信息安全管理交流

—— ISMS精要介绍

主讲：程武阳

深圳赛西信息技术有限公司

机构介绍

中国电子技术标准化研究院（工业和信息化部电子工业标准化研究院，工业和信息化部电子第四研究院，简称“标准院”、“电子四院），创建于1963年，是工业和信息化部直属事业单位，是国家从事电子信息技术领域标准化的基础性、公益性、综合性研究机构。在 2011年底根据中央编办《关于工业和信息化部电子工业标准化研究所更名的批复》，部人事教育司已正式批准CESI由“所”改“院”。标准院以电子信息技术标准化工作为核心，通过开展标准科研、检测、计量、认证、信息服务等业务，面向政府提供政策研究、行业管理和战略决策的专业支撑，面向社会提供标准化技术服务。

业务体系

标准院紧紧围绕标准化工作这一核心，研究工业领域标准化发展战略，提出相关规划和政策建议；组织建立和完善电子信息技术领域标准体系，开展共性、基础性标准的研究制定和推广应用工作；承担电子产品的试验检测、质量控制和技术评价、质量监督检测和质量争议鉴定等相关工作；负责电子工业最高计量标准的建立、维护和量值传递工作；开展管理体系认证、产品认证等相关活动；建立和维护工业领域标准信息资源网络，开展信息咨询、

我们的一切努力，都是为了我们的客户能全局性的了解自身的安全现状并为其提供全面的安全咨询服务。

目录

ISO27001（ISMS）实施总体收益

1、通过PDCA过程方法和相应的组织保障体系，使信息安全管理从“无序、零散、被动”的风险补救行为转变为“系统、连贯、主动”的风险驾驭状态。

2、改善信息安全风险水平，而且拥有可控的风险管理方法和保障落实机制。

3、建立统一的信息安全策略指导各业务部门在处理业务敏感信息方面的行为，防止机密信息泄露。

4、为业务系统的设计、开发和运行维护方面提供统一的安全规则。

5、完善各类安全管理制度，提高突发事件的处理能力，保证组织核心业务的可持续运行。

6、ISMS项目的实施，可以为企业训练出一批具有信息安全管理知识与技能的人员，一批具有“标准”意识、思维和行为方式的员工。

ISO27001（ISMS）实施总体收益

1、明确每个人对相关信息的安全责任，便于在工作中实施、监督和考核。

2、让员工了解到信息安全不仅仅是网络安全，还包括业务信息安全、人员安全、组织安全等方面的内容，使员工的安全意识有所增强，并在日常业务中按照相关规范执行信息安全要求。

3、通过ISMS提倡在行为规范上严格要求，使员工养成良好的习惯，避免发生大的事故。表面上看建立安全规则对员工多了一道约束（执行中有证据），实际上提供了对员工的保护。

ISO27001标准

ISO27001:2005

简介
- 概要
- 过程方法
- 与其他管理体系的兼容性

1 范围
- 1.1 概要
- 1.2 应用

2 标准引用

3 术语和定义

4 信息安全管理体系
- 4.1 一般要求
- 4.2 建立并管理ISMS
  - 4.2.1 建立ISMS
  - 4.2.2 实施和运行ISMS
  - 4.2.3 监督和评估ISMS
  - 4.2.4 维护和改进ISMS

ISO27001:2005

- 4.3 文件要求
  - 4.3.1 概要
  - 4.3.2 文件控制
  - 4.3.3 记录控制

5 管理责任
- 5.1 管理承诺
- 5.2 资源管理
  - 5.2.1 资源提供
  - 5.2.2 培训、意识和资格

6 内部ISMS审计

7 ISMS管理评审
- 7.1 概要
- 7.2 评审输入
- 7.3 复审输出

8 ISMS改进
- 8.1 持续改进
- 8.2 纠正措施
- 8.3 预防措施

ISO27001:2005

附录A 控制目标和控制
- A.5 安全策略
- A.6 组织信息安全
- A.7 资产管理
- A.8 人力资源管理
- A.9 物理和环境安全
- A.10 通信和操作管理
- A.11 访问控制
- A.12 信息系统获取、开发和维护
- A.13 信息安全事件管理
- A.14 业务连续性管理
- A.15 符合性

附录B OECD原则与本标准关系

附录C ISO 9001、ISO14001与本标准关系

信息安全管理体系(ISO27001) 主要内容

ISO27001 专注于信息安全的管理和流程管控

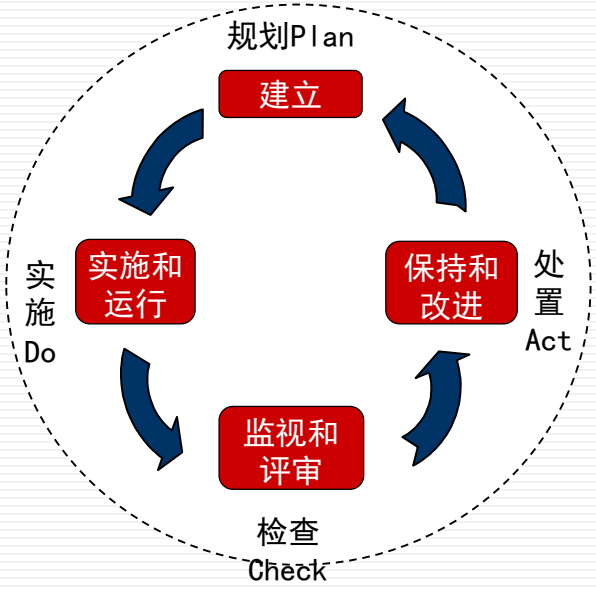
在ISO27001中,共有39个管控点和133个管控子目标

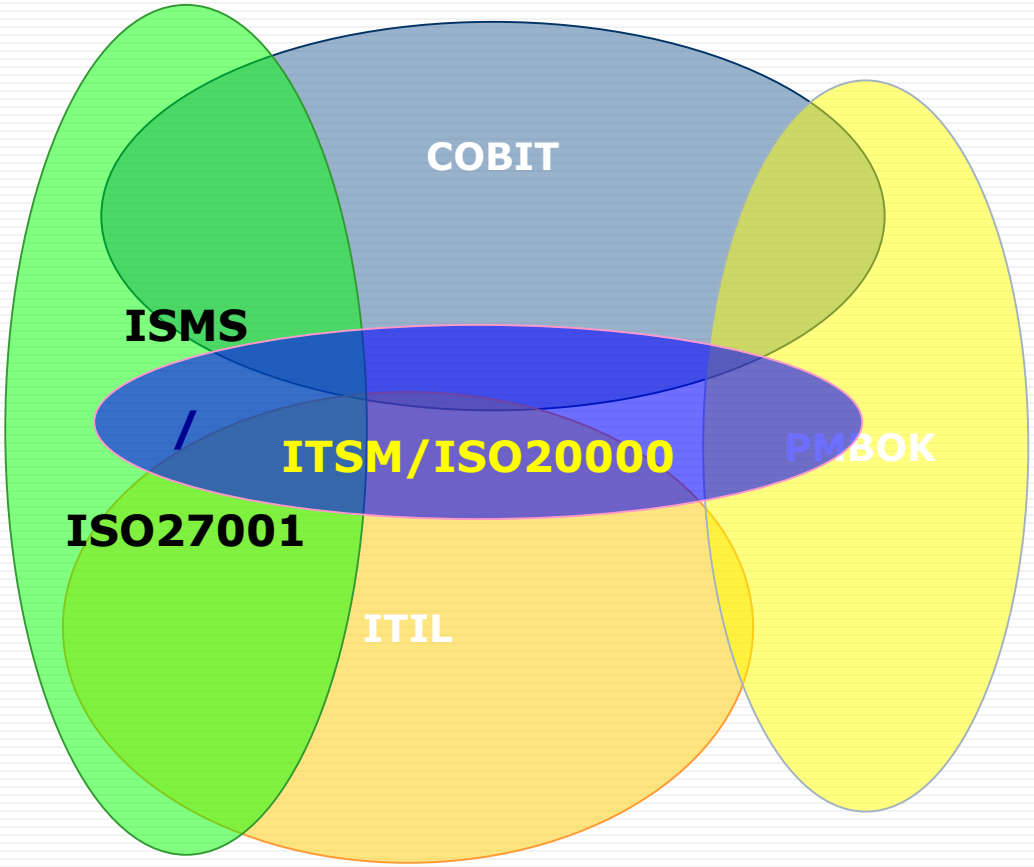
具体体现在三大方面：

- 风险源的查找,识别相关的管理控制流程，IT 技术解决方案用于防止和控制信息安全风险
- 日常的运营管理系统,确保信息安全风险的管控,包括人员,物理设备管理,操作手册等等
- 预警系统来防止或减少信息安全事故的发生

目录

持续改进&ISMS与ITSM融合（多体系融合）





持续改进&ISMS与ITSM融合

持续改进&ISMS与ITSM融合（多体系融合）

融合方法

体系融合的难点是如何处理好两个体系的共性和个性关系，应认真分析ISO20000，ISO27001两个标准的共有要素、相容要素和个性要素，运用整合思维、有机融合、共性兼容、个性互补的原则进行整合，是标准整合的关键

共有要素的融合

1. 文件及文件控制
2. 记录控制
3. 内容审核
4. 管理评审
5. 纠正和预防措施

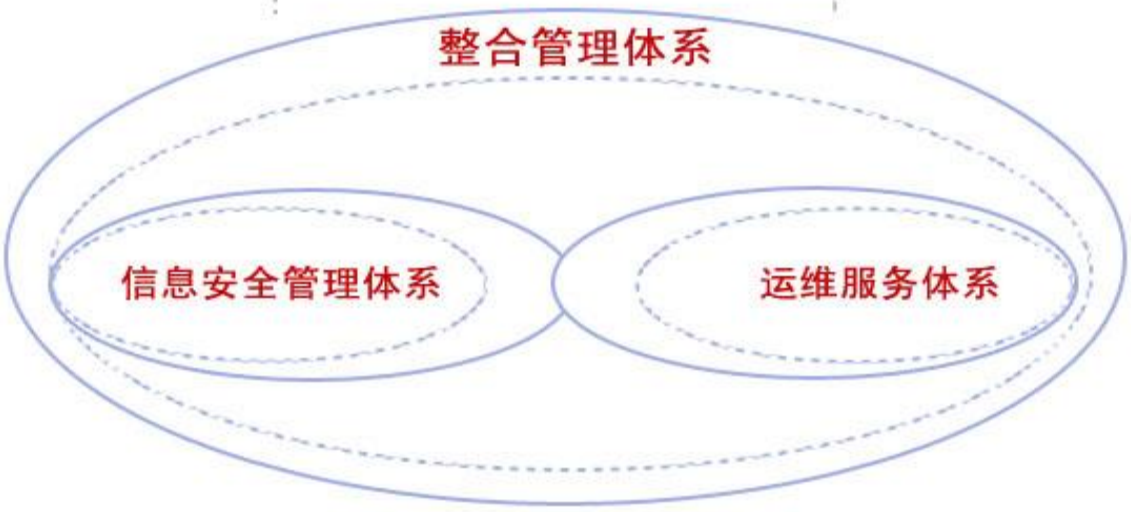
相容要素的融合

1. 管理方针
2. 管理目标
3. 法律法规及其他要求
4. 管理职责
5. 能力、意识和培训
6. 沟通和协调

个性要素的融合

1. ISO27001中，信息安全审是自己的特色要素
2. ISO20000中服务级别协议是自己的特色要素

融合规图



持续改进&ISMS与ITSM融合

ISO 20000流程	ISO 27001控制项
5 设计与转换新的或变更的服务	A9 物理和环境安全
	A10 系统验收
	A12 信息系统获取、开发和维护
6.3 服务连续性和可用性管理	A10.5 备份
	A11 访问控制
	A14 业务连续性
6.5 容量管理	A10.3.1 容量管理
7.1 业务关系管理	A6.2 外部各方
7.2 供应商管理	A10.2 第三方服务交付管理
8.1 事件和服务请求管理	A13 信息安全事件管理
9.1 配置管理	A7 资产管理
9.2 变更管理	A10.1.2 变更管理

整合的收益

1、强化组织管理，有利于提高管理水平：

通过对不同体系的审核，可以更加全面、准确和客观地评价组织的综合管理水平，有利于组织采取更为合理的措施，改进整体绩效，实现不断持续改进的目的。

2、合理配置资源，有利于提高组织效益：

减少文件数量，减少内审和外审工作量，大大降低成本，提高组织的服务水平，进而提升经济效益、社会效益。

3、有效降低风险，有利于提高外部合规性：

有效识别各类风险因素，采取切实有效的控制措施，提高组织IT管控水平，降低经营风险，满足内外部管理及合规需要。

目录

实施ISMS对组织的收益

- 对内：
  1. 对关键信息进行全面系统的保护，保障自身知识产权和市场竞争力。
  2. 按照风险理论建立管理体系，对企业安全风险达到可控的状态。
  3. 为内部审计提供依据。
  4. 改变问题驱动工作方式，信息安全以预防为主。
  5. 强化员工的信息安全意识，建立安全习惯，形成信息安全企业文化。
  6. 安全从“小安全”发展到“大安全”，已经从过去装个防火墙、杀毒软件，过渡到物理安全、人员管理、组织架构、体系建设等，从原来技术上的安全，逐步走向安全治理。
- 对外：
  1. 通过ISO27001认证，表明公司的ISMS符合国际标准，证明公司有能力保障重要信息，提高公司的知名度与公信度。
  2. 通过ISO27001认证，公司可以明确要求其他供应商相应提高信息安全水平，保证数据交换中的信息安全。
  3. 可作为公共会计审计的证据。

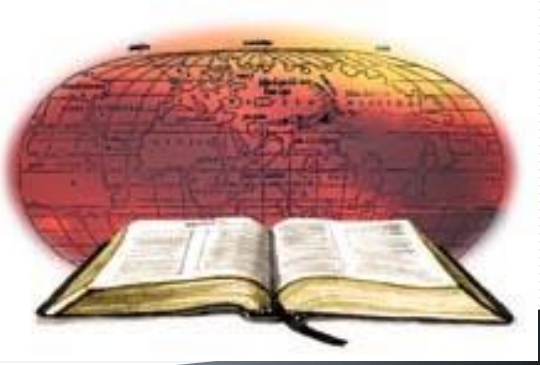
目录

项目实施总体概述

一个能通过认证的体系要有：

1.体系的职责说明（安全组织）
2.对体系覆盖范围、删减的说明
3.公司信息安全方针、目标
4.风险评估方法
5.风险接受准则
6.风险评估记录
7.不可接受风险处置计划
8.残余风险的接受
9. SOA
10.体系的文件清单
11.体系的记录清单
12.内审记录
13.内审不符合的整改
14.体系度量
15.管理评审报告
16.法律法规清单

把握审核员的底线



项目实施总体概述

项　　目　　管　　理

项目启动

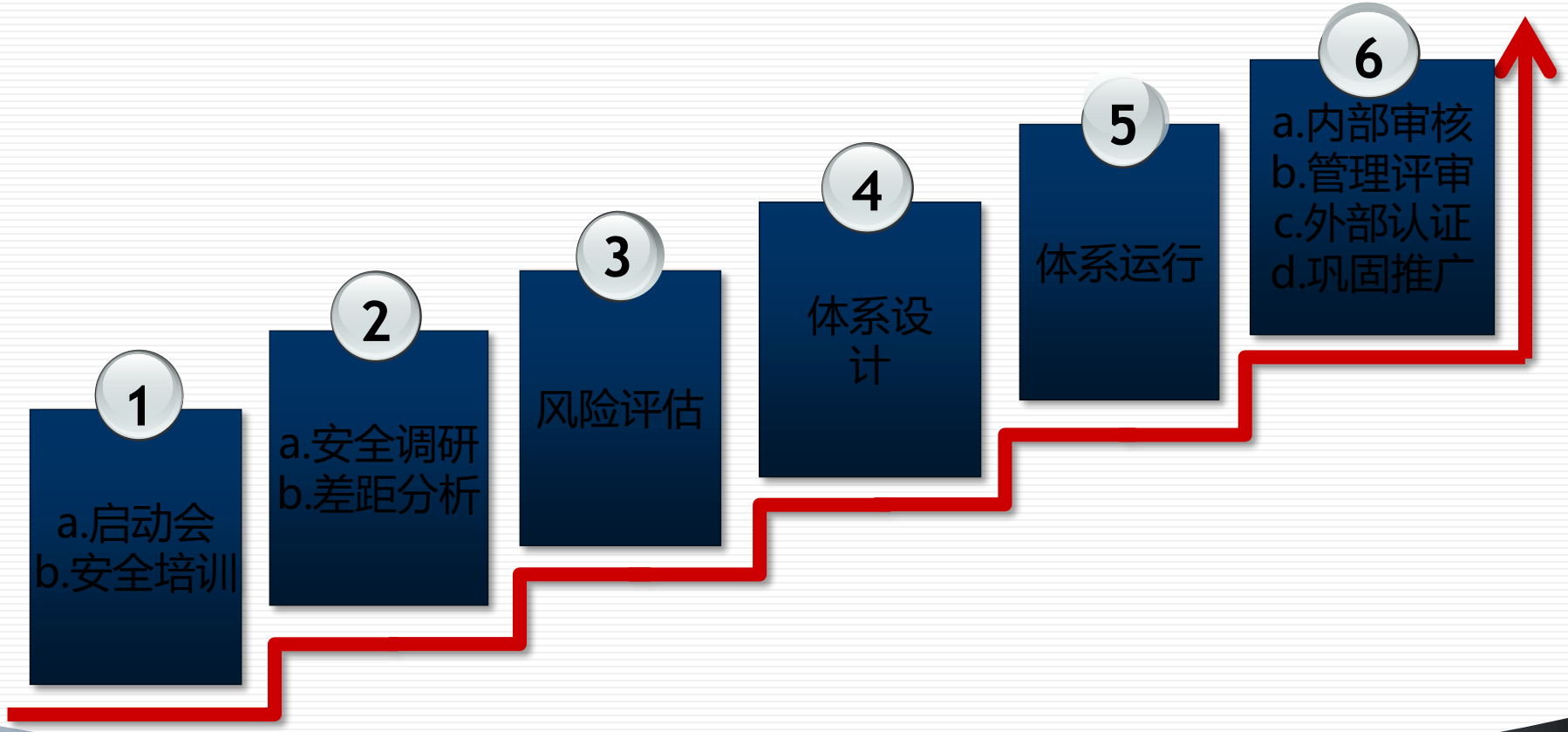
体系准备
1个月

信息安全管理体系策划
2个月

信息安全管理体系运行
2个月

体系检查与持续改进
1个月

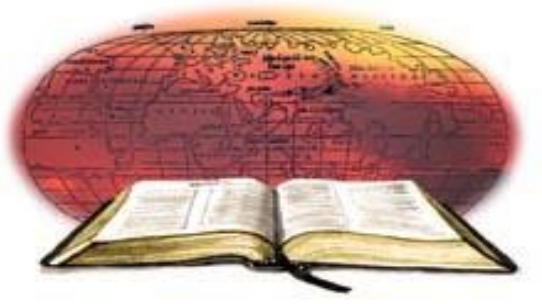
项目结束



项目实施总体概述

实施要点：

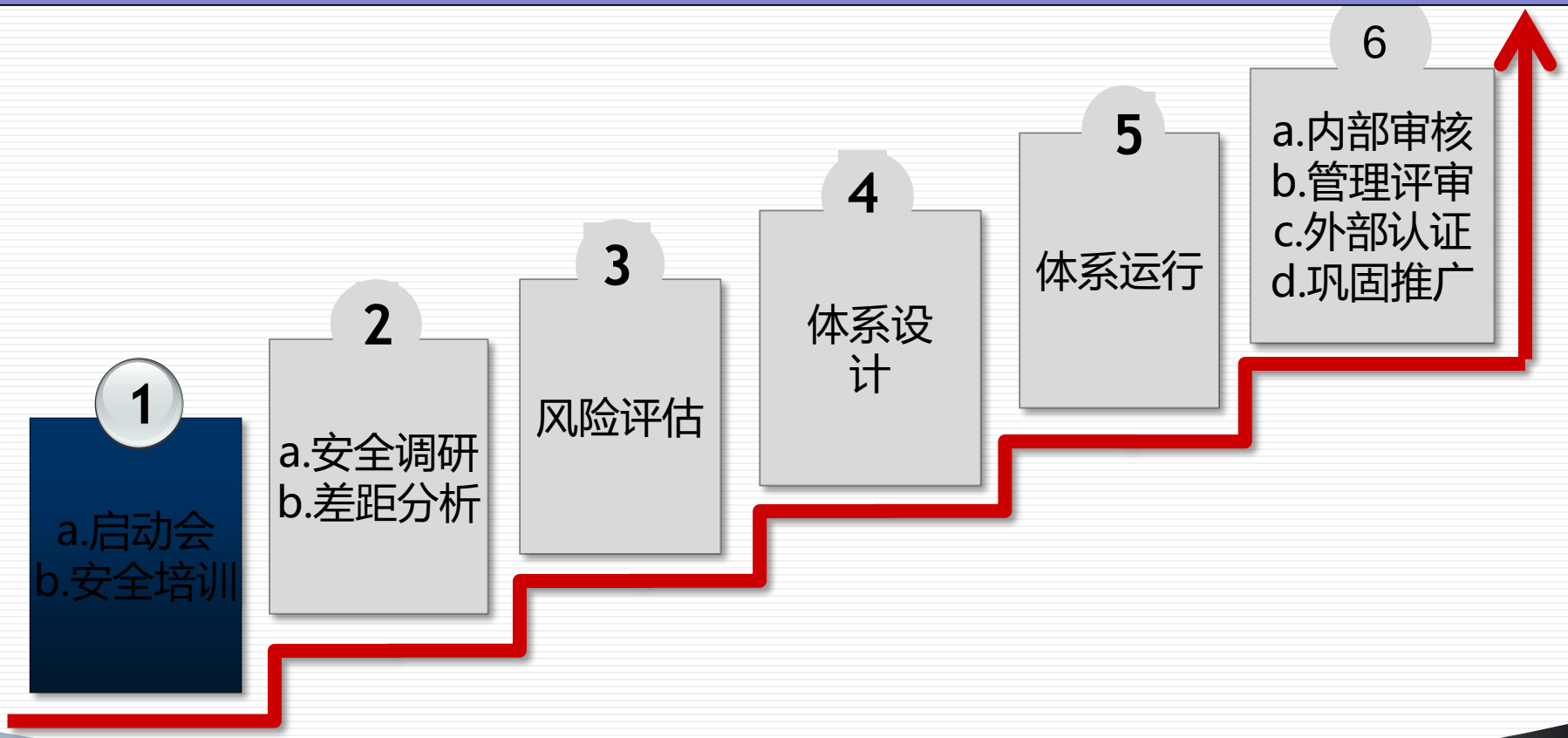
- **调动管理层，获得足够重视**
  - 组织保障
  - 指明方向和目标
  - 权威
  - 预算保障，提供所需的资源
  - 监督检查
- **遵循方法论的指导开展工作**
  - 信息安全是个管理过程
  - 应该系统地识别每项管理活动并加以控制，通过方法论的指导完成实施工作.
- **一切工作文件化/文档化**
  - 文件的作用：从“无法可依”到“有章可循，有据可查，灵活执法”.
  - 文件的类型：手册、规范、指南、记录
- **渐进式变革，消化阻力，持续改进**
  - 实现信息安全目标的循环活动
  - 信息安全是动态的，时间性强
  - 持续改进才能有最大限度的安全
- **全员培训,全员承担安全职责**
  - 信息安全不仅仅是IT部门的事情
  - 每个员工都了解安全事件报告处理要求
  - 每个员工都应具备相关的安全意识和能力
  - 让每个员工都明确自己承担的安全责任



核心活动开展与交付-1

项 目 管 理

项目启动 → 体系准备 → 信息安全管理体系策划 → 信息安全管理体系运行 → 体系检查与持续改进 → 项目结束



核心活动开展与交付-1

a 启动会

- 目的：确定双方项目组人员安排、项目计划
- 子活动：启动会前交流、启动会议
- 交付物：项目启动会议PPT、项目计划、启动会会议纪要、会议签到

——启动会前交流

（1）与客户项目经理就合同、SOW中工作内容、客户方人员投入、最终交付物等重申与确认。（重点确认项目范围）

（2）确认项目启动会议召开时间、地点、参加人。

——启动会议

（1）会议签到

（2）项目经理讲解项目目标、项目收益、项目计划、项目人员及职责、项目控制。客户方领导动员发言。

核心活动开展与交付-1

b安全培训

- 目的：使客户项目组成员对ISO27001有一定的认知，调动普通员工参与项目积极性
- 子活动：与项目负责人交流、ISO27001宣贯、安全意识培训
- 交付物：ISO27001培训PPT、员工安全意识培训PPT、培训签到、培训考核

——与项目负责人交流

（1）了解客户对培训的期望与要求。（时间/地点/人、形式、内容、是否要考试等）

（2）准备PPT，提交客户确认。

——培训

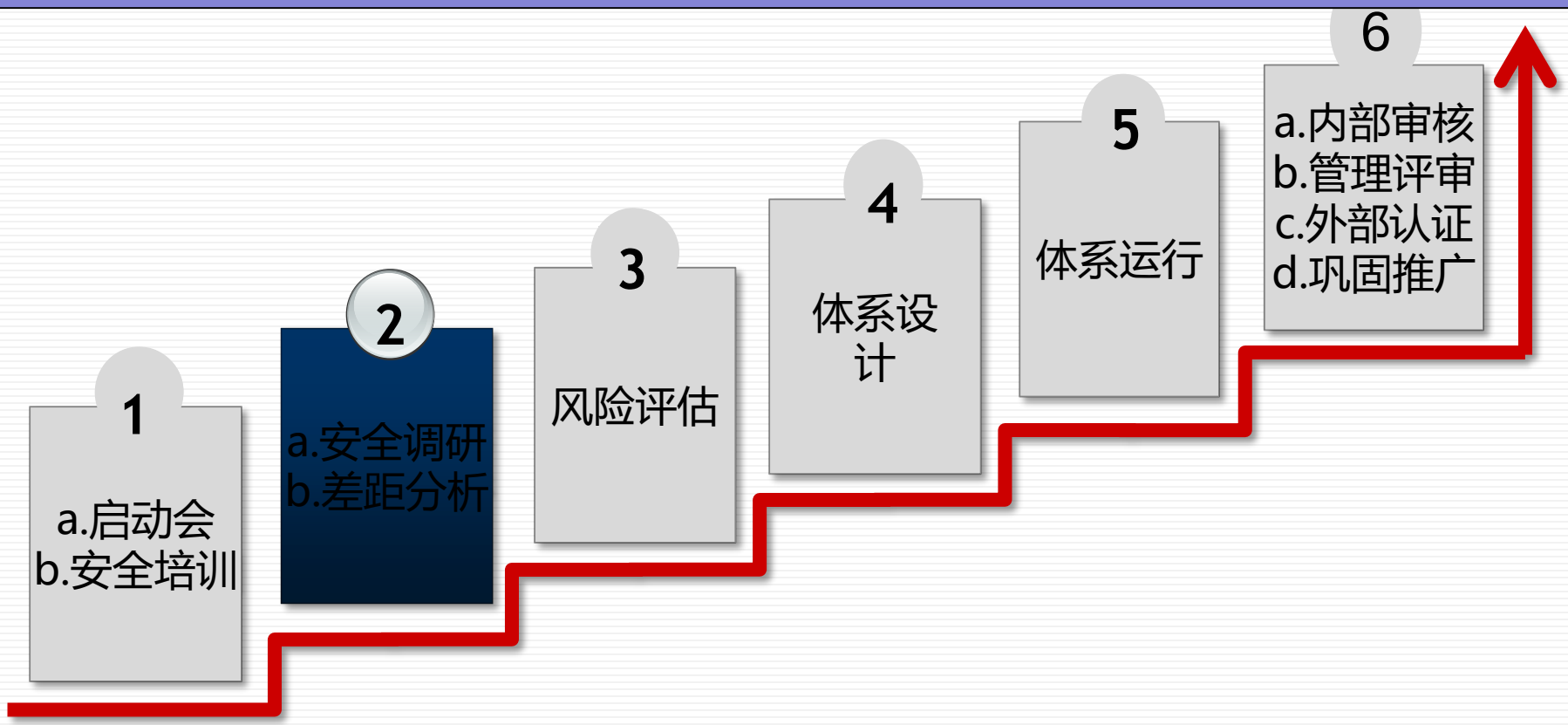
（1）ISO27001培训宣贯体系管理思想、标准内容解析（项目经理/内审人员2d）

（2）信息安全意识培训：项目跟员工有关（普通员工1h）

核心活动开展与交付-2

项　目　管　理

项目启动 → 体系准备 → 信息安全管理体系策划 → 信息安全管理体系运行 → 体系检查与持续改进 → 项目结束



核心活动开展与交付-2

a.安全调研

- 目的：收集不同部门、岗位的员工对安全现状的了解以及对项目的期望，为差距分析做准备。
- 子活动：收集阅读现有管理制度（关注安全方面）、安全访谈
- 交付物：现有制度梳理清单、访谈计划表、访谈问卷、访谈纪要

——收集阅读现有管理制度

（1）IT管理制度

（2）其他管理体系：企标/ISO9000/ISO20000/ISO22301/CMMI等

（3）上级部门下发

核心活动开展与交付-2

b.差距分析

- 目的：对比现有管理水平与标准差距，为风险评估打好基础，确定后续项目工作重点
- 子活动：编制差距分析报告、补充调研
- 交付物：差距分析报告

——编制差距分析报告补充调研

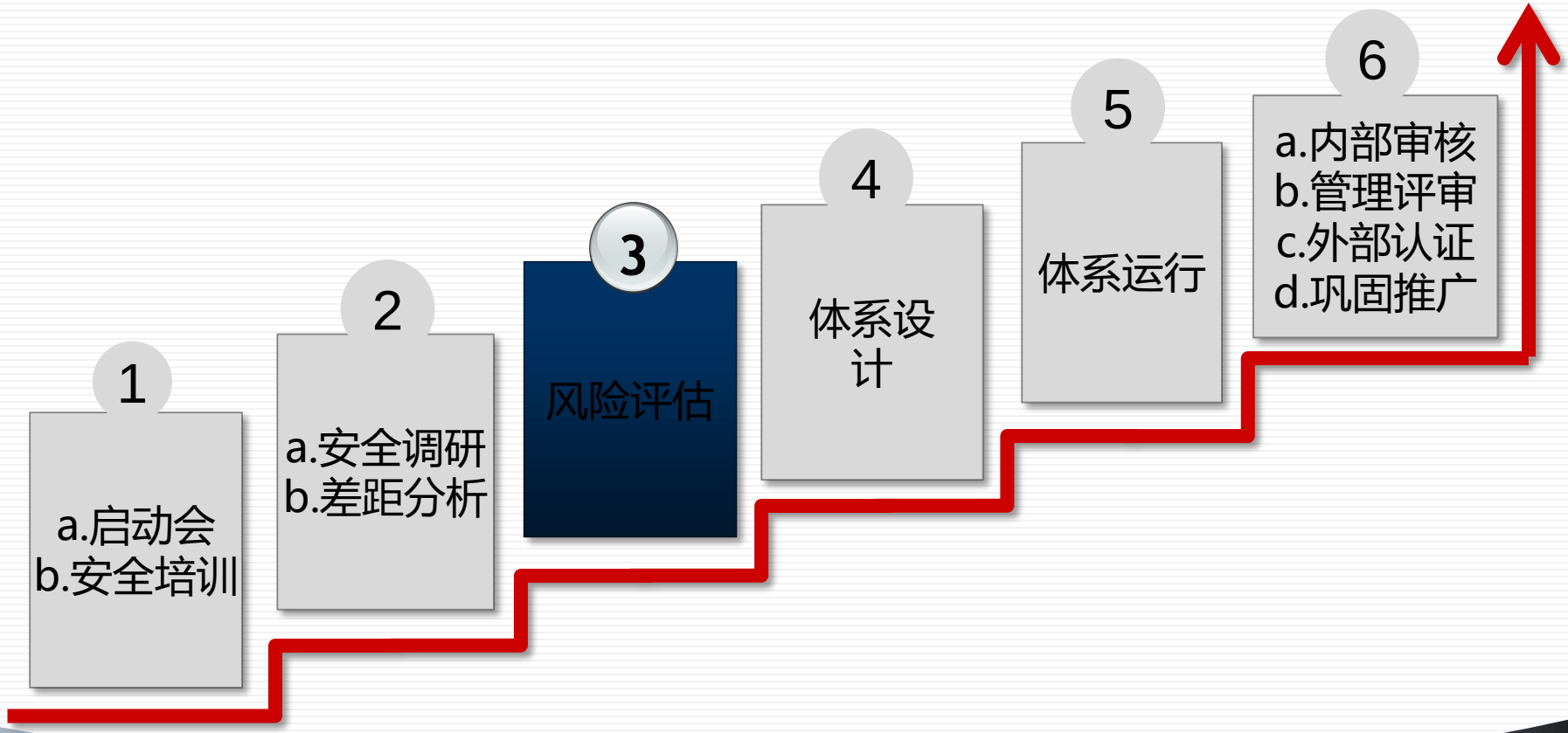
（1）差距分析报告：整理调研结果，搭建差距分析报告框架，参照标准计算现有安全管理水平得分。

（2）补充调研：根据所搭建差距分析报告内容缺失设计补充调研内容

核心活动开展与交付-3

项　目　管　理

项目启动 → 体系准备 → 信息安全管理体系策划 → 信息安全管理体系运行 → 体系检查与持续改进 → 项目结束



核心活动开展与交付-3

风险评估

- 目的：全面性地识别风险，为编制SOA提供依据。
- 子活动：定义风险评估方法、确定评估范围、实施风险评估、编制风险评估报告、制定风险处置计划、残余风险的处置
- 交付物：风险评估管理程序/风险评估实施指南、风险管理表、风险评估报告、风险处置计划、残余风险接受说明

——定义风险评估方法

（1）风险评估管理程序/实施指南：公司是否已有风险评估方法？

（2）基本要素：参照标准、评估频率、职责划分、资产分类与赋值、威胁分类与示例、弱点分类与示例、风险计算模型、风险接受准则、残余风险处理

核心活动开展与交付-3

风险评估

——确定风险评估范围

（1）资产范围：XXX信息系统/机房运维涉及资产

（2）部门范围：XXX部门所负责资产

（3）网络边界：拓扑图划定范围内的资产

——风险评估方法培训（2小时）

（1）培训准备：培训PPT/时间/地点/人员

（2）实施与考核：培训签到、考试（评估流程、表单填写）

——实施风险评估

编制风险评估报告

——制定风险处置计划

（1）包含要素：涉及风险资产、风险描述（威胁如何利用弱点产生什么后果）、风险级别、处置方式（4选1）、具体措施说明、责任人、计划完成日期；

（2）注意点：

- 风险处置计划可以以不符合方式发布、内容应与客户项目负责人确认;
- 完成时间最好不超过3个月，措施应考虑临时的和长远的。

核心活动开展与交付-3

风险评估

——残余风险的处置

（1）评价时机：内审之前

（2）评价对象：风险处置计划中风险处置后的资产

（3）评价内容：由管理者代表签署对处置后超过接受准则的资产风险处置意见。

——初步编制SOA

（1）要素：版本、条款、选择和删减理由、对应控制文件。

（2）编制人：客户方项目经理

（3）编写依据：风险评估中现有控制措施、风险处置所选择控制措施

核心活动开展与交付-4

项 目 管 理

项目启动 → 体系准备 → 信息安全管理体系策划 → 信息安全管理体系运行 → 体系检查与持续改进 → 项目结束

核心活动开展与交付-4

a.体系设计

- 目的：体系运行依据、认证核心证据、项目验收交付必备
- 子活动：安全组织/岗位设置、文件框架设计、文件审核、文件发布
- 交付物：体系文件、文件清单、记录清单、文件索引表

——安全组织/岗位设置（可放在手册内）

（1）考虑到现有的公司管理组织架构设定特点

（2）信息安全组织要有权威性，最好具有考核权

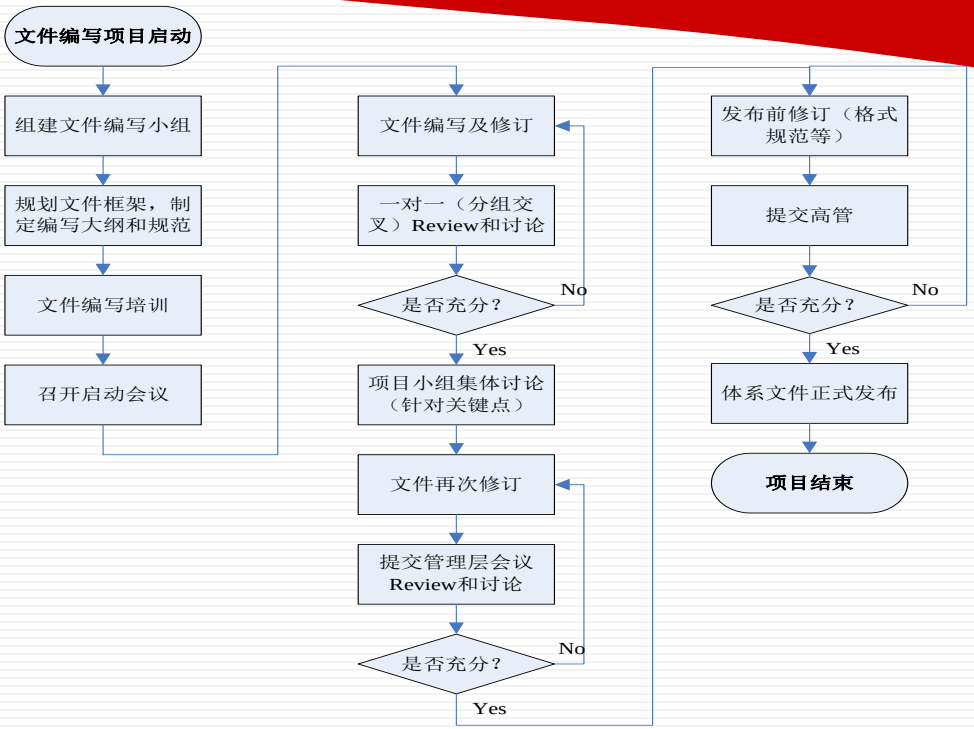
（3）形成高层支持、中层理解、员工执行的良好局面

核心活动开展与交付-4

a.体系设计

——文件实现

（1）编写流程：



编写要求：

- 体系文件的编写一定要从风险评估等得出的信息安全需求出发;
- 体系文件一定要可理解、可实施并有层次性和逻辑性，避免重叠和遗漏;
- 融合现有的管理规范: ISO9000/ISO20000/BS25999/CMMI等；
- 遵循公司的制度编写发布要求。

核心活动开展与交付-4

a.体系设计

——文件实现

（2）一级文件：手册：管理者代表任命、体系发布令、方针/目标、SOA。

（3）二级文件：规章、制度

（4）三级文件：实施细则、作业标准、指南

- 风险评估实施指南
- 信息机房安全须知
- 信息系统账号管理实施细则
- IT设备安全基线标准
- 移动介质管理规定

（5）四级文件：表格形式、名称不拘、控制措施体现即可

核心活动开展与交付-4

a.体系设计

——文件审核

（1）审核概述：制度框架、制度措辞、文件完整性/逻辑性/可操作性

（2）一级文件：管理者代表、项目经理，方针目标、组织架构职责

（3）二级文件：项目经理、文件责任部门领导，规定/流程可行性

（4）三级文件：项目经理、运维人员/普通员工，规定/流程可操作性

（5）四级文件：项目经理、运维人员/普通员工，表单要素完整性可填性

——文件发布

（1）审批方式：OA流转审批、签发发布令（附带文件清单）

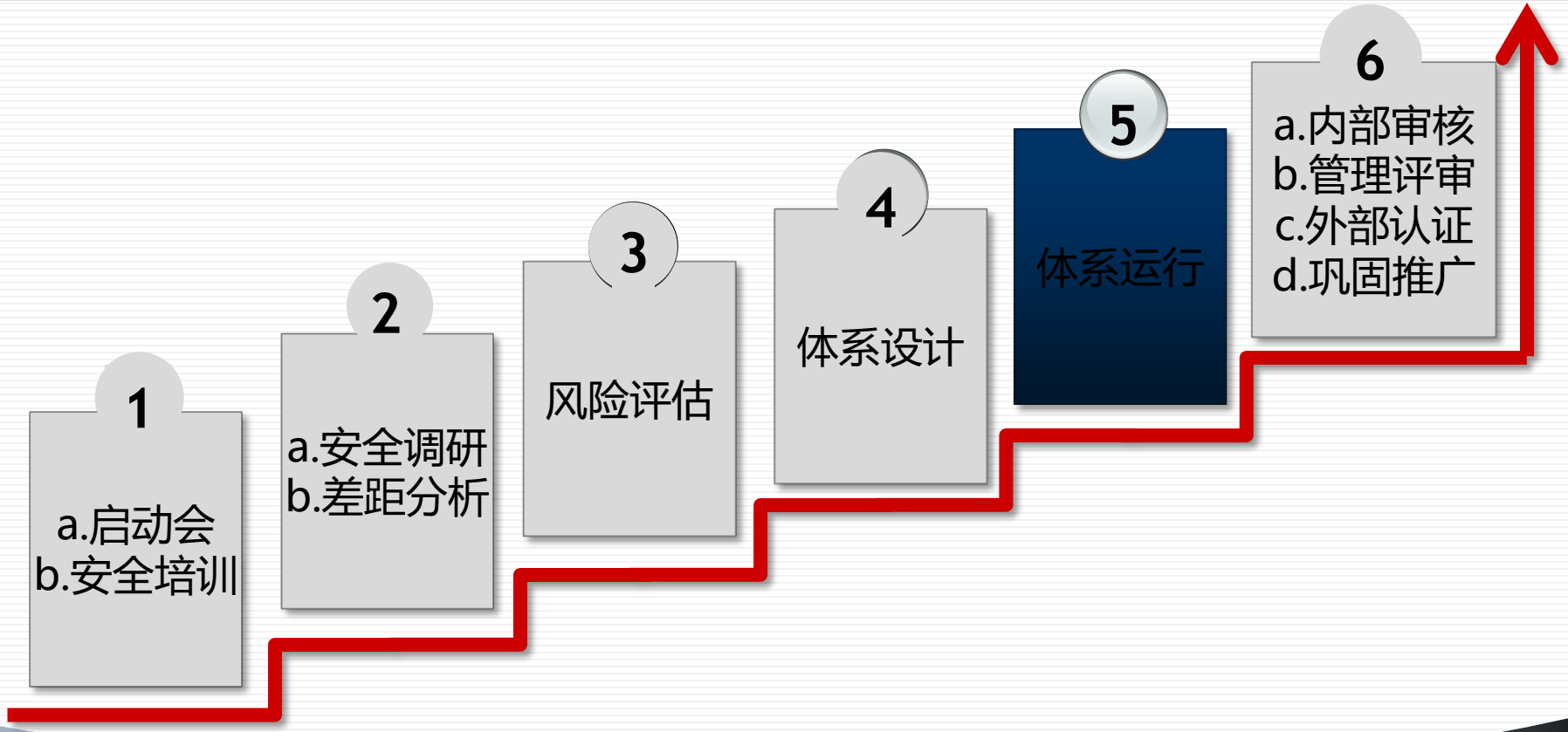
（2）发布时间：如果对认证时间点有要求需要注意此处。

（3）发布人：管理者代表以上级别

核心活动开展与交付-5

项　目　管　理

项目启动 → 体系准备 → 信息安全管理体系策划 → 信息安全管理体系运行 → 体系检查与持续改进 → 项目结束



核心活动开展与交付-5

a.体系运行

- 目的：检验所设计的文件合理性、产生认证所需的必要记录
- 子活动：落实风险处置计划、文件宣贯培训/记录填写指导
- 交付物：风险处置计划实施验证、文件宣贯PPT

——落实风险处置计划

（1）与体系设计并行执行，部分风险处置计划可能是编制相应的管理制度

（2）在约定的项目阶段工作会议（每2周一次）上督促项目经理。

——文件宣贯

（1）宣贯PPT：管理层：1-2级文件（0.5h）、体系负责人：1-4级文件（1h）、普通员工：3-4级文件（1.5h）

（2）培训签到/考核

——记录填写指导

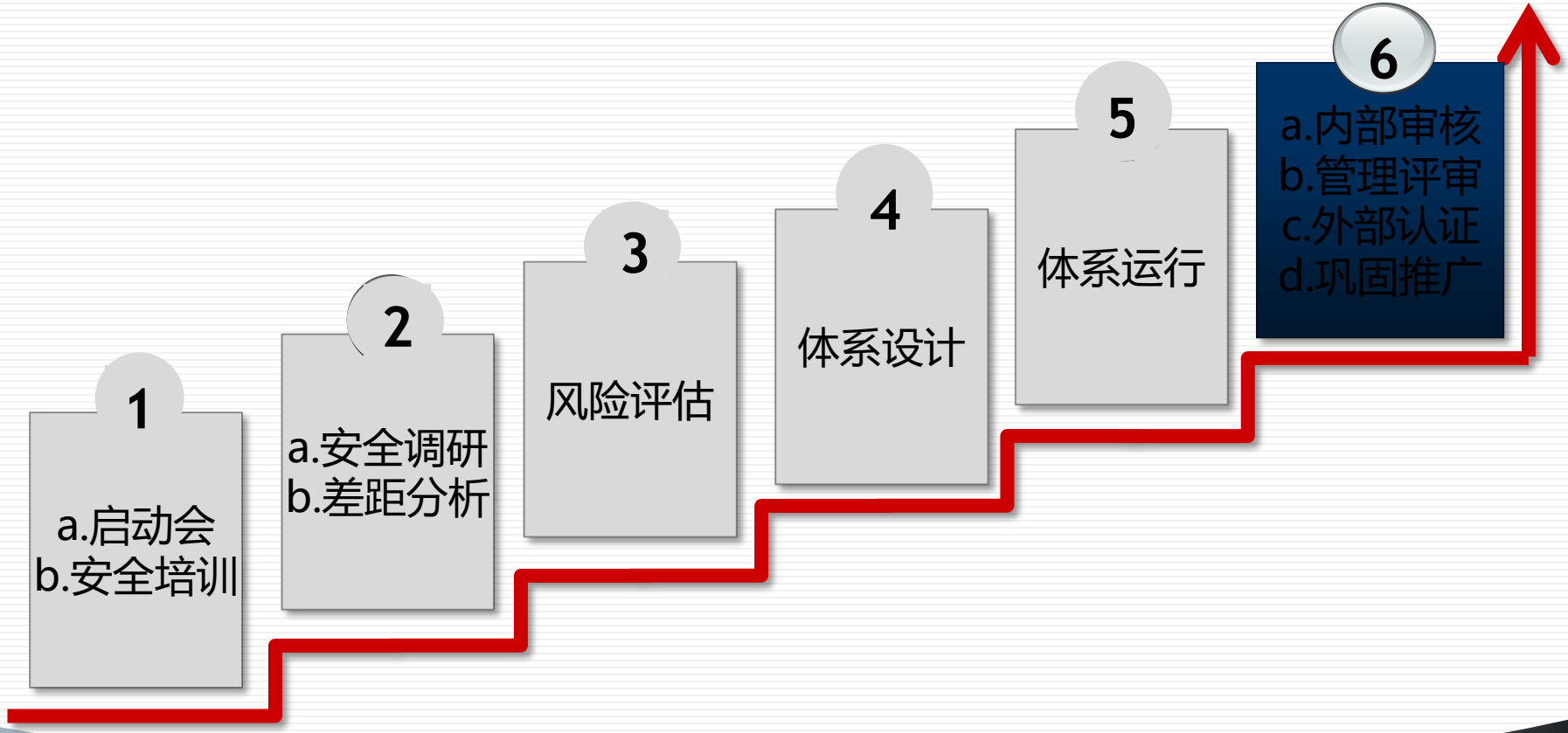
（1）表单设计的修正：体系试运行过程收集表单运行意见

（2）记录归档：用文件夹收集、年度统一归档

核心活动开展与交付-6

项 目 管 理

项目启动 → 体系准备 → 信息安全管理体系策划 → 信息安全管理体系运行 → 体系检查与持续改进 → 项目结束



核心活动开展与交付-6

a.内部审核

- 目的：使客户掌握内审方法，检验体系运行效果
- 子活动：内审培训、内审策划、内审准备、现场审核、内审总结、内审不符合整改
- 交付物：内审培训PPT、内审培训签到、内审考试、内审计划表、内审检查表、内审首次会议签到/记录、内审检查记录、内审末次会议签到/记录，内审不符合项、内审报告、不符合纠正预防计划

——内审培训

（1）培训PPT：审核介绍、审核流程、ISMS审核重点、现场审核模拟

（2）参加人：每个部门至少一个、项目经理、管理者代表

（3）培训签到/考核

核心活动开展与交付-6

a.内部审核

——内审策划

（1）内审小组成立：从参与内审培训成员中组建，1名内审组长，至少2名内审员。

（2）内审方案编制：

- 项目经理/内审组长编制，管理者代表批准
- 内容：审核依据、审核范围、审核目的、内审组成员、审核进度安排

——内审准备

（1）资料收集：内审组收集阅读体系文件、ISO27001标准要求

（2）编制内审检查表：

- 参考标准和制度要求编写
- 内容：制度文件、审核要点、审核方法、审核对象、审核发现、审核判断。

——现场审核

（1）内审首次会议

- 会议签到、内审组长发言、受审核部门代表介绍

（2）分组审核

- 管理层交流：贯标目的、对内审期望（可省略）
- 体系建立负责人交流：体系建立过程总体说明、风险评估、体系文件清单
- 各部门审核：附录A涉及的控制措施执行审核

（3）审核小组内部交流：审核过程争议项、问题交流、不符合确认

（4）内审末次会议：

- 会议签到
- 内审组长发言

核心活动开展与交付-6

a.内部审核

——内审总结

（1）内审报告编制：内审组长编制，内容包括：审核范围、审核依据、审核时间、审核情况总体描述、不符合分布统计、后续工作安排。

——不符合整改

（1）制定不符合纠正预防申请表：原因分析、整改措施、责任人、完成时间

（2）整改效果验证：项目经理跟踪，内审组长审批。

核心活动开展与交付-6

b.管理评审

- 目的：体系建立整体回顾、发现改进项、为外审做准备
- 子活动：评审输入材料准备、会议召开、评审报告编制
- 交付物：会议签到、管理评审报告

——评审输入材料准备

（1）体系审核和评审的结果

（2）相关方反馈

（3）用于改进体系绩效和有效性的方法、产品或者流程制度

（4）纠正措施执行情况：资源需求落实情况：

（5）以往风险评估没有强调的弱点或威胁

（6）有效性测量结果

（7）上次管理评审会议结果跟踪

（8）任何可能影响的变化

（9）改进建议

核心活动开展与交付-6

b.管理评审

——管理评审会议（1-2h）

（1）会议签到

（2）体系负责人汇报整体情况

（3）各部门汇报本部门运行情况

（4）问题讨论

（5）会议决议总结

——编制管理评审报告（本质是会议纪要）

要素：会议时间、编制人、与会人员、评审项目、提供评审的资料和意见、会议决议

核心活动开展与交付-6

c.外部认证

- 目的：获得证书、项目验收
- 子活动：认证前准备、一阶段审核、二阶段审核、不符合项整改、获证
- 交付物：一阶段问题整改说明（非正式）、不符合整改证据、观察项整改说明（非正式）、证书

——认证前准备

（1）应对审核培训：针对管理层、体系负责人、运维人员问题回答技巧

（2）补缺补漏：确保核心活动记录具备、内审不符合的关闭、现场物理环境检查。

核心活动开展与交付-6

c.外部认证

——一阶段审核

（1）远程审核：审核员阅读体系文件1-2级、发送一阶段审核计划

（2）首次会议：会议签到/审核员介绍一阶段审核安排

（3）主要活动：管理层交流、体系建立过程熟悉、风险评估活动审核、一阶段总结

（4）问题清单：非正式

——二阶段审核

（1）远程审核：发送二阶段审核计划

（2）主要活动：一阶段问题整改、附录A抽样检查、审核末次会议

（3）审核结论：宣布审核结论、不符合项（正式）、观察项（非正式）

（4）证书信息：客户名称、地址、认证范围（中英文）

核心活动开展与交付-6

c.外部认证

——不符合整改

（1）制定不符合纠正预防计划，明确责任人、纠正措施、完成时间

（2）执行纠正措施、管理者代表确认不符合关闭

（3）审核员确认不符合关闭

（4）正式不符合整改证据提交

——获证

（1）证书制作

（2）证书发放

交付物范例：

颁证日期：2009 年 7 月 13 日

有效期至：2012 年 7 月 12 日

GB/T22080-ISO/IEC27001

No. 01109IS10021R0M

兹 证 明

无锡软通动力科技有限公司

（江苏省无锡市滨湖区震泽路 27 号 9 号楼, 214122）

信 息 安 全 管 理 体 系 符 合 标 准：

GB/T 22080:2008/ISO/IEC 27001:2005

《信息技术 安全技术 信息安全管理体系 要求》

本 证 书 覆 盖 下 述 范 围：

位于江苏省无锡市滨湖区震泽路 27 号 9 号楼 1、2 层的
无锡软通动力科技有限公司范围内的
应用软件设计、开发和服务及相关的信息安全管理活动

《适用性声明》ISMS-2001 A/1

（本证书有效性依据发证机构的定期监督获得保持
证书有效性信息请登录www.cc.cesi.cn 进行查询）

中国电子技术标准化研究所认证中心

地址：北京东城区安定门东大街 1 号

网址：www.cc.cesi.cn

核心活动开展与交付-6

d.巩固推广

- 目的：确保体系融为企业管理的一部分，建立持续改进能力。
- 子活动：技能培训、制度意识宣贯、全面推广
- 交付物：ISO27001LA（非必须）

——技能培训

（1）针对内审人员的专项技能培训:内审员及主任审核员培训

（2）针对骨干人员的专项技能培训:CISSP/CISA/ITIL等知识体系培训

——制度意识宣贯

（1）前期、中期、后期

（2）后续

现场检查监督
红黄牌/留言

屏幕保护

意识培训
在线/现场

动态Banners
网站/服务登录提示

Do/DoNot警示
张贴便签

小物品
各种提示

张贴标语
在显眼位置

定期抽查考试
可记入业绩考核

Thank You!

chengwy@nels.org.cn