DISE数智实审

全新视角IT审计实战化的基础探讨

演讲人：王志超　　日期：2025年3月12日

数字风险赋能中心

数实融合　智审未来!

目录

CONTENTS

01 IT审计概述

02 IT审计流程

03 IT审计方法论

04 IT审计范围

05 IT审计实施方法

06 IT审计问题分享

01

IT审计概述

DISE 数智实审

为什么分享IT审计实战化经验?

01 公益宣传，分享IT审计实战化经验和技巧，深入解读国家法规及重点行业标准。

02 IT审计并不神秘，让大家都认识IT审计，了解它的基本流程、实施方法、审计要点及步骤技巧。

05 如何从IT审计过渡到数据资产审计，释放数据价值，打好坚实地基。

03 帮助大家在日常工作中提升质量和效率，更好的执行IT审计任务。

04 致力于推动IT审计公众普及化，进一步分析数智化审计的经验和实用案例。

1.1 IT审计概念

DISE数智实审

- **信息科技**：计算机、通信、微电子和软件工程等现代信息技术，在商业银行业务交易处理、经营管理和内部控制等方面的应用，并包括进行信息科技治理，建立完整的管理组织架构，制订完善的管理制度和流程——**《商业银行信息科技风险管理指引》**

- **信息系统**：信息系统是由计算机硬件、网络和通讯设备、计算机软件、信息资源、信息用户和规章制度组成的以处理信息流为目的的， 通过对信息的收集、传输、加工、存储、更新和维护，以组织战略竞优、提高效益和效率为目的,支持组织高层决策、中层控制、基层运作的集成化的人机系统——**《第3205号 内部审计实务指南-信息系统审计》**

1.1 IT审计概念（续）

DISE数智实审

商业银行视角

信息科技审计是对商业银行业务交易处理、经营管理和内部控制等方面的审计，包括信息科技治理、信息科技风险、信息安全、信息系统开发及测试、信息科技运行、业务连续性、信息科技外包等——**《商业银行信息科技风险管理指引》**

01

02

大型企业视角

信息系统审计是指内部审计机构和内部审计人员对组织信息系统建设的合法合规性、内部控制的有效性、信息系统的安全性、业务流程的合理有效性、信息系统运行的经济性所进行的检查与评价活动——**《第3205号 内部审计实务指南-信息系统审计》**

1.2 IT审计必要性

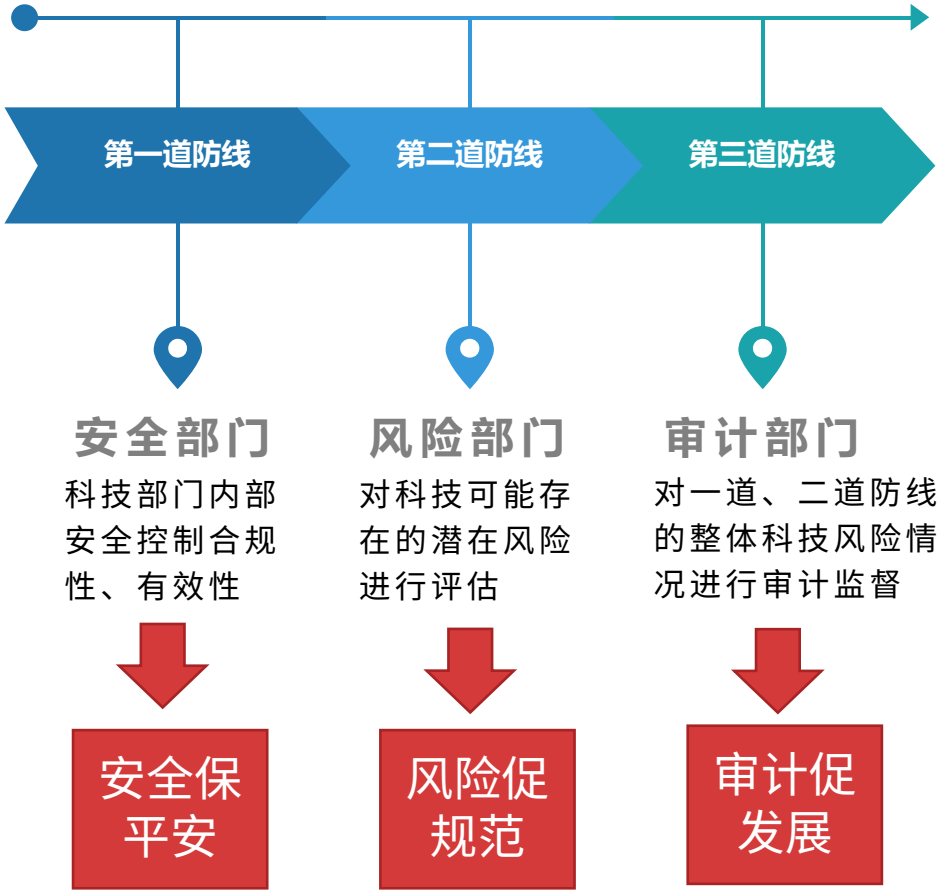
DISE 数智实审

2024年1月5日，金融监管总局开出三张大额罚单，建设银行、中国银行、中信银行合计被罚1000万元。这也是金融监管总局机关层面2024年行政处罚的首批罚单。

日趋严格的监管环境

互联网公开信息整理

相辅相成、相互监督



1.2 IT审计必要性（续）

DISE 数智实审

01

全新视角-管理视角

IT审计站在管理层视角，思考全局，从业务到IT，从风险到合规，提出整体的发展建议。

02

全新视角-控制视角

IT审计主要是对IT风险控制能力的审计，是从体制、机制的角度进行深入评价。

03

全新视角-风险视角

IT审计利用抽样和共性风险特点，从高、广、深不同层面关注风险，促进管理能力的提升。

04

全新视角-合规视角

IT审计还要站在国家法规、国家国标、行业监管等视角，全面满足合规要求。

1.3 IT审计目标

DISE数智实审

01

保障安全合规

通过对企业IT整体控制情况的全面审计，客观评价IT的**安全性、可靠性、经济性、合规性**。

02

促进转型发展

通过对IT转型发展能力，IT对于业务的创新支持，促进组织高效的**业务发展和数字化转型**。

03

提升风控能力

通过审计发现科技控制不足或系统漏洞，提出整改意见，监督整改效果，促进被审单位不断**提升信息科技风控能力。**

04

健全内控体系

通过审计帮助企业识别信息科技内控体系存在的风险及不足，推动建立健全**信息科技内部控制体系**。

1.4 IT审计趋势

DISE 数智实审

01

合规式审计

- 2006-2013年
- 以合规审计为主

02

风险式审计

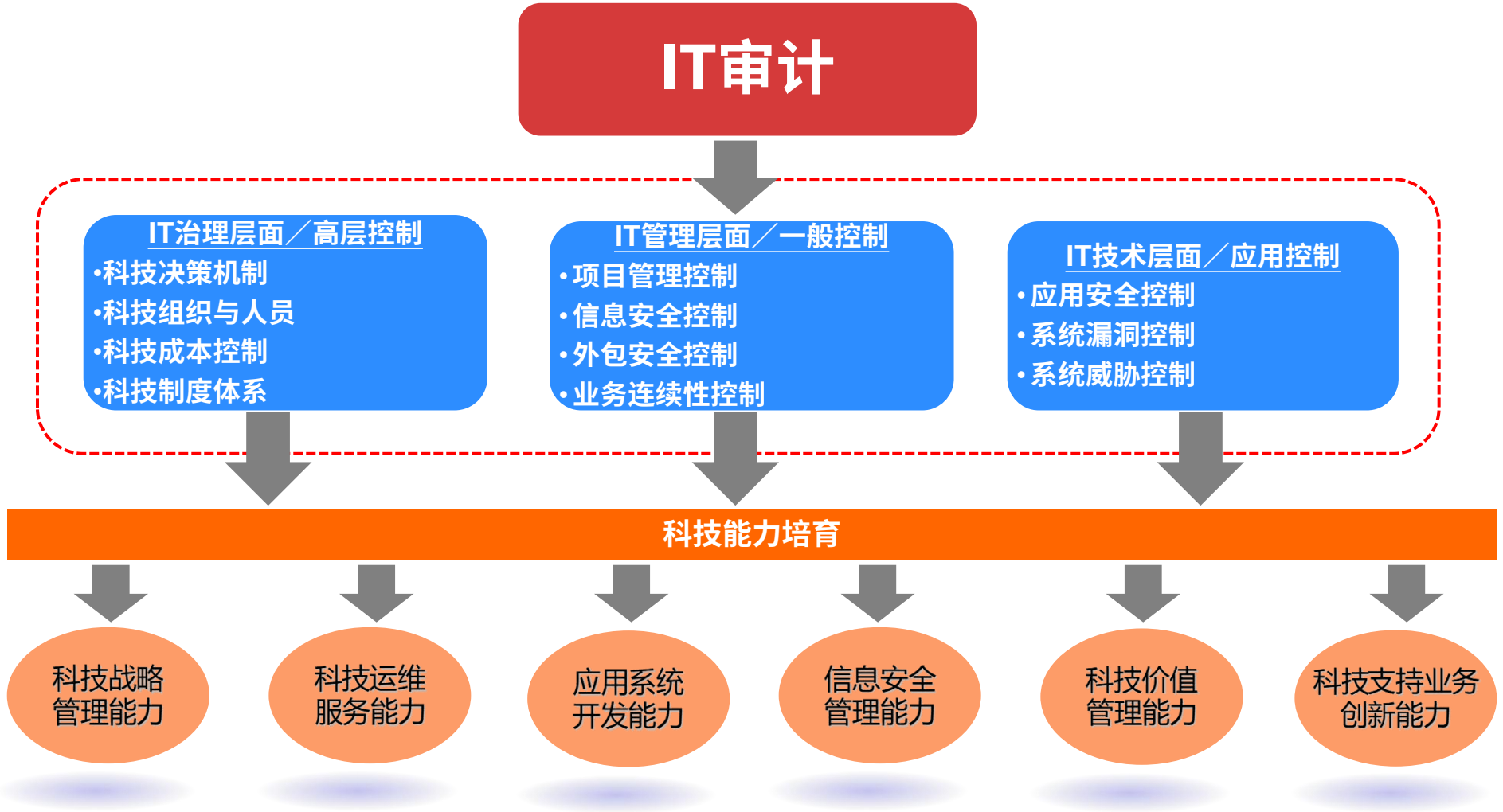
- 2014-2020
- 以风险审计为主

03

数智化审计

- 2021-未来
- 探索数智化审计

1.5 IT审计框架


IT审计
IT治理层面／高层控制
•科技决策机制
•科技组织与人员
•科技成本控制
•科技制度体系
IT管理层面／一般控制
•项目管理控制
•信息安全控制
•外包安全控制
•业务连续性控制
IT技术层面／应用控制
•应用安全控制
•系统漏洞控制
•系统威胁控制
科技能力培育
科技战略管理能力
科技运维服务能力
应用系统开发能力
信息安全管理能力
科技价值管理能力
科技支持业务创新能力

1.6 IT审计特点

DISE 数智实审

专业要求高	审计范围广	风险隐蔽强	模式更新快
1、科技知识 2、业务知识 3、审计知识	1、传统审计领域 2、金融科技领域 如云计算、大数据、移动互联、人工智能、区块链、零信任等	1、重要系统漏洞 2、敏感数据泄露 3、客户信息泄露	1、从合规-风险 2、从风险-咨询 3、从人工-智能

随着企业数字化转型步伐的逐步加快，更多新技术应用风险受到关注

1.7 IT审计核心技能

- IT与业务不能分家，IT助力业务高速发展，推动业务创新，因此要熟悉业务流程和系统功能。
- 网络拓扑、网络、系统、应用、数据、终端、介质、设备、日志等领域。
- 审计证据要充分支撑审计结论，对于审计取证的分析，要有总结、有逻辑、有依据。
- IT控制不仅局限于制度流程，更融入信息系统，要能对网络、数据、开发、运维等管理类系统效能进行评价。

1.8 IT审计主要痛点

DISE数智实审

1-审计方法不熟悉

2-科技知识不全面

3-监管理解不深入

4-审计成果不显著

5-新技术审计能力不足

6-缺乏数智审计系统辅助

后续的直播活动，将陆续和大家一起解决上述痛点！

02

IT审计流程

IT审计流程

DISE 数智实审

2.1 审计准备阶段

DISE 数智实审

- 明确审计对象(涉及组织、部门及岗位;涉及信息系统;涉及的重点领域;涉及的基础设施;涉及的技术层面)。
- 确定审计目标(如**合规性、安全性、可靠性、经济性**等)。

- 审计详细实施计划，明确审计要点、**配合部门及岗位、大致时间**，并明确关键里程碑。
- 大型项目或大规模审计，需进一步建立**访谈周计划**，以方便控制访谈进度。

- 收集相关资料，如组织架构图、拓扑结构图、岗位职责说明书、各项制度、记录、报告等。

与被审计方沟通 → **确定审计范围和目标** → **组建审计团队** → **制定审计计划** → **下发审计通知书** → **资料初步收集**

- 双方初步沟通，**明确审计重点**。
- 获取必要的支持和配合。

- 选择具备相关技能和经验的审计人员。
- 分配**每个人**具体职责和任务。

- 编制并下发审计通知书，明确审计背景、时间、内容、团队成员。
- 要求被审单位签署**审计承诺书**。
- 了解法律法规及行业标准是否有更新，并更新审计底稿，**标记审计重点**。

2.2 审计实施阶段

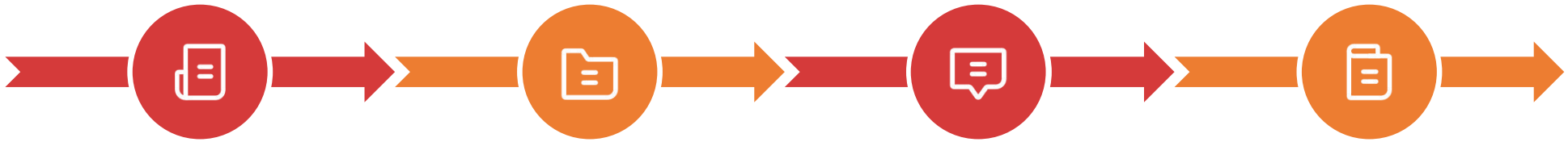
DISE 数智实审

审计实施

- 与**关键人员**（如高管层领导、技术总监、部门领导、安全管理岗、网络管理岗、系统管理岗、应用管理岗等）进行**深入交流**。
- 了解该企业的科技战略规划、**实际管控措施和潜在风险点**等。

记录发现的问题

- 记录所有不符合项或潜在风险，确保**逻辑清晰、证据充分。**
- 编制审计问题清单（序号、问题概述、取证记录、风险及影响、风险等级、审计依据、整改牵头部门、整改配合部门等）。



审计取证

- 资料审阅
- 现场观察
- 系统查看
- 技术测试

审计实施确认

- 与被审计单位保持沟通，**确认问题的真实性**，必要时进行补充取证。
- 充分沟通，并认真解答被审计单位的疑问。
- 进一步收集企业数据，完善审计报告使用。

2.3 审计报告阶段

DISE 数智实审

- 包括审计背景、审计目标、审计依据、审计范围、主要方法、发现的问题、改进建议等内容。
- 报告需**逻辑清晰、数据准确、语言简洁**。

- 将审计过程中产生的所有文件和记录存档，用于审计交付。
- 交付完毕后，组织相关人员**召开审计总结会**。

提出整改建议 → **编写审计报告** → **向管理层汇报** → **归档审计资料**

- 针对发现的问题提出具体的解决方案和建议。
- 考虑**措施落地的可行性**。
- 考虑**成本效益的可行性**。

- 向管理层汇报**审计结果和建议**。
- 获取管理层的认可和支持。

2.4 整改追踪阶段

DISE 数智实审

- 协助被审计单位制定详细的整改计划。
- 明确**整改措施、责任人和完成时间**。

- 通过复查或测试**验证整改措施是否有效**。
- 确保问题不再复发。

- 总结审计全过程的**经验和不足**。
- 提出改进**审计方法和流程的建议**。

制定整改计划 → 跟踪整改进度 → 验证整改效果 → 编制复审报告 → 总结经验教训

- 定期检查**整改措施的完成情况**。
- 记录整改过程中的问题和进展。

- 将整改结果进行记录，更新问题清单。
- 编制复审报告，形成闭环管理。

O3

IT审计方法论

3.1 基于合规的方法论

基于合规的方法论是一种以法律法规、行业标准和内部政策为依据，确保组织活动符合外部监管要求和内部管理规范的评价方法论。这种方法论主要适用于银行、保险、证券、非金融机构、能源等行业。

核心理念

1、法律与法规遵从
2、遵守行业特定的标准
3、内部政策执行
4、优秀的行业实践

实施步骤

1、合规需求分析
2、合规差距分析
3、合规问题清单
4、编制审计报告
5、制定合规计划
6、跟踪合规整改

一般有明确的审计依据，从符合性角度进行审计。

3.2 基于风险的方法论

基于风险的方法论是一种以识别、评估和管理风险为核心，通过系统化的方式优化资源配置并实现业务目标的管理方法。这种方法论通常建立在风险评估结果之上。

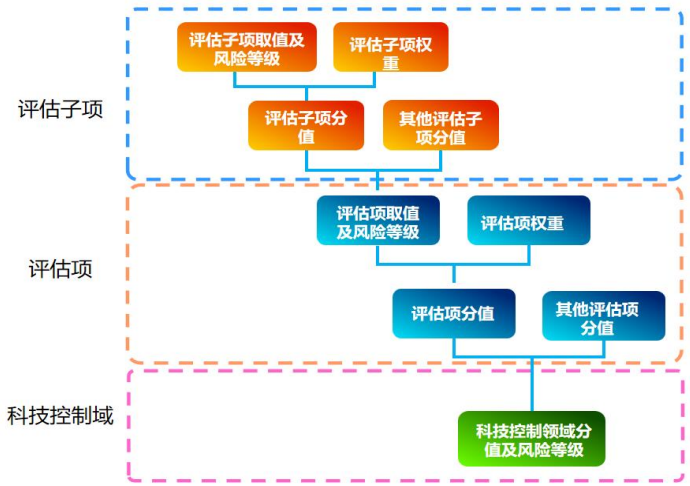
核心理念

01

1、基于历史评估结果
2、关注高风险领域
3、对高风险领域深入评价
4、评分区间对应风险等级

02

层次分析法 专家经验法



序号	评估项	标准分	权重	评估得分	综合得分
1.	数据治理体系规划	100	0.2	80	16
2.	数据管理组织架构及职责	100	0.2	80	16
3.	数据治理制度体系	100	0.2	80	16
4.	数据治理平台	100	0.2	90	18
5.	数据治理培训与推广	100	0.2	90	18
总计			1		84

序号	评估项	标准分	权重	评估得分（0-100）	综合得分（权重*得分）
1.	数据管控环境	100	0.2	84	16.8
2.	元数据管理	100	0.15	82	12.3
3.	数据标准管理	100	0.1	87	8.7
4.	数据质量管理	100	0.15	84	12.6
5.	数据应用及服务	100	0.2	86	17.2
6.	数据安全管理	100	0.2	85	17
总计			1	--	84.6

后续可设计分值对应风险等级，可参考：优秀、良好、中等、一般、待改进

04

IT审计范围

4.1 组织及岗位

DISE 数智实审

✓ 从部门视角：董/理事会、高级管理层、各专委会、人力部门、科技部门、风险部门、财务部门、行政部门、相关业务部门等。

主要领域	编号	访谈部门或岗位
信息科技治理	01	董/理事会办公室
	02	高级管理层（分管科技、风险、审计行领导）
	03	首席信息官
	04	各委员会（信科委、业务连续性委员会、数据治理委员会）主任
	05	人力资源部主管
	06	科技部门主管
信息安全管理	01	安全管理岗
	02	网络管理岗
	03	系统管理岗
	04	应用管理岗
	05	数据管理岗
	06	资产管理岗
	07	设备管理岗
	08	日志管理岗

主要领域	编号	访谈部门或岗位
系统开发及测试	01	项目管理岗
	02	质量管理岗
	03	需求管理岗
	04	系统开发岗
	05	系统测试岗
	06	部分项目的项目经理
信息科技运行	01	运维主管
	02	机房主管
	03	事件经理
	04	变更经理
	05	配置经理
信息科技外包	01	外包管理岗
……	……	……

以银行为例

4.2 重要系统及重大项目

- **从银行视角：**重要信息系统是指支撑重要业务，其信息安全和服务质量关系公民、法人和组织的权益，或关系社会秩序、公共利益乃至国家安全的信息系统。包括面向客户、涉及账务处理且时效性要求较高的业务处理类、渠道类和涉及客户风险管理等业务的管理类信息系统，以及支撑系统运行的机房和网络等基础设施。——《银行业金融机构重要信息系统投产及变更管理办法》
- **系统范围：核心系统、柜面系统、银行卡系统、信用卡系统、中间业务系统、二代支付系统、网上银行系统、手机银行系统、信贷管理系统等。**

- ✓ **从企业视角：**重要信息系统是指对企业的业务运营、战略目标实现以及核心竞争力具有关键作用的信息系统。这些系统通常承载着企业的重要数据和业务流程，其安全性、可靠性和可用性直接影响到企业的正常运转和市场竞争力。
- ✓ **系统范围：**ERP系统、决策支持系统、企业绩效管理系统、安全管理系统、投资项目管理系统、数字档案馆系统、客户关系管理系统、全面预算管理系统、供应商管理系统、数据治理平台、大数据平台、云桌面系统、人力资源管理系统、门户系统等。

4.3 数据中心

DISE 数智实审

生产数据中心 → 同城灾备中心 → 异地灾备中心

数据中心主要依据

银行数据中心关注范围

4.4 关键领域

DISE 数智实审

- 信息科技治理
- 信息科技风险
- 信息安全管理
- 系统开发及测试
- 信息科技运行
- 业务连续性
- 信息科技外包

- 数据中心
- 重要系统及重大项目
- 重要系统效能
- 数据治理及数据安全
- 客户信息保护
- 供应链安全
- 数字化转型

4.4 关键领域（续）

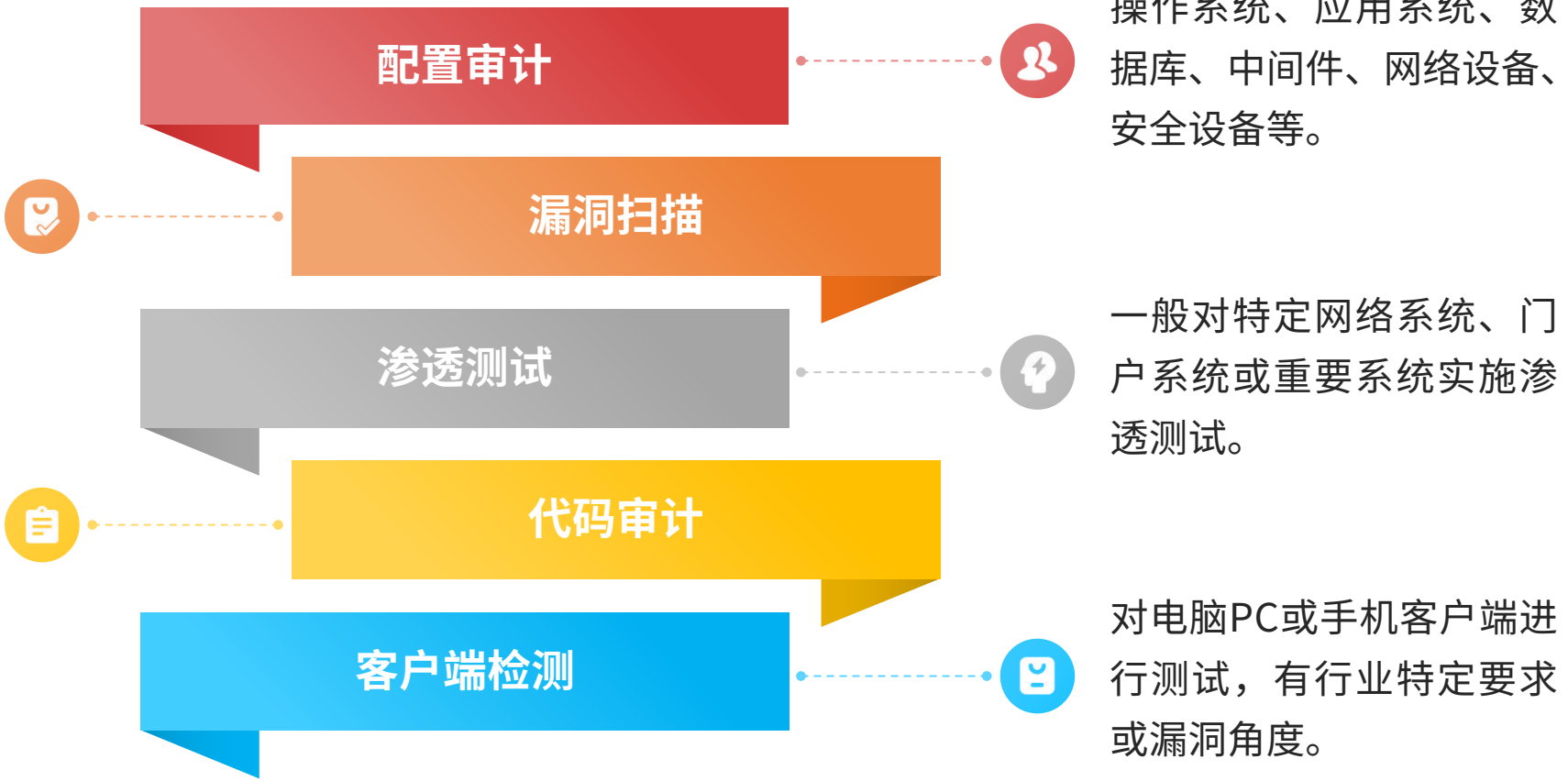
DISE 数智实审

领域	核心要点
信息科技治理	科技治理架构及职责、科技战略规划、科技投入、科技制度体系、人力资源管理、业务创新、知识产权保护等。
信息科技风险	科技风险架构及职责、科技风险策略、风险评估计划、全面风险评估、专项风险评估、风险问题整改、风险监测、风险平台等。
信息安全管理	网络安全管理机构、安全策略及制度、检查与评估、技术安全测试、网络安全、系统安全、应用安全、数据安全、终端安全、介质安全、设备安全、日志安全等。
系统开发及测试	项目管理架构及职责、项目制度体系、项目风险管理、项目沟通管理、可行性研究、需求、设计、开发、测试、上线、验收、后评价、正版化等。
信息科技运行	运维组织架构、运维制度体系、服务台管理、事件管理、问题管理、配置管理、变更管理、服务水平管理、容量管理、监控管理、智能运维等。
业务连续性	组织架构及职责、业务连续性战略、业务连续性管理制度、业务影响分析、风险评估、业务恢复策略、生产及灾备中心建设、系统灾备恢复能力、高可用性、备用人员、业务连续性计划、总体应急预案、系统应急预案、业务应急预案、应急与演练、业务连续性培训、危机管理、平台建设等。
信息科技外包	组织架构及职责、外包战略、外包制度体系、外包依赖、重要外包识别、尽职调查、非驻场外包管理、外包准入、外包合同、外包人员、外包安全、外包质量、外包应急与演练等。

领域	核心要点
数据中心	数据选址与规划、物理访问控制、综合布线、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、防鼠、温湿度控制、电力供应、UPS管理、发电机管理、电磁防护、数据中心保险、绿色数据中心等。
重要系统及重大项目	项目启动、项目管控、系统实施、系统变更交付、系统后评价、运营维护管理、信息安全、业务连续性、系统外包管理、数据治理等。
重要系统效能	项目可行性研究、需求、设计、开发、测试、上线、验收、后评价、效益与价值、质量与效率、转型与发展等
数据治理	组织架构及职责、数据治理制度体系、数据战略、评估机制、问责机制、数据字典、数据标准、数据质量、元数据、主数据、数据安全、数据应急、数据应用、数据治理工具等。
客户信息保护	组织架构及职责、方针及策略、制度体系、授权管理、脱敏管理、安全影响评估、访问控制、监控与审计、事件处置、生命周期安全防护等。
供应链安全	供应链安全管理制度、开源技术应用管理制度、软件开源风险管控、开源技术应用台账、开源组件版权许可管理、开源技术安全评估、数字生态合作数据安全风险自查等。
数字化转型	数字化转型治理、数字化人才建设、数字化保障机制、内部运营数字化、业务数字化、财务管理数字化、数据战略、数据治理评价体系、数字化基建、新技术架构、科技能力建设、新技术研究与自主可控、数字化风控等。

4.5 技术方面

DISE 数智实审



05

IT审计实施方法

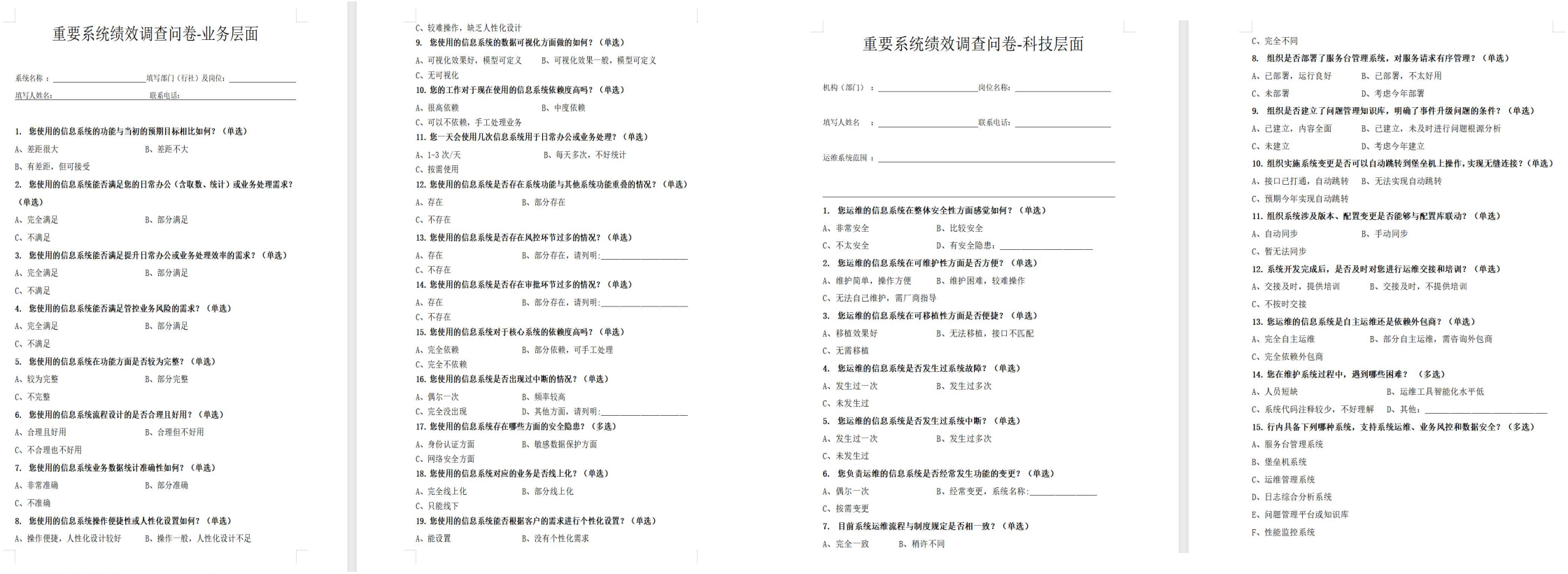
DISE数智实审

IT审计的核心和基础是什么？

审计思维

5.1 问卷调查

为了更有效的对重要信息系统绩效情况进行审计，针对业务、科技两个条线编制的调查问卷，通过对业务部门使用系统的情况进行调研，了解科技部门系统维护情况，可以更深入的了解重要信息系统的使用情况、需求满足度、系统便捷性、系统安全性等方面。



重要系统绩效调查问卷-业务层面

系统名称：_____填写部门（行社）及岗位：_____

填写人姓名：_____联系电话：_____

1. 您使用的信息系统的功能与当初的预期目标相比如何？（单选）

A、差距很大　B、差距不大

B、有差距，但可接受

2. 您使用的信息系统能否满足您的日常办公（含取数、统计）或业务处理需求？（单选）

A、完全满足　B、部分满足

C、不满足

3. 您使用的信息系统能否满足提升日常办公或业务处理效率的需求？（单选）

A、完全满足　B、部分满足

C、不满足

4. 您使用的信息系统能否满足管控业务风险的需求？（单选）

A、完全满足　B、部分满足

C、不满足

5. 您使用的信息系统在功能方面是否较为完整？（单选）

A、较为完整　B、部分完整

C、不完整

6. 您使用的信息系统流程设计的是否合理且好用？（单选）

A、合理且好用　B、合理但不好用

C、不合理也不好用

7. 您使用的信息系统业务数据统计准确性如何？（单选）

A、非常准确　B、部分准确

C、不准确

8. 您使用的信息系统操作便捷性或人性化设置如何？（单选）

A、操作便捷，人性化设计较好　B、操作一般，人性化设计不足

C、较难操作，缺乏人性化设计

9. 您使用的信息系统的数据可视化方面做的如何？（单选）

A、可视化效果好，模型可定义　B、可视化效果一般，模型可定义

C、无可视化

10. 您的工作对于现在使用的信息系统依赖度高吗？（单选）

A、很高依赖　B、中度依赖

C、可以不依赖，手工处理业务

11. 您一天会使用几次信息系统用于日常办公或业务处理？（单选）

A、1-3 次/天　B、每天多次，不好统计

C、按需使用

12. 您使用的信息系统是否存在系统功能与其他系统功能重叠的情况？（单选）

A、存在　B、部分存在

C、不存在

13. 您使用的信息系统是否存在风控环节过多的情况？（单选）

A、存在　B、部分存在，请列明:_____

C、不存在

14. 您使用的信息系统是否存在审批环节过多的情况？（单选）

A、存在　B、部分存在，请列明:_____

C、不存在

15. 您使用的信息系统对于核心系统的依赖度高吗？（单选）

A、完全依赖　B、部分依赖，可手工处理

C、完全不依赖

16. 您使用的信息系统是否出现过中断的情况？（单选）

A、偶尔一次　B、频率较高

C、完全没出现　D、其他方面，请列明:_____

17. 您使用的信息系统存在哪些方面的安全隐患？（多选）

A、身份认证方面　B、敏感数据保护方面

C、网络安全方面

18. 您使用的信息系统对应的业务是否线上化？（单选）

A、完全线上化　B、部分线上化

C、只能线下

19. 您使用的信息系统能否根据客户的需求进行个性化设置？（单选）

A、能设置　B、没有个性化需求

重要系统绩效调查问卷-科技层面

机构（部门）：_____岗位名称：_____

填写人姓名　：_____联系电话：_____

运维系统范围：_____

_____

1. 您运维的信息系统在整体安全性方面感觉如何？（单选）

A、非常安全　B、比较安全

C、不太安全　D、有安全隐患：_____

2. 您运维的信息系统在可维护性方面是否方便？（单选）

A、维护简单，操作方便　B、维护困难，较难操作

C、无法自己维护，需厂商指导

3. 您运维的信息系统在可移植性方面是否便捷？（单选）

A、移植效果好　B、无法移植，接口不匹配

C、无需移植

4. 您运维的信息系统是否发生过系统故障？（单选）

A、发生过一次　B、发生过多次

C、未发生过

5. 您运维的信息系统是否发生过系统中断？（单选）

A、发生过一次　B、发生过多次

C、未发生过

6. 您负责运维的信息系统是否经常发生功能的变更？（单选）

A、偶尔一次　B、经常变更，系统名称:_____

C、按需变更

7. 目前系统运维流程与制度规定是否相一致？（单选）

A、完全一致　B、稍许不同

C、完全不同

8. 组织是否部署了服务台管理系统，对服务请求有序管理？（单选）

A、已部署，运行良好　B、已部署，不太好用

C、未部署　D、考虑今年部署

9. 组织是否建立了问题管理知识库，明确了事件升级问题的条件？（单选）

A、已建立，内容全面　B、已建立，未及时进行问题根源分析

C、未建立　D、考虑今年建立

10. 组织实施系统变更是否可以自动跳转到堡垒机上操作，实现无缝连接？（单选）

A、接口已打通，自动跳转　B、无法实现自动跳转

C、预期今年实现自动跳转

11. 组织系统涉及版本、配置变更是否能够与配置库联动？（单选）

A、自动同步　B、手动同步

C、暂无法同步

12. 系统开发完成后，是否及时对您进行运维交接和培训？（单选）

A、交接及时，提供培训　B、交接及时，不提供培训

C、不按时交接

13. 您运维的信息系统是自主运维还是依赖外包商？（单选）

A、完全自主运维　B、部分自主运维，需咨询外包商

C、完全依赖外包商

14. 您在维护系统过程中，遇到哪些困难？（多选）

A、人员短缺　B、运维工具智能化水平低

C、系统代码注释较少，不好理解　D、其他：_____

15. 行内具备下列哪种系统，支持系统运维、业务风控和数据安全？（多选）

A、服务台管理系统

B、堡垒机系统

C、运维管理系统

D、日志综合分析系统

E、问题管理平台或知识库

F、性能监控系统

重要信息系统绩效问卷示例

5.2 人员访谈

DISE数智实审

一、人员访谈重要性

- 了解企业现状。
- 获取风险线索，为审计取证打下基础。

二、人员访谈要点

- 针对性的设置访谈提纲或要点，如高管层、科技主管或技术总监、相关岗位。
- 访谈要讲究技巧，访谈不是闲聊，也不是泛谈，即使吐槽，也要控制节奏。

A：总部级内部审计：建议正常交谈，直面主题。

B：总部对分公司审计：话题轻松，可以吐槽，但要验证。

C：对现状进行准确记录，简明扼要，对风险线索详细询问清楚，尽量把要取证的***记录、制度、报告、系统、环境***等记录清楚，若首次没听清，要记得再次询问，以便后续验证。

5.3 资料审阅

通过对相关制度、记录、报告等的审阅，验证控制措施的**合规性、合理性和有效性**。

01 控制设计

- 记录、报告：建议有标准化的模版，设计要合理。
- 制度：内容框架设计、岗位职责、控制流程、风险管控、内容输出等

02 控制执行

- 完整性、准确性、时效性。
- 制度体系——宣贯培训——落实执行——检查跟踪——总结优化

5.4 现场观察

DISE数智实审

哪些审计控制点需要现场观察的方法?

1

安全意识

密码输入操作、双因素认证

2

办公安全

办公环境敏感信息保护、统一安全U盘

3

机房安全

机房内部环境、外部周围环境

4

外包安全

外包开发及测试环境、开发代码安全管控环境、办公网移动存储介质安全性

5.5 系统查看

DISE 数智实审

序号	管控方向	系统/设备名称
1	资产管理	数据资产管理系统
2		配置管理系统
3	漏洞管理	配置稽核系统
4		漏洞扫描系统
5		代码审计系统
6	开发管理	项目管理平台
7		云桌面系统
8		看板系统
9		软件测试平台
10	网络安全	防DDOS设备
11		SSL服务器
12		VPN设备
13		网闸设备
14		应用防火墙WAF
15		链路负载均衡
16		威胁态势感知平台
17		流量监控系统
18		网络防病毒服务器
19		网络准入系统
20		IPS/IDS系统
21	系统安全	堡垒机
22		终端病毒防护软件
23	应用安全	网页防篡改服务器
24		应用安全控件
25		签名验签服务器
26		钓鱼网站监控系统
27	数据安全	数据加密系统
28		数据脱敏系统
29		数据防泄漏系统
30	终端安全	桌面管控系统

除了管理系统、安全系统外，有一些IT审计，还会涉及业务系统查看，如对手机银行系统、信贷系统、支付系统、核心系统、商户管理系统等。

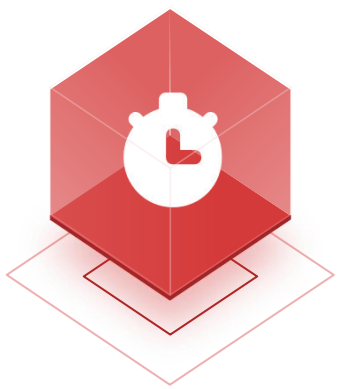
1、每个管理系统均有专项检查点

2、通过查看相关系统，验证系统设计的**合规性、有效性**，也验证系统功能的**全面性及落地性**

3、关注系统的效能（**安全、效果、效率、连续、成本**等）

5.6 技术测试

DISE 数智实审



配置审计

系统或设备的配置参数进行检查，确保其符合安全基线和行业实践的过程。

漏洞扫描

通过自动化工具对系统、网络或应用程序进行扫描，以识别已知漏洞的过程。

渗透测试

一种模拟真实攻击的技术手段，通过尝试利用系统漏洞来评估系统的安全性。

代码审计

对软件源代码进行审查的过程，发现代码中的安全漏洞或不符合安全规范的地方。

客户端检测

对客户端的安全状态进行检查的过程，包括程序异常检测、数据有效性校验、反编译、敏感数据安全、数据篡改等。

06

IT审计问题分享

DISE数智实审

业务和财务审计人员可以做IT审计吗?

转变思维，掌握方法，勇于尝试，善于总结。

6.1 IT治理层面

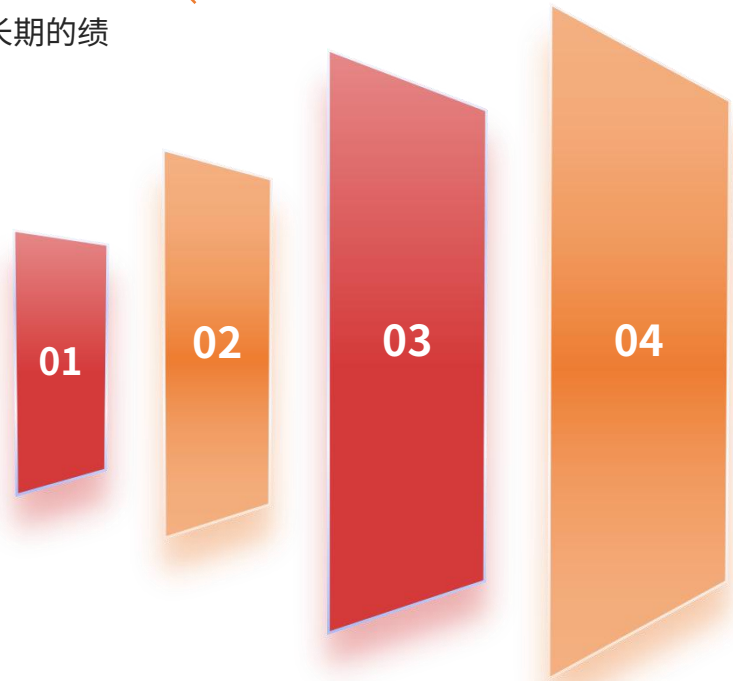
DISE数智实审

人员配备方面

信息安全、科技风险方面，虽然配备了专职人员，但缺乏相应的工作经验及专业资质，未有效执行安全检查自评估和科技风险评估工作。

绩效考核方面

人力部门制定企业绩效考核指标，但目前绩效考核与科技薪酬不挂钩，科技方面未建立长期的绩效考核激励机制。



IT规划方面

1）IT规划未通过董事会审批。
2）IT规划内容不全面，缺少应用架构、网络架构、数据架构的整体规划和布局
3）IT规划与业务规划脱离
4）IT规划的具体任务缺少工作任务分解
5）IT规划中的项目与实际落实项目不一致
6）原IT规划中的工作任务未有效落实或实施延迟并未说明原因

制度执行力

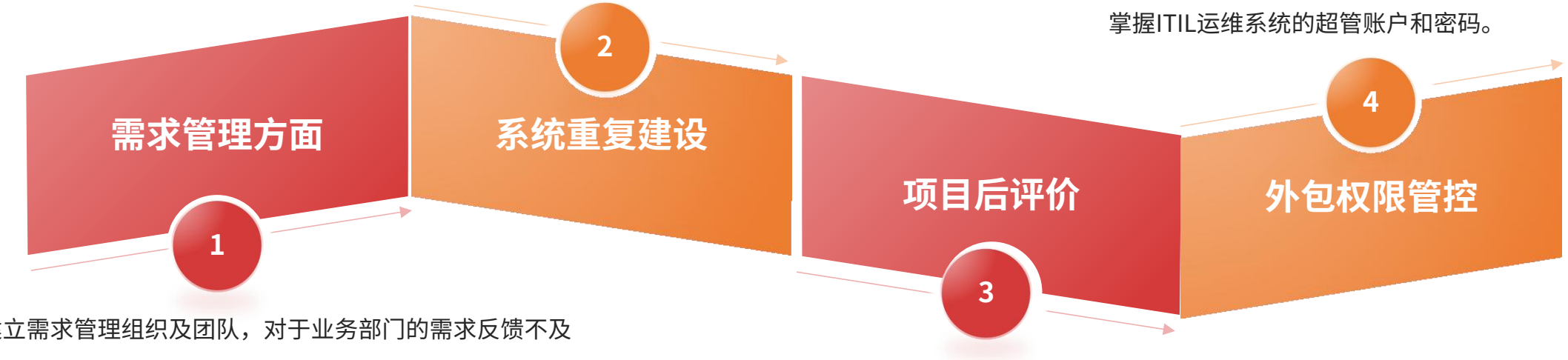
发现该企业未定期对信息安全制度执行情况进行评审，现有安全制度与数据治理制度在分类分级方面存在冲突，部分制度，如《A制度》《B制度》中的岗位设置与实际工作不符，《C制度》《D制度》中的工作流程与系统应用流程不符。

6.2 IT管理层面

DISE 数智实审

经过对下属40家行社的系统调研分析，发现10家行社存在功能类似的A系统和B系统，15家行社存在功能类似的C系统，只是名字约有差别；由于测试不充分及功能设计不足，D系统未按原计划下架，目前与E系统同时运行。

由于XX系统的运维是由外包人员负责，外包驻场人员掌握堡垒机的超管账户和密码，同时也掌握ITIL运维系统的超管账户和密码。



1）未建立需求管理组织及团队，对于业务部门的需求反馈不及时，同时缺少对于需求的统筹管理、需求分类、优先级判定、需求沟通等关键控制。

2）未对互联网系统进行安全需求评审工作，现有需求中，缺少对网络安全性、应用安全性、密码安全性、交易安全性等内容

40多个系统未进行项目后评价，已执行项目后评价的系统未保持独立性原则，且评价维度缺少系统效率、效果、成本、安全性等评价因素。

6.3 IT技术层面

DISE 数智实审

网络拓扑

1）现有开发测试网与办公网未采取有效的逻辑隔离机制。
2）网络间病毒缺少有效的控制手段，未部署网络防毒墙。
3）总部与部分的分公司之间缺少安全的加密通道，目前仍使用未加密通道传输数据。

设备配置

1）XX、XX等6个系统未设置密码长度和复杂度，目前允许简单口令123456登录。
2）IDS、IPS设备均未开启事件告警功能。
3）有6个系统的360天擎防病毒系统未开启实时防护功能，病毒库超过1年未更新。

系统漏洞

1）通过对XX网段、XX网段等20个网段的扫描，发现存在高危漏洞20个，中危漏洞漏洞36个，低危漏洞60个，同时发现历史的漏洞扫描结果整改后未得到及时验证。
2）通过对10个重要系统进行渗透测试，发现A系统、B系统等6个系统均存在跨站漏洞、目录遍历漏洞、任意文件执行漏洞等6个高危漏洞，C系统可任意修改缴费金额，并可验证通过。其他3个系统可绕过安全验证机制，非授权登录系统并查看交易明细。
3）通过对XX系统、XX系统的2个客户端进行测试，发现存在反编译漏洞、ROOT执行漏洞。

DISE数智实审第二期问题征集

为了推动IT审计和数据资产审计实战化的普及，加强与大家的广泛交流和互动，体现真正解决工作中的问题，从实战出发，第二期为问答交流模式，希望大家可以踊跃提出自己在工作中遇到的IT审计相关问题，宣讲团成员会尽量为大家解答，和大家一起进行经验交流，问题征集可参考如下内容：

征集方式：后续直播回放时会发送问题征集任务，征集**截止时间为3月19日**，大家可通过手机app填写**问卷星小程序**，直接提交问题即可。

DISE数智实审后续直播方向预告

DISE 数智实审

后续陆续直播方向如下，感兴趣的朋友可以持续关注“数智实审”视频号！

群聊： 数智实审生态群

1、国家重要法规解读
2、主要行业标准解读
3、关键审计领域底稿讲解
4、典型领域共性问题分享
5、审计实战化案例解析
6、行业热点技术漏洞分析
7、重点行业痛点及难点剖析
8、数智化审计经验分享

大家可以关注视频号，私信回复‘进群’，获取微信生态群入口，获取直播 PPT、标准汇编、标准解读报告、安全牛行业分析报告等众多福利，同时，宣讲团也招募分享嘉宾，可以私信留言，进群后发您申请表，期待您的加入！

DISE数智实审

感谢观看

演讲人：王志超　　日期：2025年3月12日