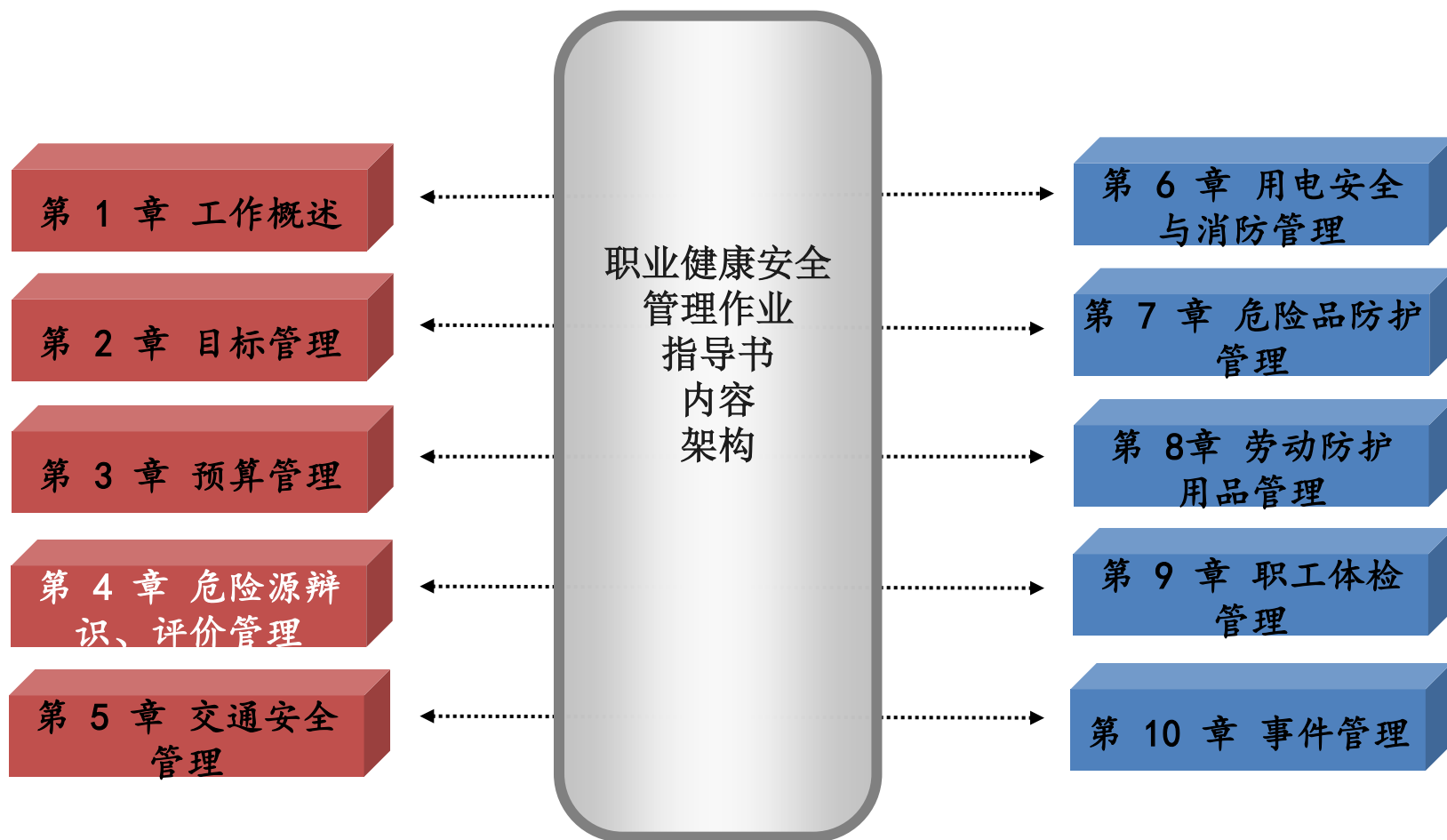
（一）高度优先的重要环境因素，制定环境目标、指标和管理方案进行控制。

（二）中度优先、低度优先的重要环境因素，应根据其具体情况决定。

（三）对于相关方活动中产生的重要环境因素，应采取施加影响的方式进行间接控制。

二、新三标一体化管理体系介绍

第二层文件 职业健康安全管理作业指导书



二、新三标一体化管理体系介绍

归纳

第二层文件 职业健康安全管理作业指导书

- ◆ 让每个员工参与到职业健康安全管理体系中，能够辨识危险源、评估风险，主动生产采取相应控制措施，进行安全风险防范，正确应对事件的发生，降低员工和企业所面临的风险；
- ◆ 对各种安全事件，制定应急预案和措施；
- ◆ 职业健康安全重要危险因素主要有物体打击、机械伤害、高处坠落、中毒，触电、火灾、职业病等等，公司目前识别的重要危险因素有：

序号	活动/设施/场所	危险源	可能导致的危害	涉及部门	控制方式
1	办公室区域活动、 监理现场	触电	触电造成人身伤害	所有办公室职能部门和生产部门	制定专项应急预案、管理方案，定期开展应急演练管理
2	办公室区域活动、 监理现场	潜在火灾	火灾引起人身伤害	所有办公室职能部门和生产部门	制定专项应急预案、管理方案，定期开展应急演练管理
3	监理现场	高空坠落	高空坠落造成人身伤害	所有生产部门	使用劳动防护用品，制定专项应急预案、管理方案
4	监理现场	物体打击	造成人身伤害	所有生产部门	使用劳动防护用品，制定专项应急预案、管理方案

二、新三标一体化管理体系介绍

归纳

第二层文件 职业健康安全管理作业指导书

步骤一：如何识别危险源识别

（一）辨识危害因素范围应包括：

- 1、常规和非常规活动；
- 2、所有进入作业场所人员的活动；
- 3、作业场所的地理位置及环境、设施。

（二）危害因素辨识的要求

在进行危害因素辨识时，应考虑三种时态（过去、现在、将来）、三种状态（正常、异常、紧急）。

二、新三标一体化管理体系介绍

归纳

第二层文件 职业健康安全管理作业指导书

步骤一：如何识别危险源识别

(三) 危害因素辨识的方法

- 1、项目管理部对公司作业活动按部门分解。
- 2、各部门由具备管理经验、熟悉工作流程的人员组成危害因素调查小组，对业务范围内的危害因素进行辨识。
- 3、调查小组针对某项具体的作业活动，对照国家《生产过程危险和危害因素分类与代码》和《企业职工伤亡事故分类》，确定本项作业活动中的危害因素，填入“危害因素调查表”，反馈到项目管理部。
- 4、新建项目应由项目负责部门组织本项目的危害因素辨识，填写“危害因素调查表”，反馈到项目管理部。

二、新三标一体化管理体系介绍

归纳

第二层文件 职业健康安全管理作业指导书

步骤二：风险评价

5、项目管理部对“危害因素调查表”进行汇总，组织对危害因素逐项进行评价，填写“危害因素评价表”。

（四）危害因素评价方法

1、采用工作条件危险性评价法对危害因素进行评价。

2、评价公式： $D=L \times E \times C$ ，式中： D —危害因素总分； L —发生事故的可能性大小； E —人体暴露在危险环境中的频繁程度； C —发生事故造成的后果。 L 、 E 、 C 三种因素分值。

（五）确定风险等级

求出 D 值后，按附表确定风险等级，1、2级为不可接受的危害；3级为不希望接受的危害；4级为可控制的接受；5级为可接受。

二、新三标一体化管理体系介绍

归纳

第二层文件 职业健康安全管理作业指导书

步骤三：确定重要危害因素

(一) 凡具备下列条件之一的，应定为重要危害因素：

- 1、当 $D \geq 100$ 且无有效防护措施的；
- 2、不符合法律法规和其它要求中硬性指标的，如：有毒有害气体浓度、粉尘浓度、噪声等级等；
- 3、直接观察到的可能导致事故的危险且无控制措施；
- 4、曾经发生过事故仍未采取有效措施。

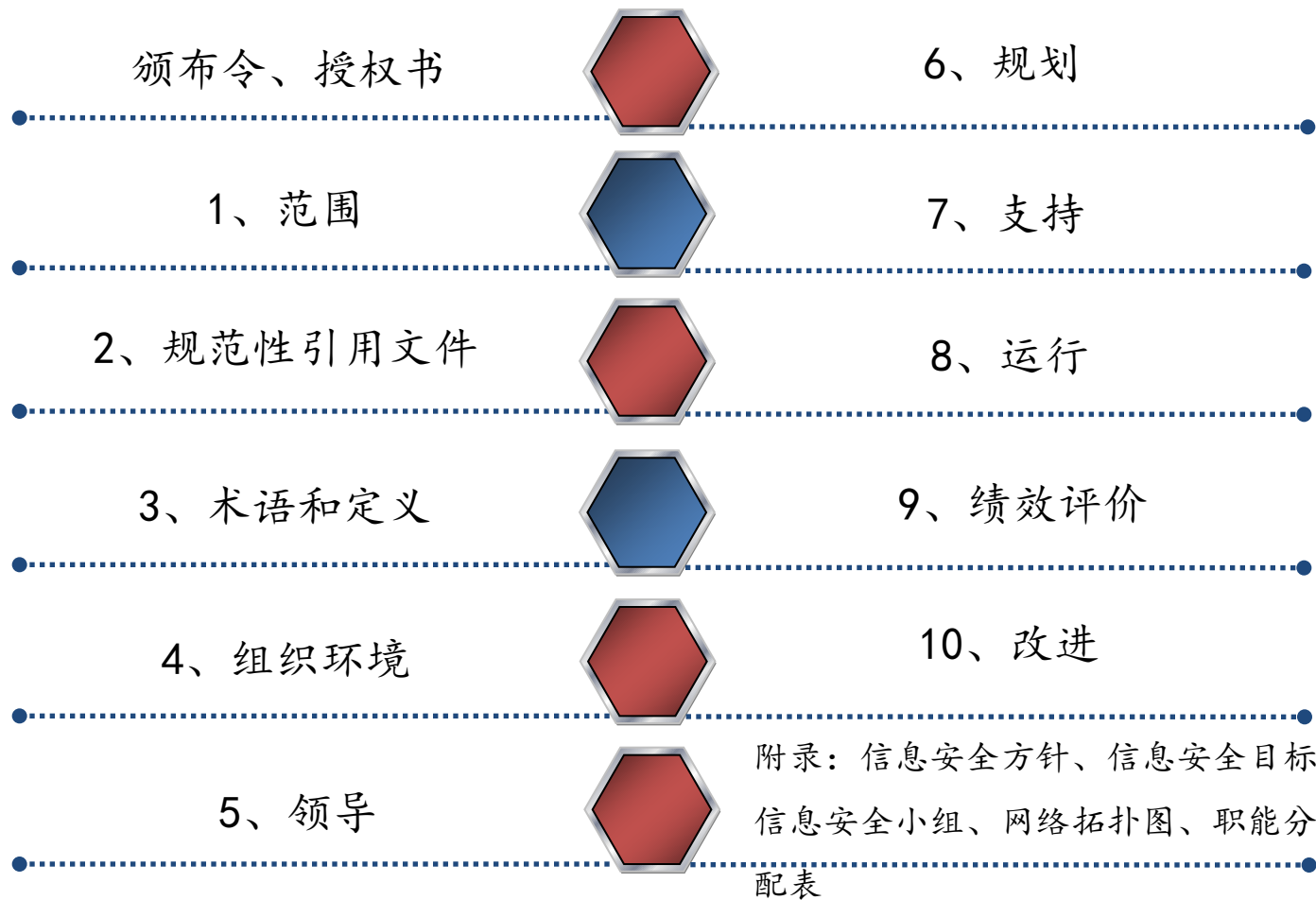
(二) 项目管理部根据评价结果，编制公司“重要危害因素清单”，报管理者代表批准后，发至各部门。

步骤四：重要危害因素控制

- (一) 公司针对不同的风险等级，策划相应的控制措施。
- (二) 制定职业健康安全目标、指标和管理方案。
- (三) 对风险等级高的重要危害因素，制定职业健康安全目标、指标和管理方案进行控制。

三、信息安全管理体系介绍

第一层文件 管理手册



三、信息安全管理体系介绍

认证覆盖范围

资质范围内工程监理、工程咨询、工程造价咨询、招标代理、企业管理软件开发服务的信息安全管理。

覆盖人数：2000人。（全员）

覆盖组织机构：不包含分公司

体系文件架构

一级文件：信息安全管理手册及适用性申明

二级文件：程序文件（37篇程序文件）

三级文件：作业指导书（含质量管理体系中业务类作业指导书）

四级文件：记录表格

管理手册

信息安全方针：预防为主，共筑信息安全；完善管理，赢得顾客信赖。

信息安全目标：无重大信息安全事件发生；实现信息资产无破坏零损失；确保业务系统持续可靠运行。

成立虚拟信息安全小组，由信息安全领导小组、管理者代表、工作小组组成。

三、信息安全管理体系介绍

第一层文件：管理手册和适用性申明

信息安全小组

(1) 信息安全领导小组成员：

组长：许勇飞

副组长：谭文涛、林团平、罗志勇、陈伟峰

成员：各部门负责人

(2) 信息安全管理者代表：林团平

(3) 信息安全工作小组成员：

信息安全工作小组组长：林团平

信息安全工作小组副组长：梁远忠、陈敬源

信息安全工作小组成员：陈敬源、任晶、简智斌、杜素青、夏锦涛、敖结兰、陆一峰、巫克纯、梁耀华、张科胜、陈子庭

三、信息安全管理體系介紹

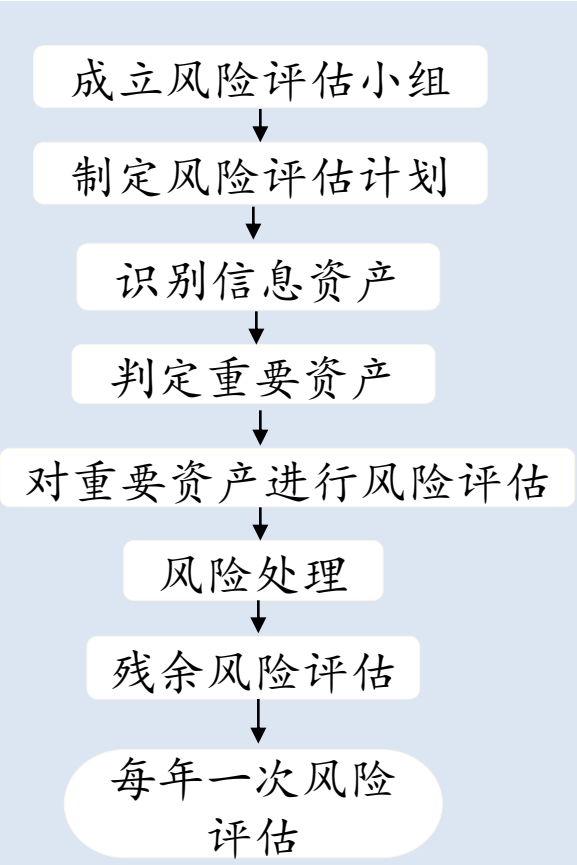
第二層文件 程序文件

GCMC-ISMS-02-01 文件、記錄管理控制程序	GCMC-ISMS-02-14 惡意軟件控制程序	GCMC-ISMS-02-27 信息安全溝通控制程序
GCMC-ISMS-02-02 管理評審控制程序	GCMC-ISMS-02-15 信息備份控制程序	GCMC-ISMS-02-28 信息安全法律法規控制程序
GCMC-ISMS-02-03 內部審核控制程序	GCMC-ISMS-02-16 容量管理控制程序	GCMC-ISMS-02-29 信息資產安全控制程序
GCMC-ISMS-02-04 糾正措施控制程序	GCMC-ISMS-02-17 機房安全控制程序	GCMC-ISMS-02-30 信息系統開發控制程序
GCMC-ISMS-02-05 信息安全風險評估控制程序	GCMC-ISMS-02-18 物理訪問控制程序	GCMC-ISMS-02-31 信息系統接收控制程序
GCMC-ISMS-02-06 信息安全度量控制程序	GCMC-ISMS-02-19 網站信息發布控制程序	GCMC-ISMS-02-32 信息系統變更控制程序
GCMC-ISMS-02-07 員工聘用控制程序	GCMC-ISMS-02-20 信息處理設施安裝使用控制程序	GCMC-ISMS-02-33 信息系統監控控制程序
GCMC-ISMS-02-08 員工培訓控制程序	GCMC-ISMS-02-21 信息處理設施維護控制程序	GCMC-ISMS-02-34 工程監理控制程序
GCMC-ISMS-02-09 員工離職控制程序	GCMC-ISMS-02-22 網絡設備安全配置控制程序	GCMC-ISMS-02-35 招標代理服務控制程序
GCMC-ISMS-02-10 用戶訪問控制程序	GCMC-ISMS-02-23 第三方服務控制程序	GCMC-ISMS-02-36 項目管理諮詢服務控制程序
GCMC-ISMS-02-11 計算機控制程序	GCMC-ISMS-02-24 業務持續性控制程序	GCMC-ISMS-02-37 造價諮詢服務控制程序
GCMC-ISMS-02-12 可移動介質控制程序	GCMC-ISMS-02-25 信息安全事件控制程序	
GCMC-ISMS-02-13 電子郵件控制程序	GCMC-ISMS-02-26 信息安全獎懲控制程序	

三、信息安全管理體系介紹

風險評估

GCMC-ISMS-02-05 信息安全風險評估控制程序

流程	說明	文檔
 <pre>graph TD; A[成立風險評估小組] --> B[制定風險評估計劃]; B --> C[識別信息資產]; C --> D[判定重要資產]; D --> E[對重要資產進行風險評估]; E --> F[風險處理]; F --> G[殘余風險評估]; G --> H[每年一次風險評估];</pre>	<p>1、信息安全工作小組協同項目管理部，牽頭成立風險評估小組，制定風險評估計劃；</p> <p>2、風險評估小組成員識別各部門資產，進行資產賦值，針對對資產自身價值、資產分類、保密性、完整性、可用性和法律法規合同符合性進行分析；資產分類：人員、無形資產（安全區域）、有形資產；</p> <p>3、根據資產賦值判定重要資產，風險賦值分為3級，級別越高表示資產重要性程度越高；</p> <p>4、對重要資產的威脅性、脆弱性進行風險評估，計算出風險等級，風險等級分為3級，等級3為高風險，為不可接受的風險。</p> <p>5、對風險應進行處理，對可接受風險，可保持已有的安全措施；如果是不可接受風險，則需要採取安全措施以降低、控制風險；</p> <p>6、對採取安全措施處理後的風險，信息安全小組應對其進行再評估，以判斷實施安全措施後的殘余風險是否已經降低到可接受的水平。</p> <p>7、每年對信息安全風險重新評估一次，有特殊情况需及時進行風險評估。</p>	<p>1、《風險評估計劃》</p> <p>2、《資產識別清單》</p> <p>3、《風險評估表》</p> <p>4、《風險處理計劃》</p> <p>5、《風險評估報告》</p> <p>6、《殘余風險評估報告》</p>

三、信息安全管理体系介绍

信息资产

GCMC-ISMS-02-29 信息资产安全控制程序

一、信息资产定义：公司信息安全所保护的有价值的任何事物，以多种形式存在，公司对信息资产进行科学识别，以便于进行信息资产的管理。

二、公司的信息资产分类：人员【（1）部门负责人、（2）关键岗位人员、（3）非关键岗位人员】、有形资产【固定资产、低值易耗品（携带信息）、文档（合同、项目资料、法律法规）】、无形资产【软件、知识产权、数据（电子）、安全区域】。

三、信息安全管理體系介紹

信息资产保护策略表

GCMC-ISMS-02-29 信息资产安全控制程序

	保密事项	内部公开事项	公开事项
标注	文件资料类（纸质或电子版文件），在封面或首页的右上角标明密级和保密期限；非文件资料类，在载体的包装或明显处标明密级和保密期限	公司制度程序类文件需标识为“内部公开”。各部门所使用的表格表单默认为内部公开使用。	公司宣传类资料、公司资质等对外发布文件无需标识。
授权	需要得到公诚咨询相关负责人批准	需要得到资产直接责任人同意	无特别要求
访问	只能被得到授权的人员访问，调阅使用应有记录	可以被公诚咨询员工访问，外部相关人员可以在签署保密协议/条款的前提下访问	可以被公诚咨询员工或外部相关人员访问
存储	电子文件在不加密的状态下存储在访问受控的环境中；纸质文件应锁在带锁的柜子中；其他资产应放置于风险受控的环境内	电子文件应妥善保管；纸质文件不应放在可以随意获取的地方	应恰当保管，避免被无关人员访问，避免丢失
复制	可以在得到授权的情况下复制，复制件视同原件管理，保留复制记录	经授权后可以复制，复制件视同原件管理	无限制
打印	可以在得到授权的情况下打印，打印件视同原件管理，保留打印记录	经授权后可以打印，打印件视同原件妥善保管	无限制
邮件	可以在得到授权的情况下使用内部邮件系统发送，文件需配置密码并保留发送记录	经授权后可以通过内部邮件系统发送	无限制，可以使用外部邮件系统发送
传真	禁止传真	经授权后可以传真	无限制
邮递	经授权后可以由指定机构邮递，保留邮寄记录	经授权后可以由指定机构邮递	无限制
内部分发	在生成分发过程中应严格管理，核定份数，统一编号，登记分发	经授权后可以在内部分发	无限制
对外分发	经授权后分发，需签署保密协议（不包括有权机构）并保留分发记录	经授权可以对外分发，需签署保密协议	无限制
销毁	由指定部门负责集中销毁；所有销毁结果需检查确认，保留销毁记录	文件和数据资产由信息资产使用人负责销毁；其他资产由指定部门负责集中销毁	无限制
记录	保留信息资产的全部处理记录	无限制	无限制

三、信息安全管理體系介紹

數據流轉區域控制表

GCMC-ISMS-02-29 信息資產安全控制程序

流轉區域		保密性		
		保密事項	內部公開事項	公開事項
外部區域	互聯網絡	×	×	√
	外部郵件系統	×	×	√
	筆記本計算機（個人使用）	×	√	√
	一般介質（個人使用）	×	√	√
研發開發區	辦公網絡	√	√	√
	內部郵件系統	√	√	√
	台式計算機/辦公服務器	√	√	√
辦公區	辦公網絡	√	√	√
	內部郵件系統	√	√	√
	台式計算機/辦公服務器	√	√	√
機房區	辦公網絡	√	√	√
	辦公服務器	√	√	√
	辦公操作終端	√	√	√

注：保密事項在辦公環境下流轉，可以在得到授權的情況下使用內部郵件系統發送，文件需配置密碼并保留發送記錄。

三、信息安全管理体制介绍

信息安全事件

GCMC-ISMS-02-25 信息安全事件控制程序

一、信息设备故障、线路故障、软件故障、恶意软件危害、人员故意破坏或工作失职等原因直接造成下列影响（后果）之一，均为信息安全事件：

- a) 企业内部公开事项泄露或丢失；
- b) 造成信息资产损失的火灾、洪水、雷击等灾害；
- c) 损失在五万元以上的故障/事件。

二、信息设备故障、线路故障、软件故障、恶意软件危害、人员故意破坏或工作失职等原因直接造成下列影响（后果）之一，属于重大信息安全事件：

- a) 企业保密事项信息泄露；
- b) 造成机房设备毁灭的火灾、洪水、雷击等灾害；
- c) 损失在十万元以上的故障/事件。

三、信息安全管理体系介绍

信息安全事件

GCMC-ISMS-02-25 信息安全事件控制程序

三、事件、安全薄弱点报告要求

事件、安全薄弱点的发现者应按照以下要求履行报告任务：

a) 各个信息管理系统使用者，在使用过程中如果发现软硬件故障、事件、安全薄弱点，应该向该系统归口管理部门和信息安全小组报告；如故障、事件会影响或已经影响线上生产，必须立即报告相关部门，采取必要措施，保证对生产的影响降至最低；

b) 发生火灾应立即触发火警并向信息安全小组报告，启动消防应急预案；

c) 涉及企业保密事项泄露、丢失应向信息安全小组报告；

d) 发生重大信息安全事件，事件受理部门应向信息安全管理者代表和总经理报告。

四、事件的响应

事件处理部门接到报告以后，应立即进行迅速、有效和有序的响应，包括采取以下适当措施：

a) 报告者应保护好故障、事件的现场，并采取适当的应急措施，防止事态的进一步扩大；

b) 按照有关的事件处理文件（程序、作业手册）排除故障，恢复系统或服务，必要时，启动业务持续性管理计划。

三、信息安全管理體系介紹

第三層文件 作業指導書文件

GCMC-ISMS-03-01 信息安全管理體系組織及職責管理策略	GCMC-ISMS-03-10 即時通訊工具使用管理規定
GCMC-ISMS-03-02 信息安全策略	GCMC-ISMS-03-11 項目信息安全風險管理規定
GCMC-ISMS-03-03 防病毒策略	GCMC-ISMS-03-12 數據加密管理規定
GCMC-ISMS-03-04 網絡通信安全策略	GCMC-ISMS-03-13 工程監理作業指導書
GCMC-ISMS-03-05 業務持續性管理策略	GCMC-ISMS-03-14 工程造價諮詢作業指導書
GCMC-ISMS-03-06 審計策略	GCMC-ISMS-03-15 工程諮詢作業指導書
GCMC-ISMS-03-07 員工信息安全管理規定	GCMC-ISMS-03-16 企業管理軟件開發作業指導書
GCMC-ISMS-03-08 移動媒體介質銷毀管理規定	GCMC-ISMS-03-17 招標代理作業指導書
GCMC-ISMS-03-09 辦公通訊設施管理規定	

三、信息安全管理體系介紹

員工信息安全管理制度

GCMC-ISMS-03-07 員工信息安全管理制度

一、桌面系統使用規範

(一) 公司全體員工必須使用正版軟件。使使用的基础軟件必須使用公司統一提供的安裝介質或軟件包，而不能非法安裝盜版系統軟件。不得將個人辦公機器設置成服務器，因工作性質有特殊需求的，則應在經過綜合部批准、備案後使用。如無特殊需要，員工不應在辦公桌面計算機上設置共享文件夾。如必須設置時，應設置保護口令、只讀權限等安全措施，並在共享完成後及時取消共享。

(二) 嚴格禁止在桌面辦公設備上安裝或使用對公司信息安全造成威脅、非法獲取公司或他人信息的、帶有攻擊性的各類軟件。

(三) 員工對於自己所使用的桌面辦公系統的安全承擔最終責任，除非有特殊情况，否則不應授權他人使用自己的桌面辦公系統。

二、口令使用規範

員工在設定系統或網絡登陸口令時，應選擇至少6位數以上口令，口令要求具有一定複雜度的字母數據組合。應盡量避免將口令書寫在紙面上或是存放在電子文檔之中，不應將記錄有口令信息的載體任意放置在工作區域。禁止員工在使用終端系統時使用任何形式的“自動保存口令”功能。

三、病毒防護和可移動代碼管理規範

員工在日常工作中必須保證安全軟件的正常運轉，並確保安全軟件及時升級和更新。

四、電子郵件使用規範

三、信息安全管理體系介紹

員工信息安全管理制度

GCMC-ISMS-03-07 員工信息安全管理制度

五、保密信息使用规范

(一) 员工办公桌面禁止摆放带有保密信息的文件，员工日常的含有保密信息的文件应当妥善保管在各人的抽屉中，并加锁保护。

(二) 敏感或重要信息打印、复印、传真后应立即拿走。

(三) 不得在公共、私下等非工作需要的场所谈论自己掌握或知晓的公司需要保密的消息和事件。不探听、保留那些自己职责外的保密信息。

(四) 涉及个人信息、客户信息、系统网络设置等查询，应在确认对方身份后再进行回答。

(五) 对重要的信息数据（如手头的重要资料、重要分析报告文件、专用的程序等）要做好备份，防止因丢失造成不必要的损失。

六、网络使用规范

七、办公设备使用规范

(一) 员工不应在设备旁边摆放食品、饮料。

(二) 办公设备若长时间不使用，员工应选择将其电源开关置于关断位置。员工应保护设备不受震动。不得连续开关电源。

(三) 硬件设备在外借、维修或报废（弃用）时，需对机内涉密数据作相应处理，防止泄密。

(四) 员工在离开座位或办公PC时，应及时锁屏。员工应根据情况设置进入屏幕保护的时间和口令，通常设定进入屏幕保护的等待时间不应超过5分钟。

(五) 若员工笔记本电脑被盗，确保立即报告当地执法机构及信息安全工作小组。

三、信息安全管理體系介紹

員工信息安全管理制度

GCMC-ISMS-03-07 員工信息安全管理制度

八、工作環境安全規範

(一) 員工在日常工作時，應佩戴身份識別標誌（徽章、工作牌、名卡）等，不得偽造或冒用他人的身份識別標誌。員工必須妥善保管身份識別標誌，以及所持有的特定辦公區域的門卡和鑰匙，禁止將自己的門卡、鑰匙以及所佩帶的識別標誌轉借他人。一旦遺失應立即向相關區域的負責部門匯報。

(二) 未經批准，員工不得帶任何外部人員參觀公司的內部工作區域。

(三) 員工應明確自己所擁有的權限，不得採用任何手段隨意出入自己無權進入的區域。如果確有需要，必須嚴格遵循相關的審批和登記手續，不得偽造虛假的登記信息。

(四) 禁止攜帶任何危險品、可燃品或其它可能影響人員和設備安全的物品進入辦公場所，如有特殊需要必須得到相關管理人員的批准。

九、移動存儲介質使用規範

(一) 移動存儲介質包括：軟盤、U盤、光盤、磁帶、移動硬盤、筆記本電腦等，對於移動存儲介質的存放和保管，要防止高溫、潮濕、磁場、強光、輻射的影響。

(二) 員工不應在辦公電腦上使用任何可疑的來歷不明的移動存儲介質

(三) 員工應及時將存有公司重要信息和工作文檔的存儲介質移交給專門的保管人員歸檔，在進行移交前應確保介質以及其存儲信息的完整和可用。

三、信息安全管理體系介紹

員工信息安全管理制度

GCMC-ISMS-03-07 員工信息安全管理制度

十、信息安全事件報告規範

(一) 員工在發現系統異常、網絡速度大幅下降、口令被篡改、影響業務、財產或聲譽的事或其它可疑情況時，應及時向上級負責人及信息安全部門報告。

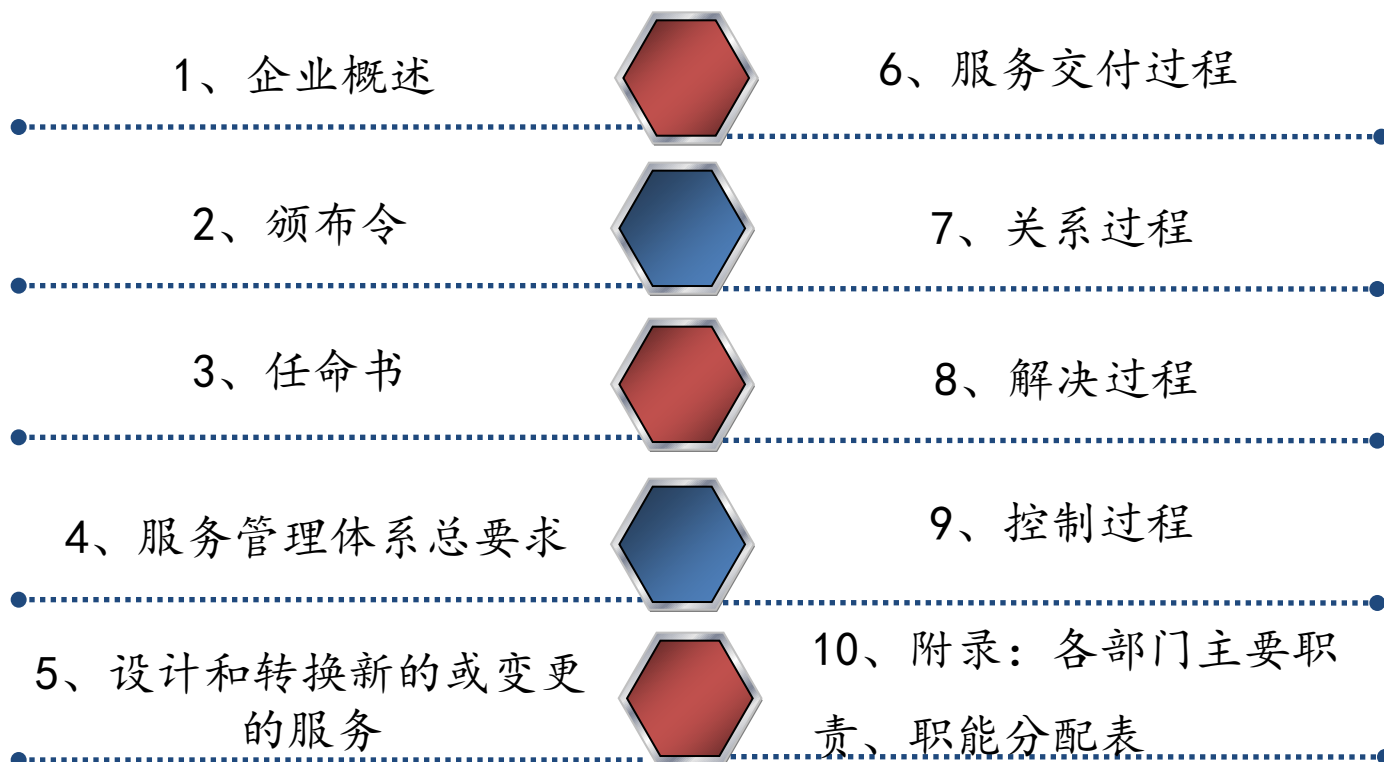
(二) 所有的員工、合同方和第三方用戶應關注並及時報告系統或服務中已發現或疑似的安全弱點或技術薄弱點。

(三) 對於突發信息安全事件，員工應按相關應急預案要求採取有效措施，儘可能防止事態擴大。

(四) 員工應事先熟悉信息安全事件響應流程，了解自身在其中承擔的角色，並在信息安全事件發生後自覺按要​​求履行應盡的職責。員工應當從信息安全事件中認真學習，汲取經驗教訓。

四、信息技术服务管理体系介绍

第一层文件 管理手册



四、信息技术服务管理体系介绍

认证覆盖范围

信息系统工程监理、信息系统工程咨询、企业管理软件的运维服务。

覆盖人数：1000人。（全员）

覆盖组织机构：不包含分公司

体系文件架构

- 一级文件：信息技术服务管理手册.
- 二级文件：程序文件（31篇程序文件，含公共程序9篇，监理和咨询业务程序10篇，软件开发业务程序12篇）
- 三级文件：记录表格

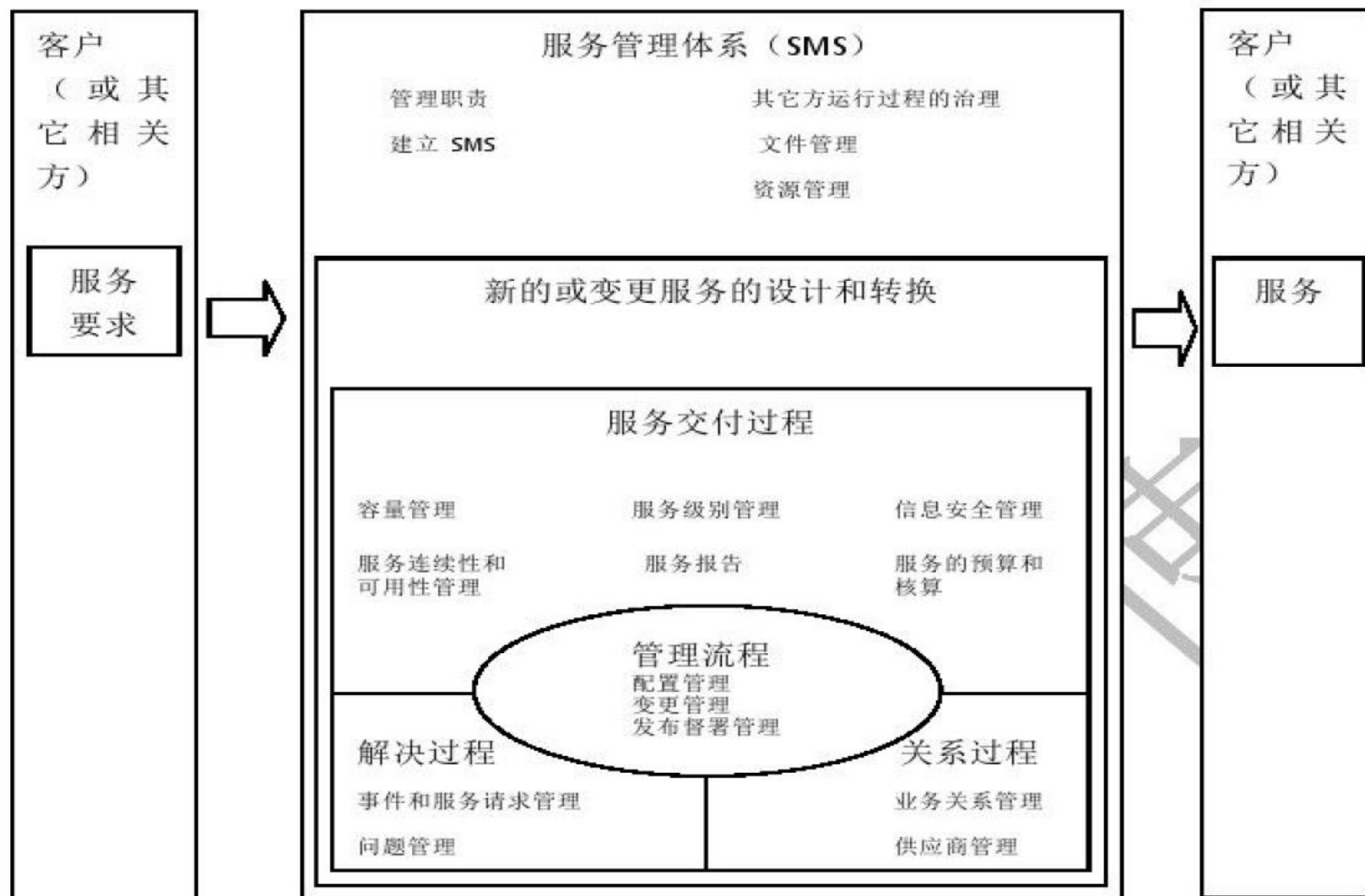
管理手册

IT服务方针：全员参与 过程控制 顾客满意 业界一流

IT服务目标：

- 1、合同履行率=100%（提供7*24小时服务）
- 2、用户满意度(R1) ≥ 85 分（满分为100分）
- 3、确保每年无重大安全事故发生

四、信息技术服务管理体系介绍



四、信息技术服务管理体系介绍

第二层文件 程序文件

GCMC-ITSMS-02-01 文件、记录管理控制程序	GCMC-ITSMS-02-11 服务策划管理控制程序（监理咨询）	GCMC-ITSMS-02-21 可用性管理控制程序（软件开发）
GCMC-ITSMS-02-02 人力资源管理控制程序	GCMC-ITSMS-02-12 服务级别管理控制程序（监理咨询）	GCMC-ITSMS-02-22 服务策划控制程序（软件开发）
GCMC-ITSMS-02-03 内部审核控制程序	GCMC-ITSMS-02-13 服务报告管理控制程序（监理咨询）	GCMC-ITSMS-02-23 服务级别控制程序（软件开发）
GCMC-ITSMS-02-04 管理评审控制程序	GCMC-ITSMS-02-14 服务改进管理控制程序（监理咨询）	GCMC-ITSMS-02-24 服务报告控制程序（软件开发）
GCMC-ITSMS-02-05 预算与核算管理控制程序	GCMC-ITSMS-02-15 事件和服务请求管理控制程序（监理咨询）	GCMC-ITSMS-02-25 服务改进控制程序（软件开发）
GCMC-ITSMS-02-06 能力管理控制程序	GCMC-ITSMS-02-16 问题管理控制程序（监理咨询）	GCMC-ITSMS-02-26 事件和服务请求控制程序（软件开发）
GCMC-ITSMS-02-07 信息安全管理控制程序	GCMC-ITSMS-02-17 配置管理控制程序（监理咨询）	GCMC-ITSMS-02-27 问题管理控制程序（软件开发）
GCMC-ITSMS-02-08 业务关系管理控制程序	GCMC-ITSMS-02-18 变更管理控制程序（监理咨询）	GCMC-ITSMS-02-28 配置管理控制程序（软件开发）
GCMC-ITSMS-02-09 供应商管理控制程序	GCMC-ITSMS-02-19 发布管理控制程序（监理咨询）	GCMC-ITSMS-02-29 变更管理控制程序（软件开发）
GCMC-ITSMS-02-10 可用性和持续性管理控制程序	GCMC-ITSMS-02-20 持续性管理控制程序（软件开发）	GCMC-ITSMS-02-30 发布管理控制程序（软件开发）

五、管理体系下阶段工作安排

1

- 4-5月份组织各单位参加内审员取证培训和考试

2

- 7-8月份组织内审、管理评审

3

- 9月份质量、环境与职业健康安全管理体系外审，11月-12月份信息安全和信息技术服务管理体系外审。

感谢各位聆听！

