目录

角色职责

第一章

基本职责归纳

活动	角色	职责	页码
信息系统审计职能组织	最高管理层和审计委员会	✧ 审批审计章程	P7
审计规划	IS 审计师	✧ 了解定期风险评估结果、技术应用变革和不断发展的隐私问题和法律要求等其他考虑因素可能会影响到整体审计方法； ✧ 考虑系统安装启用/升级期限、当前和未来技术、业务流程负责人的要求以及 IS 资源限制； ✧ 对审查的整体环境有所了解，熟悉业务运营所处的监管环境。	P12
内部控制	董事会和高级管理层	✧ 负责建立相应的文化来促成有效且高效的内部控制系统，并且还负责持续监视内部控制系统的有效性，使组织中的每个成员都必须参与此过程	P99
舞弊检查	管理层	✧ 负责建立、实施和维护 IT 控制的框架和设计，以实现内部控制目标	P132
	管理部门	✧ 对检测和披露所有舞弊行为（无论是否属于实质性舞弊）负有主要责任	
	IS 审计师	✧ 对检测和披露所有舞弊行为（无论是否属于实质性舞弊）负有主要责任； ✧ 在工作的各个方面奉行应有的专业怀疑态度。	
	审计委员会	✧ 对检测和披露所有舞弊行为（无论是否属于实质性舞弊）负有主要责任	
审计优势和弱势评估	IS 审计师	✧ 判断呈现给各级管理人员的结果并向其报告	P190
沟通审计结果（退出面谈）	管理人员	✧ 与 IS 审计师讨论结果和建议，讨论审计目标和范围以及说明 IS 审计过程	P192
	IS 审计师	✧ 最终决定审计报告中应该包括或排除哪些内容，与管理人员讨论结果和建议，讨论审计目标和范围以及说明 IS 审计过程	P192、196
审计文档	IS 审计师	✧ 外部人员申请存取审计记录，审计师应事先获得相关高级管理层和法律顾问的批准； ✧ 制定有关保管、保留要求和审计记录的发布政策； ✧ 考虑如何保持审计测试证据的完整性和如何对其进行保护。	P201
控制自评估 CSA	IS 审计师	✧ 推动决策制定过程	P205

项目流程 RACI

项目管理流程 RACI 图 P216 A / F	CEO	CFO	BEM	CIO	BPO	DO	CA	DD	ITA	PMO	CARS
定义 IT 投资的项目群/投资组合管理框架	C	C	A	R	/	/	/	/	/	C	C
建立并维护 IT 项目管理框架	I	I	I	A/R	I	C	C	C	C	R	C
建立和维护 IT 项目监控、测量和管理系统	I	I	I	R	/	C	C	C	C	A/R	C
建立项目章程、进度表、质量计划、预算、沟通和风险管理计划	/	/	C	C	C	C	C	C	C	A/R	C
确保项目利益相关方的承诺和参与	I	/	A	R	C	/	/	/	/	/	C
确保项目和项目变更的有效控制	/	/	C	C	/	C	C	C	/	A/R	C
定义和实施项目保障和评审方法	/	/	I	C	/	/	/	I	/	A/R	C

R：责任人　　A：负责人　　C：被咨询人　　I：被通知人

A / F：活动/职能　　CEO：首席执行官　　CFO：首席财务官

BEM：业务执行经理　　DO：运营总监　　ITA：IT 行政主管
CIO：首席信息官　　CA：首席架构师　　PMO：项目管理官
BPO：业务流程所有者　　DD：开发总监

抽样方法及作用

抽样方法	运用条件及作用	例题
属性抽样	用于测试交易的合规性，如：交易经过了适当的审批	AS1-11、A1-46
变量抽样	在实质性测试的情况下使用，用于处理会发生变化的总体特征，如：货币值和重量	
停走抽样	当预期发生概率极低时使用，有助于限制样本大小，可让测试尽早停止	
判断抽样	用于确定样本量和样本元素选择标准的一种主观方法	
发现抽样	尝试确定是否发生某类事件时使用，适合评估欺诈风险，确定是否曾经发生过，发现之后深入分析	
概率比例规模抽样	通常与样本中有分组情况的整群抽样有关	

职业独立性与组织独立性区别：

职业独立性：审计师推荐了一个特定的供应商就会破坏职业独立性
组织独立性：组织独立性在接受约定时考虑

对独立性/客观性是否造成危害的情况：

造成危害	不造成危害
参与风险管理框架的设计（独立性）	为不同的实施方法提供建议（独立性）
对新数据库软件采用哪些应用程序控制提供建议（客观性）	协助风险意识培训（独立性）
为项目团队将来所需的许可费用提供评估（客观性）	对风险管理程序执行尽职调查（独立性）
在项目规划会议中就如何提高迁移率提供建议（客观性）	在执行验收测试之前，审查验收测试个案文档（客观性）

证据属性

属性	作用	例题
实用性	由审计目标决定	AS1-12
可靠性	使用 CAAT 收集并分析数据影响最大	
关联性	由审计目标决定	
充分性	由流程和制作数据的人员决定	

审计技术比较

抽样方法	运用条件及作用	例题
测试数据	将测试**是否存在某种控制可防止多付工资现象，但不会检测先前的具体错误计算**	AS1-28
通用审计软件 GAS（属于↓）	功能包括数学计算、分层、统计分析、顺序检查、重复检查和重新计算，可以设计适当测试来重新计算工资，从而确定是否存在多付工资的现象，以及**给哪些人多付了工资**	
计算机辅助审计技术 CAAT	通过 CAATs，IS 审计师可以**审查整个发票文件，以寻找能够满足选择条件的那些项**。可以审查主文件内容	

集成测试设施 ITF	不会检测前期的错误，在数据库中创建了一个虚拟实体，以便于实时输入同时处理测试交易，其优点是定期测试，不需要单独测试流程，但是周密的规划是有必要的，并且测试数据必须与生产数据分离	
系统控制审计复核文件 SCARF	使用预定义的异常情况，**监控超出预定义阀值交易最有效**	
决策支持系统 DSS	强调用户决策方法的灵活性，但无法指定目标和只使用模式	
嵌入式审计模块	不会检测前期的错误	

其他考点：

信息审计顺序

确定业务流程→控制目标及活动→关键信息资产→部署审计资源→约谈相关人员

第二章

基本职责归纳

活动	角色	职责	页码
公司治理	管理人员	指明战略方向从而确保实现目标、恰当解决风险并合理利用组织资源	P6
企业 IT 治理	董事会	从利益相关者（期待从投资中获得回报）的利益出发管理 IT 资源，督促管理层	P8
	管理层	按照负责管理此工作的董事的要求实施必要的制度和 IT 控制	
	高级管理层	指导和监督双重关注	P10
	IT 战略委员会	✧ 成员：董事会成员和非董事会成员的专家 ✧ 权利：向董事会和管理层提供 It 战略方面的建议 代表董事会起草战略并提交审批 关注当前和未来的 IT 战略问题 ✧ 职责：向董事会提供见解和建议 从业务角度的 IT 方向；IT 与业务方针的一致性；符合战略目标的 IT 资源、技能及基础设施的可用；优化 IT 成本，包括外部 IT 资源的角色和价值交付；IT 投资的风险、汇报和竞争力；重要 IT 项目的进展；IT 对业务的贡献（如交付预期业务价值）；IT 风险承受能力，包括合规性风险；IT 风险减缓；在 IT 战略方面向管理层提供指导；推动董事会的 IT 事务	P23
	IT 督导委员会	✧ 成员：主管执行层高管、业务执行层（关键用户）、首席信息官、所需关键顾问（IT、审计、法律、财务） ✧ 权利：协助执行层实现 IT 战略 监督 IT 服务交付及 IT 项目的日常管理 关注实施 ✧ 职责：如下 决定 IT 开销的整体水平以及如何分配；调整和批准企业 IT 架构；批准项目计划和预算、设定优先级和里程碑；获取并分配适当的资源；确保项目满足业务需求，包括对业务模式的再评估；监督项目执行，确保在预算内及时交付预期价值和既定产出；监督 IT 职能与企业各部门及各项目间的资源冲突和优先级冲突；对调整战略计划提出建议和要求（优先级、资金、技术方法及资源等）；与项目管理团队沟通战略目标；管理层企业 IT 治理职责的主要承担	

		者	
信息安全治理	董事会	支持管理层推进信息安全治理；参与政策审批、进行适当的监控、设定指标并进行报告和趋势分析；了解组织的信息资产及其对于业务持续运营的重要性	P32、P41~46
	高级管理层 CXO	推进与信息隐私以及信息安全本身相关的信息安全工作可解决与信息相关的风险、利益和过程领域的问题；参与政策审批、进行适当的监控、设定指标并进行报告和趋势分析；制定有效的信息安全策略需要业务流程负责人的合作和配合	
	督导委员会	成员：受影响团体高级代表，交流渠道，在设定优先顺序和权衡取舍时达成一致	
	首席信息安全专员 CISO	若没有 CISO 可由 CIO、CTO、CFO 甚至 CEO 担任，承担高级管理责任	
	首席风险官 CRO/首席合规官 CCO	没有则由高级管理层或董事会担任，承担信息安全责任	
信息系统战略	管理层、IS 督导委员会和战略委员会	提供与股东利益相关的重要战略性意见，对计划的制定和实施均起着重要作用	P56
	IS 审计师	考虑 CIO 或高级 IT 管理人员参与整体业务策略制定过程的方式，缺少参与将导致 IT 策略和计划与业务策略不一致	P58
	高级信息技术督导委员会	由企业高级管理层任命，成员包括高级管理层、用户管理部门以及 IS 部门的代表，对 IS 职能部门及其活动进行监管，确保 IS 部门与企业使命和目标协调一致	P59
政策	管理层	保持信息安全与业务目标一致方面的改进，组织信息安全管理方法及其过程的改进，控制目标和控制的改进，修订后的政策获得管理层批准，审查由管理层执行	P79
风险管理	董事会和高级管理层	选择风险应对措施（避免、降低、转移、接受）	P84
业务连续性计划 BCP	高级管理层	批准业务连续性政策	P247
	管理人员	基于 BIA 选择恢复策略	
	管理部门和用户	参与 BCP 将会影响其成功的执行	
业务影响分析 BIA	高级管理层	BIA 需要大力支持和资助	P256
	IT 人员和终端用户	广泛参与	

安全治理成果与管理职责关系 P45

管理层级	战略一致	风险管理	价值交付	绩效评测	资源管理	流程管理
董事会	需要显著的一致性	确定风险承受能力监督风险管理政策	需要安全活动成本报告	需要安全效果报告	监督知识管理和资源使用政策	监督保证流程整合政策
执行管理层	制定安全与业务目标的整合流程	确保在所有活动中明确了风险管理角色与职责监督法规符合性	需要安全工作的业务模式研究	需要监督和衡量安全活动	确保知识获取流程及其有效衡量	监督所有保证职能及其整合计划
指导委员会	对安全战略和整合工作进行检查并提供协助	识别新出现风险，推行业务单元安全实务并识别合规性问题	对服务与业务职能的安全工作的充分性进行检查并提出建议	对安全是否满足业务目标要求进行检查并提出建议	对知识获取与宣传流程进行督导	识别关键业务流程及其保证人指导保证整合工作
CISO/信息安全管理	制定安全战略、监督安全程序和	确保已执行风险和业务影响评估	监督安全资源的使用及其效果	制定并实施监督及衡量方法，指	制定知识获取与宣传方法，并制	与其他保证人员建立关联

层	工作、确保与业务流程所有人持续保持一致	制定风险减缓策略推行对法规的符合性政策		导和监督安全工作	定衡量其效果和效率的指标	确保识别并落实个保证工作的重叠及空缺部位
审计人员	评估并报告一致性程度	评估并报告企业风险管理实务及其结果	评估并报告效率	评估并报告衡量方式及所用指标的效果	评估并报告效果或资源管理	评估并报告由不同领域管理人员所执行的保证流程的效果

信息系统职责分离 P209

职责分离矩阵	控制组	系统分析员	应用程序员	帮助台和支持经理	最终用户	数据录入	计算机操作员	数据库管理员	网络管理员	系统管理员	安全管理员	系统程序员	质量保证人员
控制组		×	×	×		×	×	×	×	×		×	
系统分析员	×			×	×		×				×		×
应用程序员	×			×	×	×	×	×	×	×	×	×	×
帮助台和支持经理	×	×	×		×	×		×	×	×		×	
最终用户		×	×	×			×	×	×			×	×
数据录入	×		×	×			×	×	×	×	×	×	
计算机操作员	×	×	×		×	×		×	×	×	×	×	
数据库管理员	×		×	×	×	×	×		×	×		×	
网络管理员	×		×	×	×	×	×	×					
系统管理员	×		×	×		×	×	×				×	
安全管理员		×	×			×	×					×	
系统程序员	×		×	×	×	×	×	×		×	×		×
质量保证人员		×	×		×							×	

风险应对措施及举例

措施	举例	例题
转移	保险	A2-16、
缓解	互惠协议	
回避	停止带来风险的业务或活动	

接受	没有规避风险的方法，坦然接受，比如风险损失在可承受范围内	

控制措施及作用

措施	举例	例题
重叠控制	针对同一控制目标或暴露风险实施的两种控制	A2-83
边界控制	用于在计算机系统的目标用户与计算机系统本身之间建立接口，并且是基于个人而非角色的控制	
访问控制	基于个人而非角色	
补偿控制	内部控制，在无法适当分离职责时，可以降低现有或潜在的控制弱点可能面临的风险	

常用工具/分析方法的区别

工具/方法	举例	例题
业务连续性自我审计	用于评估业务连续性计划是否充分	A2-178
资源恢复分析	用于确定业务恢复策略	
风险评估	和业务影响评估均适用于了解业务之间连续性计划的工具	
差距分析	在业务连续性计划（BCP）中判断计划中的缺陷	

其他考点：

业务影响分析 BIA

BIA 的主要产出是了解运营中断成本，而不是 BCP

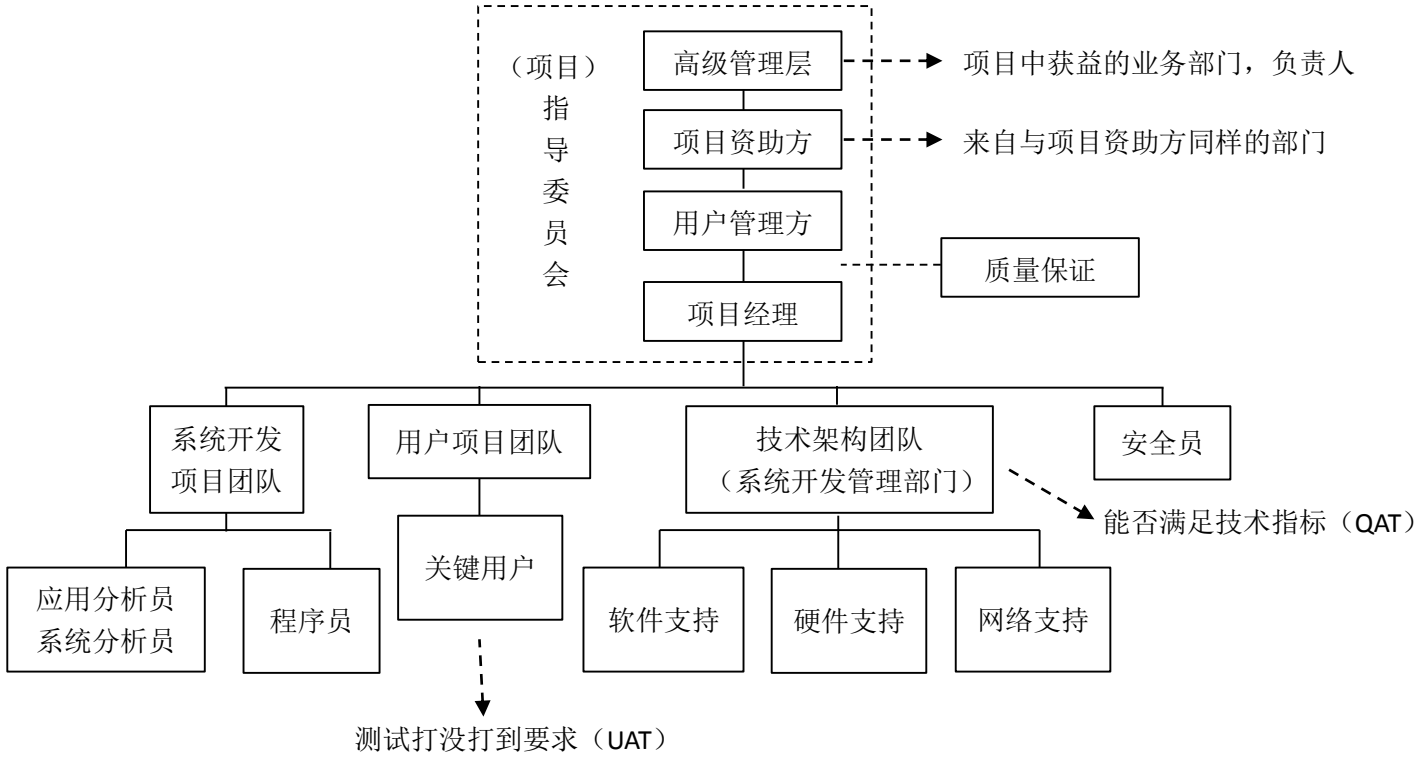
第三章

基本职责归纳

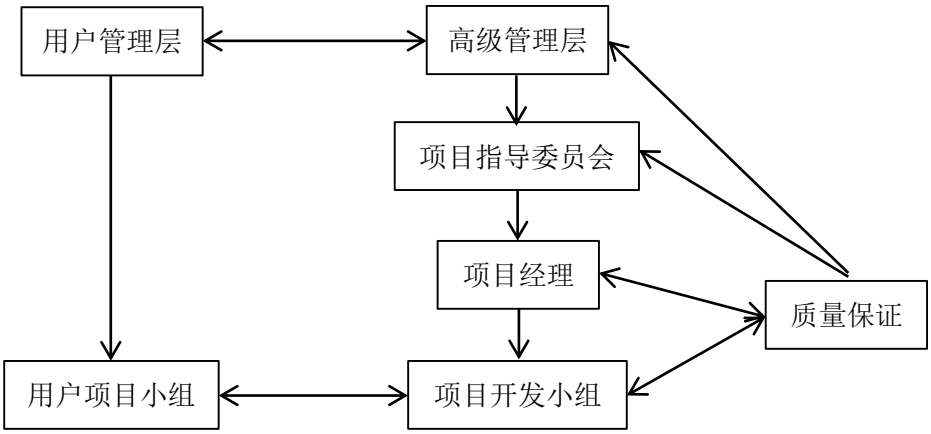
活动	角色	职责	页码
项目组合与项目群管里	项目管理办公室	提高项目和项目群的管理质量并保证项目顺利进行	P11
	IS 审计师	对审计项目内容和/或审计项目群/项目的流程加以区分	
项目中的团队及个人角色和职责	高级管理层	对项目负责，批准完成项目所需资源	P36
	用户管理层	派用户代表到项目团队中参与系统需求定义、验收测试和用户培训，评价和批准系统的交付	
	项目指导委员会	对项目工作提供总体指导，对所有的成本和时间表最终负责，定期评价项目进程，协调人和顾问。（组成：发起人、PM、职能部门代表）	
	项目发起人	为项目提供基金，与 PM 配合工作，定义成功标准	
	系统开发管理部门	对软硬件环境提供必要的技术支持，系统安装后的支持和维护	
	项目经理	对项目进行日常管理	
	系统开发项目小组	完成分配的开发任务，与用户沟通，向 PM 报告	
	用户项目小组	配合需求调查和进行验收测试	
	安全官员	安全管理、咨询、评价	
	质量保证	评价面向过程的活动和阶段结果	

项目启动	经理或发起人	启动项目，为要创建的项目收集通过审批所需的信息	P50
项目控制	CCB（代发起人）	评估与推荐	P75
风险管理	项目资助人	减轻对收益产生的冲击及对项目的存在性构成风险的。（第一类风险）	P78
	项目经理	减轻对项目本身产生的风险。（第二类风险）	
传统的 SDLC 各阶段描述	IS 审计师	主要关注是否在系统规格说明和测试计划中融入了适当的控制系统，是否在系统中内置了连续在线审计功能（尤其是电子商务应用和其他类型的物质环境）；还应关注并评估设计流程自身的效能（例如在使用结构化设计技术、原型设计和测试计划以及软件基线时），以建立正式的软件变更流程，从而在没有正式审查和批准过程的情况下对包含系统需求更改进行有效冻结。	P124
	QA	针对应用程序的各方面技术执行的质量保证测试（QAT），以及针对应用程序的各方面功能执行的用户验收测试（UAT）	P142
变更管理过程简介	编程人员/分析人员	允许使用紧急 ID/救火 ID，先执行变更，然后更新变更文档	P397
审计应用控制	IS 审计师	确定组件和控制薄弱环节，审查、分析和评估	P463

项目组织结构 P29



系统开发团队 P37



项目后审查与实施后审查区别 P80

项目后审查：参与人员为项目人员；目的是知识共享，流程改进；时间为项目结束后。
实施后审查：参与人员为非项目人员，独立的审计师；目的是确保项目满足预期的业务要求（主要目标）、评价项目收益、评估控制的充分性；时间为实施后 6 到 18 个月。
其他：确认符合技术标准、符合法规要求通常不是实施后审查的一部分，因为这应该是在设计和开发阶段需要解决的事情。

各类项目管理工具、技术、测试的作用和目的

名称	作用和目的	例题
Alpha 测试	Beta 测试的前一个阶段，通常由编程人员和业务分析人员执行，不由用户来执行，用于识别可以在外部用户开始 Beta 测试前修复的缺陷或故障	AS3-1 、AS3-4 、AS3-8 、A3-2 、A3-4 、A3-20 、A3-71
Beta 测试	测试的最终阶段，通常包括开发团队以外的用户，是用户验收测试的一种形式	
验证测试	用于根据详细的系统用功能需求做测试，以确保软件建设符合客户要求	
并行测试	将数据送入改良系统和备用系统，然后对二者的结果进行比较	
试点测试	先在一个位置想进行，然后再扩展到其他位置，校验其能否运行良好	
社交测试	用于测试系统是否可以在目标环境中运行，并且不会对现有系统产生不利影响	
软件质量保证或代码审查	用于确定开发标准是否得到贯彻	
回归测试	用于测试在应用变更后是否在系统中引入了新的错误	
白箱测试/白盒测试	涉及对程序代码行为进行详细审查，是在开发的设计和构建阶段适用于简单应用程序的质量保证技术，在 Alpha 之前，评估软件程序逻辑的有效性，在功能级别是否按预期方式运行	
黑盒测试	黑盒测试也称功能测试，它是通过测试来检测每个功能是否都能正常使用。在测试中，把程序看作一个不能打开的黑盒子，在完全不考虑程序内部结构和内部特性的情况下，在程序接口进行测试，它只检查程序功能是否按照需求规格说明书的规定正常使用，程序是否能适当地接收输入数据而产生正确的输出信息。黑盒测试着眼于程序外部结构，不考虑内部逻辑结构，主要针对软件界面和软件功能进行测试。	
程序输出测试	用户可以通过检查程序输入并将其与系统输出进行对比来测试输出，通常编程人员执行，用户完成同样有效	
系统配置	技术性过强及考虑安全方面的问题，很难由用户来完成	
程序逻辑说明	技术含量高，由编程人员执行	
性能调整	需要编程人员执行	
计划评估和审查技术 PERT	用于规划和控制系统项目的项目管理技术（最好、最坏、一般，三个时间表估算），**安排项目优先顺序最有效**	
功能指数分析 FPA	根据功能指数数量确定开发任务工作量的技术，功能指数包括输入、输出、查询、内部逻辑站点等因素，对安排项目活动的优先顺序没有帮助，例如：某个系统链接了 12 个模块，每个数据项可承载 10 个属性字段，**可以用 FPA 估算开发量**	
关键路径法 CPM	用于确定项目的关键路径，该路径代表**完成项目需要的可能的最短时间**	
源代码行计数	可直**接衡量程序规模**，但**无法顾及因拥有多个连接模块以及各种输入和输出所产生的复杂性**	

甘特图	通过与基准进行比较来确定已提前或延迟完成的活动，可以从甘特图**读取整个项目的进度**，以确定项目进度是落后、提前还是按进度进行，有助于安排欧系按顺序	
挣值分析 EVA	一种跟踪项目成本与项目交付成果之间关系的技术，但是对于安排任务的优先顺序没有帮助，但是没有 PERT 有效，**可对项目进行最佳测量**	
快速应用开发	可以使组织在减少开发成本和保障质量的同时更快地开发具有策略重要性的系统	
面向对象的系统开发	对解决方案进行规范和建模的过程	

SDLC 各阶段

名称	作用和目的	例题
验收测试	在系统人员完成除湿系统测试后执行，用于确定解决方案是否满足业务需求，此测试包括质量保障测试（QAT）和用户验收测试（UAT），但二者并不合并进行	A3-8 、A4-115
系统测试	系统测试与测试团队或系统维护人员执行的一系列测试相关，用于确保修改后的程序与其他组件正确交互，将参考系统的功能要求	
接口/集成测试	用于评估将信息从一个区域传递到另一个区域的两个或多个组件的连接情况，其目的是利用单元测试过的模块，根据设计构建集成结构	
单元测试	单元测试参考系统的详细设计，并使用一系列侧重于程序设计控制结构的案例来确保程序的内部操作按照规范执行	
压力测试	在计算机数量较少或系统资源匮乏的条件下运行测试。通常要进行软件压力测试的资源包括内部内存、CPU 可用性、磁盘空间和网络带宽	

质量评估指标

指标	说明	例题
报告重复性故障的平均间隔时间	反映了在修复首次报告的故障方面效率低下，并反映了相应团队或客户服务部门团队在处理报告问题时的情况	AS3-13
平均修复时间	反映了相应团队或客户服务部门团队在处理报告问题时的情况	
首次报告的故障平均间隔时间	反映了生产环境中用户报告的软件缺陷，帮助 IS 审计师评估已开发并适时的软件的质量	
响应时间	反映了相应团队或客户服务部门团队在处理报告问题时的灵活性	

攻击方法及说明

指标	说明	例题
缓冲区溢出	编写不良的代码遭到黑客利用，尤其在基于 Web 的应用程序中	AS3-98、A5-28 、A5-44 、A5-70
穷举攻击	用于破解密码	
死亡之 Ping	发送大小超过 65K 的数据包且没有加入分段标志	
跳步攻击	是指在一台或多台主机中使用远程网络技术以逃避攻击源地址被跟踪的行为，其实用通过非法手段从某主机中取得的用户 ID 和密码信息对另一台主机进行攻击	
否定应答 NAK 攻击	一种渗透技术，利用操作系统不能适当处理异步中断的潜在脆弱性，使在这类中断发生时该系统处于无保护状态	
分布式拒绝服务攻击 DDOS	会用大量数据包将目标淹没，以阻止其对合法请求作出响应	
战争拨号攻击	使用调制解调器扫描工具来破解专用交换机 PBX	

战争散步	一种设计到利用手持设备破坏无线网络安全的技术	
渗透测试	通过模拟来自恶意人员或黑客的攻击，来评估计算机系统或网络的安全性的方法	
社会工程	一项用于寻找人性漏洞，以获得组织机密或敏感信息的技术，被动攻击	
漏洞评估	一种通过运行自动扫描软件来举例系统和 IT 架构的漏洞，从而评估网络和服务器安全的方法	
冒充	一种模仿形式，一台计算机企图使用另一台计算机的身份	
中间人攻击	一种主动窃听，拦截双方计算机的会话，然后向双方转播相应的数据使会话继续，同时监控经过攻击者通道的数据	
端口扫描	一种侦查技术，可在发起更猛烈攻击之前，收集有关攻击目标的信息	

网络组件及其作用

指标	**说明**	**例题**
防火墙	防止网络间未授权访问的主要工具	AS3-138
路由器	可以根据参数（如源地址）过滤数据包，但不是主要的安全工具，根据介质访问控制 MAC 地址	
第二层交换机	将特定端口上的通信分为不同部分，但并不确定是经授权的通信还是未经授权的通信	
虚拟局域网 VLAN	一些交换机的功能，该功能使得交换机可以在不同端口间切换通信，如同这些端口在同一 LAN 中一样，然而这些交换机兵不厌就是经授权还是未经授权的通信	

开发方法描述及优缺点 P312

传统软件生命周期模型包括：瀑布模型、V 模型、原型法、演化模型、增量模型、螺旋模型、喷泉模型、构件组装模型、快速应用开发模型（RAD）

新型软件生命周期模型：敏捷模型

方法	**描述**	**例题**
瀑布模型	**定义阶段：**计划、需求分析；**开发阶段：**设计、编码、测试；**维护阶段：**运维；**评价并循环**	
V 模型	**弥补瀑布模型：**制定计划→获取用户需求①→系统和软件需求分析②→概要设计③→详细设计④→编码→单元测试（验证④）→组装测试/集成测试（验证③）→系统测试（验证②）→验收测试（验证①）	
原型法	可以减少误解，使需求准确，可支持软件生命周期的不同阶段。快速分析修改→快速构造→用户使用→评价反馈，循环	
演化模型	**提倡两次开发：**第一次是试验开发，得到试验性原型产品，其目标只是在于探索可行性，弄清软件需求，第二次在此基础上获得较为满意的软件产品	
增量模型	首先对系统最核心或最清晰的需求进行分析、设计、实现、测试并集成到系统中，再按优先级逐步对后续的需求进行上述工作，逐步建设成一个完整系统	
螺旋模型	主要针对大型软件项目的开发，引入明确的风险管理	
喷泉模型/迭代模型	软件开发过程的各个阶段是相互重叠和多次反复的，各个开发阶段没有特定的次序要求，完全可以并行进行，可以在某个开发阶段中随时补充其他任何开发阶段中遗漏的需求，**优点是：**提高开发效率、缩短开发周期、**缺点是：**难于管理	
构件组装模型	将整个系统模块化，并在一定构建模型的支持下复用构件库中的一个或多个软件构件，通过组装高效率、高质量地构造软件系统，本质上是演化的，过程是迭代的	
快速应用开发模型 RAD	增量型的软件开发过程模型，强调极端的开发周期	
敏捷模型	是一种态度，不是一个说明性过程，对已有生命周期模型的补充，本身不是一个完整的方法论，是可以借鉴的指导思想	

联机/在线事务处理数据完整性 ACID 原则

原则	描述	例题
原子性	全部完成或全部未完成，中断时之前操作全部撤销	
一致性	数据库中所有完整性条件的维持与每个业务信息相关，期间数据库将从一个一致性状态变到另一个一致性状态	
隔离性	每个业务都与其他业务相互隔离，所以每个业务只能访问一致性数据库状态的部分数据	
持久性	如果业务已经以完成状态汇报给客户，则产生的数据库更改应能够承受在此之后的硬件或软件故障	

其他考点：

第四章

基本职责归纳

活动	角色	职责	页码
质量保证	质量保证人员	验证系统变更在进入生产环境前已经在受控方式下得到授权、测试和实现	P43
问题管理报告审核	IS 审计师	保证问题管理机制正在得到适当维护，并且重要问题得到了充分重视和及时解决	P270
组织和职责分配	IS 和最终用户人员	应被确定为参与已制定的整个恢复流程，以恢复业务/过程和制定重要决策	P320~326
	事件应对团队	接受每个可被视为对资产/过程的威胁的时间的相关信息等（……）	
	应急行动团队	第一响应者、指定的消防检查员和救火队，负责处理火灾或其他紧急响应情景（……）	
	信息安全团队	制定维护相似级别的信息和 IT 资源安全所需步骤，使其在意外发生之前于主要站点准备就位，并在备用流程环境中实施所需的安全措施（……）	
	损失评估团队	在灾难发生后评估损失的程度（……）	
	应急管理团队	负责协调所有其他恢复/连续性/响应团队的活动，并制定关键的决策（……）	
	异地存储团队	负责获取、包装介质和记录并将其传输给恢复设施，以及建立和监督在恢复站点操作期间创建的信息的异地存储时间表	
	软件团队	负责恢复系统包、加载和测试操作系统软件，以及解决系统级问题	
	应用程序团队	到系统恢复站点工作，灾备份系统上恢复用户包和应用程序（……）	
	应急操作团队	在灾难和恢复项目的整个过程中对系统操作进行管理（……）	
	网络恢复团队	负责路由广域语音和数据通信流量，为数据通信提供不间断的支持（……）	
	通信团队	到恢复站点工作，与远程网络恢复小组合作建立用户/系统网络（……）	
	运输团队	将公司员工运输到远处的恢复站点（……）	
	用户硬件团队	对用户终端、打印机、打字机、影印机和其他必要设备的交付和安装进行定位和协调（……）	
	数据准备和记录团队	在连接到用户恢复站点的终端工作，负责更新应用程序数据库（……）	
	管理支持团队	向其他团队提供人员方面的支持并作为用户恢复站点的消息中心（……）	
	补给团队	联系供应商并协调后勤部门，确保不间断地提供必需的办公用品（……）	
	抢救团队	管理重新安置项目（……）	
	重新安置团队	协调从热备援中心转移到新地点或到已恢复的原位置的过程（……）	

	协调团队	负责协调位于不同地理位置的多个办公室的恢复工作（……）	
	法律事务团队	负责处理由于任何事故或服务的不可用等各种原因而产生的法律问题（……）	
	恢复测试团队	负责测试所制定的各种计划以及分析结果（……）	

恢复指标及作用

指标	作用	例题
恢复时间目标 RTO	灾难发生后，恢复业务功能或资源所允许的时间量，它并不能决定可接受的数据损失	AS4-3 、AS4-9 、AS4-18
恢复点目标 RPO	对给定数据的恢复策略影响最大，它是根据在发生运营中断时可接受的数据损失确定的，能够有效地量化在发生运营中断时允许的数据丢失量，在确保相关数据在系统之间适当同步方面最为关键，可以确保系统中不会包含来自不同时间点的数据，否则可能会导致会计交易无法对帐或参照完整性受损	
可容忍的最长断电时间 MTO	在发生灾难后，恢复业务功能或资源所允许的时间量，她对回复没有直接影响	
服务交付目标 SDO	与业务需求直接相关，是恢复正常状况之前在备用流程模式期间要达到的服务水平	
恢复服务的恢复力	用于衡量对数据异常的容错能力以及在发生内部故障后重新启动并从故障恢复的能力	
恢复服务的可扩展性	指的是恢复解决方案可能具有的与原始系统配置有关的容量约束和限制	

不同计划及作用

方式	目的	例题
事故应对计划 IRP	用于确定对诸如系统和/或网络受到攻击等事故做出的信息安全响应，此计划建立的流程能够是安全人员确定和减少恶意计算机事故（例如对系统或数据的未经授权访问，拒绝服务，或系统硬件软件的未授权更改）这些事故中恢复	A4-12
IT 应急计划	针对 IT 系统中断问题并建立了从主要应用程序或常规支持系统中恢复的流程	
业务连续性计划 BCP	针对的是各种业务流程	
运营连续性计划 COOP	针对的是组织最终使得一部分任务并且描述了短时间内在备用站点维持这些功能的流程	

检查校验方式及目的

方式	目的	例题
循环冗余校验 CRC	数据传输的有效性，根据帧的内容，在每个传输的帧中生成一组校验位	AS4-10、A3-36 、A3-37 、A4-42 、A5-78
数据验证	如：选择列表、交叉检查、合理性检查、总数核对控制、允许的字符检查等，数据输入的准确性	
校验和	验证所下载程序或其他所传输数据的完整性	
有效性检查	检查数据有效性是否符合预定标准	
合理性检查	将数据与数据的预定义合理限制或发生率作比较	
奇偶校验	是一种硬件控制，用以检测当数据从一台计算机读取到另一台计算机时。从内存中读取时，或在传输过程中发生的数据错误	
冗余校验	通过在每个数据段结尾追加经过计算的位来检测传输错误	

校验位	用以检测易位和抄写错误	
范围检查	检查数据是否符合预定的值范围	
重复检查	应将新交易与先前输入的交易进行匹配，以确保系统中不包含这些新交易	
回送校验	通过将数据重新传输到发送设备与原始传输进行比较来检测命令行错误	
反馈错误控制	传输的附加信息只能是接收方可以确认错误已经发生	
块总和校验	对奇偶校验的扩展，在字符块中计算出一组附加的校验位	
向前错误控制	涉及随字符或帧一起传输冗余的信息，以便于错误的检测及纠正	

廉价磁盘冗余阵列（RAID）

方式	目的	例题
RAID-0	将数据分条，存储到多个磁盘中，不带任何冗余信息，需要一个或多个磁盘，单独一个磁盘可以被认为是一个 RAID-0 阵列，**速度最快**，如果一个磁盘物理损坏，所有数据将无法使用	A4-156
RAID-1	至少有两个（只有两个）硬盘才能组成，可提供磁盘镜像，便于管理，确保数据的可用性，**可用性最高**，数据安全性最高，磁盘利用率最低，不会提高性能，数据写入时间会稍长一些，可同时读取，速度同 RAID-0，并且与身份认证及提供数据机密性毫无关系	
RAID-3	最常使用的磁盘阵列技术，至少需要 3 个硬盘，总容量之和为各个硬盘容量和减去一块的容量，数据分条存储在多个磁盘内，会产生奇偶校验并一起存储在磁盘内，对于大量的连续数据可提供很好的传输率，但对于随机数据，奇偶盘会成为写操作的瓶颈	
RAID-5	和 RAID-3 相似，都是数据分条，奇偶校验产生冗余，但它不采用一个固定的硬盘来存储奇偶校验值，数据和校验值都分布在所有硬盘上，最大好处是在一块盘掉线的情况下照常工作，相对于 RAID-0 容错性能好很多，因此 RAID-5 是 RAID 级别中最常见的一个类型	
RAID-10	容错功能和 RAID-1 相同，分条使用 RAID-1 段得到较高的 I/O 率，巧妙的利用了 RAID-0 的速度以及 RAID-1 的保护两种特性，缺点是硬盘数量多，至少必须拥有四个以上的偶数个硬盘才能使用	

OSI 七层结构

方式	目的	例题
应用层	为必须与网络设备进行通信的应用程序提供标准接口（如：打印已联网打印机上的文件、发送电子邮件或将数据存储与文件服务器）	
表示层	通过转换数据为应用层提供标准接口，同时提供常用通信服务（如：加密、文本压缩和重格式化），表示曾将传出数据转换为网络标准可接受的格式，然后将数据传到会话层，讲会话层收到的数据转换为应用层可接受的格式	
会话层	控制计算机之间的对话（会话），负责建立、管理和终止本地与远程应用层之间的连接，应用层之间的所有交流、数据交换和对话均由会话层管理	
传输层	提供端点间数据的可靠透明传输、端到端错误恢复和流控制，负责确保会话层发给自己的所有数据均被远程系统的传输层接收，负责确认从远程传输层收到的每个数据包得到确认，如果未收到确认则重发	
网络层	在本地设备的传输层与远程设备的传输层之间创建虚拟电路，此为堆栈中能够识别 IP 地址含义一层，负责路由转发，这一层通过将每个数据包转换为一帧或多帧，为数据链路层准备数据包	
数据链层	对物理链路中的数据进行可靠传输，从网络层接收数据包，将其封装成帧，然后以位流形式发送到物理层，进行各种错误校验	
物理层	提供硬件，通过相应介质或载体收发电气、光学或无线电信号等形式的位流，不进行错误纠正和检测	

备份方法优缺点

方法	优缺点	例题
完全备份	回复时**完整**，备份**时间长**，需要**介质容量大**	
增量备份	**较快恢复**，需要的**介质容量也较小**，但需要**所有备份集才能完全恢复**，花费**时间更长**	
差分备份	与完全备份相比：**较短的备份时间和较少的介质容量**，仅需要最近一次完全备份和最近一次差分备份介质进行恢复，与增量备份相比：恢复时间较短，但是由于备份数据是累计的，其每次备份的**时间较长且需要更大的介质容量**	

其他考点：

协议等安全性

以太网：明文，不安全
Telnet：远程终端连接的标准终端模拟协议，明文，不安全
FTP：文件传输协议，绕过防火墙，非授权修改、删除，不安全
SMTP：电子邮件传输协议，明文传输，不安全
SNMP：网络管理协议
NSP：网络服务提供商

容量/能力管理

DAS：直连存储，直接外挂存储服务器存储设备，**最经济的一种结构**
NAS：网络附加存储，网络上直接挂接的存储设备，**相当于一个网络文件共享服务器**
SAN：存储局域网络，应用光纤技术的 SAN 网络，传输介质为光纤，**性能最高，目前使用较广**
iSCSI（IP-SAN）：利用 TCP/IP 协议连接存储设备，可以理解为 SCSI over IP，是将 SCSI 命令封装到 TCP/IP 数据包中，通过 IP 网络传输 SCSI 数据

第五章

基本职责归纳

活动	角色	职责	页码
信息安全管理的关键因素	高级管理层	高级管理层的承诺和支持是成功和持续实施信息安全管理程序的重要保证	P18
	信息安全管理委员会	安全政策、准则和流程会影响整个组织，各级管理层代表英译委员会的形式会面，商讨问题以建立和批准相关安全实务	P22
	执行管理部门/高级经理层	负责总体的信息资产保护，以及发布和维护政策框架	
	公司行政高级管理层	对信息安全负责	
	安全顾问小组/咨询组	负责定义信息安全风险管理程序和可接受的风险等级，以及审查组织的安全计划	P23
	首席隐私官	制定和实施公司用来保护客户及员工隐私权的相关策略	
	首席信息安全专员/信息安全	制定和执行公司用来保护其信息资产的相关政策，职责范围比首席安全专员 CSO 更广泛，CSO 只负责组织内的物理安全，类似保卫部门	

	官 CISO		
	流程负责人/过程所有者	确保相应的安全措施符合组织政策并得到维护	P24
	信息资产所有者和数据所有者	对所拥有的资产承担相应的所有权责任，包括执行风险评估、选择可将风险降至可接受水平的适当控制，以及承担剩余风险	
	用户	遵循组织的安全政策中所阐述的流程，并遵守隐私和安全法规，包括医疗、金融、法律等较为敏感的应用领域	
	外部第三方	遵循组织的安全政策中所阐述的流程，并遵守隐私和安全法规，包括医疗、金融、法律等较为敏感的应用领域	P25
	安全管理员	员工级职位，负责充分确保 IS 程序、数据和设备的物理和逻辑安全，通常信息安全策略会提供基本准则，安全管理员可以依此执行操作。	
	安全专家/咨询顾问	帮助设计、实施、管理和审查组织的安全政策、标准及流程，只起辅助作用，不负责管理责任	
	IT 开发人员	在其应用程序内部实施信息安全保护	P26
	IS 审计师	就信息安全目标及其相关控制的适当性和有效性问题为管理人员提供独立保障	
审计信息安全管理框架	数据所有人	授予访问权限、确保访问规则在人员发生变动时得到更新，以及定期对其负责的数据进行访问规则审查	P324
	数据管理员	负责存储和保护数据，其中包括系统分析员和计算机操作等 IS 人员	P325
	安全管理员	负责充分确保 IS 程序、数据及设备的物理和逻辑安全	
	新 IT 用户	履行安全义务	P326
	数据用户	由数据所有者授权，由安全管理员监控	P327

渗透测试方法比较

方法	目的	例题
盲测	不向测试人员提供与组织网络有关的信息，渗透测试人员对目标信息系统毫不了解	AS5-15、AS5-30
双盲测试	事故响应团队并不知晓即将发生旨在评估其响应能力的入侵，此外，渗透测试人员实现也不知道要攻击的基础设施或目标	
外部测试	是指从组织外围发起的入侵尝试，但并不考虑测试人员或目标已了解哪些信息，还可用于从目标系统之外（如互联网）对目标的网络周边进行规避控制的行为	
内部测试	是指从组织网络内部发起攻击，事故响应团队事先可能已获得通知，尝试从外围的内部对目标进行攻击并规避控制，主要目的是确定如果外部网络被攻破或网络内部的授权用户想要损害网络中特定资源的安全，将会出现什么情况	
针对性测试	当目标的 IT 团队和测试人员都获得与目标和网络设计相关的信息时	

机密性与访问控制

名称	目的	例题
网络访问控制 NAC	位于网络层级，可限制对网络的系统访问	AS5-22、
公共密钥基础结构 PKI	用于公钥/私钥加密，尽管 PKI 本身可以存储在授权机制中，但并不是一种访问控制	
强制访问控制 MAC	由管理员强制执行的，最终用户不能对其进行更改，通常这是一种有效的预防性控制	
自主访问控制	是一种根据主体和/或主题所属组的身份限制对对象进行访问的方法，具有一定访问权限的主体能	

DAC	够将权限传递并给人以其他主体（可能是通过间接方式），从这个意义上说，控制具有任意性	

权限安全管理相关

名称	目的	例题
访问控制列表	访问控制列表是应用在路由器接口的指令列表，这些指令列表用来告诉路由器哪些数据包可以接收、哪些数据包需要拒绝	A5-48
安全日志文件	系统安全日志就是每次开关机、运行程序、系统报错时，这些信息都会被记录下来，保存在日志文件中。而日志文件会随着时间的增长而越集越多，从而影响系统速度。	
用户配置文件	用户配置文件就是在用户登录时定义系统加载所需环境的设置和文件的集合。它包括所有用户专用的配置设置，如程序项目、屏幕颜色、网络连接、打印机连接、鼠标设置及窗口的大小和位置等。	

电力安全相关

名称	目的（电压不稳稳压器，电流不稳 UPS）	例题
电压调节器	防止短期电源波动，通常不能防止长期电涌，在发生电源中断或丢失时，也不能维持完整性	A5-137
电源线调节器	可用于弥补电力供应的高峰和低谷，并将电力流量的峰值减小至机器所需的值，该设备中储存的电力可以消除谷值	
电涌保护器	防御高压脉冲，大电流，电压急升，短时中断（短时下降或急升，凹谷尖峰）	
不间断电源 UPS	中期中断，持续时间从几秒到 30 分钟不等	
备用电源	目的是延长计算机设备的运行时间，通常与不间断电源 UPS 等其它设备一起用于补偿电力损失，直至电源可以使用	

防火墙相关

名称	目的	例题
屏蔽路由器	能够基于地址、端口、协议、接口等允许或避免网络间或节点间通信的节点	A5-269、A5-275
数据包过滤器	检查在互联网和公司网络之间传送的每个数据包或数据的头	
应用网关	与电路网关相似，但其对于每个服务都使用特定代理，应用网关提供了很高等级和粒度的控制	
电路网关	用作外部和内部访问之间的中介的代理或程序	
屏蔽子网防火墙	还用作隔离区 DMZ，使用两个数据包过滤路由器和一个防御主机，这是最安全的防火墙系统	
屏蔽主机防火墙	使用数据包过滤器和防御主机	
双宿主机防火墙	属于限制性更强的屏蔽主机防火墙	
状态监测防火墙	在传输层运作，客队离开组织内部网络的每个数据包的目标互联网协议地址进行跟踪并允许来自记录的 IP 地址的回复	

其他考点：

公共密钥基础结构 PKI

PKI 不是访问控制

访问控制

IS 资源的库存→IS 资源的分类→IS 资源的标记→访问控制列表的创建