### 安全管理制度

| **序号** | **类别** | **测评项** | **测评实施** | **预期结果** | **说明** |
| --- | --- | --- | --- | --- | --- |
| 1 | 管理制度 | a）应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等。 | 1）应检查信息安全工作的总体方针和安全策略，查看文件是否明确机构安全工作的总体目标、范围、原则和安全框架等。 | 1）具有信息安全工作的总体方针和安全策略。  2）总体方针和安全策略里明确了机构安全工作的总体目标、范围、原则和安全框架等。 |  |
| b）应对安全管理活动中的各类管理内容建立安全管理制度。 | 1）应检查各项安全管理制度，查看是否覆盖安全管理活动中的各类管理内容（制度管理、机构管理、人员管理、系统建设管理和运维管理等方面）。 | 1）建立了安全管理制度。  2）安全管理制度覆盖了机构管理、制度管理、人员管理、系统建设和运维等层面的管理内容。 |  |
| c）应对安全管理人员或操作人员执行的日常管理操作建立操作规程。 | 1）应检查是否具有对重要管理操作的操作规程，如系统维护手册和用户操作规程等。 | 1）具有日常管理操作的操作规程。  2）操作规程覆盖了物理、网络、主机、应用等层面的重要操作规程（如系统维护手册和用户操作规程等）。 |  |
| 2 | 制定和发布 | a）应指定或授权专门的部门或人员负责安全管理制度的制定。 | 1）应访谈安全主管，询问由何部门或人员负责安全管理制度的制定，参与制定人员有哪些。 | 1）具有人员职责或岗位设置等相关文件。  2）文件明确了由专门的部门或人员负责安全管理制度的制定工作。 |  |
| 2）应检查人员职责、岗位设置等相关管理制度文件，查看是否明确由专门的部门或人员负责安全管理制度的制定工作。 |
| b）应组织相关人员对制定的安全管理进行论证和审定。 | 1）应访谈安全主管，询问安全管理制度的制定程序，是否对制定的安全管理制度进行论证和审定，论证和审定方式如何（如召开评审会、函审、内部审核等）。 | 1）具有管理制度评审记录，有评审意见。 |  |
| 2）应检查管理制度评审记录，查看是否具有相关人员的评审意见。 |  |
| c）应将安全管理制度以某种方式发布到相关人员手中。 | 1）应检查安全管理制度制定和发布要求管理文档，查看文档是否说明安全管理制度的制定、发布程序和发布范围等各项要求。 | 1）具有制度制定和发布要求的管理文档。  2）文档内容覆盖安全管理制度制定和发布程序。  3）各项安全管理制度文档都是通过正式、有效的方式发布的，如具有版本标识和管理层的签字或单位盖章。 |  |
| 3 | 评审和修订 | a）应定期或不定期对安全管理制度进行检查和审定，对存在不足或需要改进的安全管理制度进行修订。 | 1）应访谈安全主管，询问是否对管理制度定期修订，修订周期多长。询问系统发生重大安全事故、出现新的安全漏洞以及技术基础结构和组织结构等发生变更时是否对安全管理制度进行检查，对需要改进的制度进行修订。 | 1）具有安全管理制度的检查或评审记录。  2）如果有修订版本，具有修订版本的安全管理制度。 |  |
| 2）应检查是否具有安全管理制度修订记录。 |

### 安全管理机构

| **序号** | **类别** | **测评项** | **测评实施** | **预期结果** | **说明** |
| --- | --- | --- | --- | --- | --- |
| 1 | 岗位设置 | a）应设立信息安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责。 | 1）应访谈安全主管，询问是否设立安全管理机构（即信息安全管理工作的职能部门）。机构内部门设置情况如何，是否设立安全主管及安全管理各个方面的负责人，是否明确各部门和各负责人的职责。 | 1）具有部门、岗位职责文件。  2）文件中明确了职能部门、安全主管、负责人等相关职责。 |  |
| 2）应检查部门、岗位职责文件，查看文件是否明确安全管理机构的职责，是否明确机构内各部门和各负责人的职责和分工。 |  |
| b）应设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责。 | 1）应访谈安全主管，询问设置了哪些工作岗位（如安全主管、安全管理各个方面的负责人、机房管理员、系统管理员、网络管理员、安全管理员等重要岗位），是否明确各个岗位的职责分工。 | 1）具有部门、岗位职责文件。  2）文件中明确了系统管理员等相关岗位的工作职责。 |  |
| 2）应检查文件是否明确设置安全主管、安全管理各个方面的负责人、机房管理员、系统管理员、网络管理员、安全管理员等各个岗位，各个岗位的职责范围是否清晰、明确。 |  |
| 2 | 人员配备 | a）应配备一定数量的系统管理员、网络管理员、安全管理员等。 | 1）应访谈安全主管，询问各个安全管理岗位人员（如机房管理员、系统管理员、网络管理员、安全管理员等重要岗位人员）配备情况。 | 1）具有岗位与人员对应关系表。  2）表中每个岗位都有对应的人员。 |  |
| 2）应检查管理人员名单，查看其是否明确机房管理员、系统管理员、网络管理员、安全管理员等重要岗位人员的信息。 |  |
| b）应配备专职安全管理员，不可兼任。 | 1）应访谈安全主管，询问安全管理员的配备情况，是否是专职。 | 1）具有岗位与人员对应关系表。  2）确认表中的安全管理员是专职人员。 | 安全管理员不得兼任同一系统的系统管理员 |
| 2）应检查管理人员名单，确认安全管理员是否是专职人员。 |  |
| 3 | 授权和审批 | a）应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等。 | 1）应访谈安全主管，询问对哪些信息系统活动进行审批，审批部门是何部门，审批人是何人。 | 1）明确了各项审批事项的审批部门和审批人。 |  |
| b）应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度。 | 1）应访谈安全主管，询问其对重要活动的审批范围（如系统变更、重要操作、物理访问和系统接入、重要管理制度的制定和发布、人员的配备和培训、产品的采购、外部人员的访问等），审批程序如何，其中是否需要需要逐级审批。 | 1）与审批活动相关的制度（如变更管理、产品采购、机房管理等）中明确了审批程序以及重要活动的逐级审批流程。  2）具有经过逐级审批的文档。 |  |
| 2）应检查各类管理制度文档，查看文档中是否明确事项的审批程序（如列表说明哪些事项应经过信息安全领导小组审批，哪些事项应经过安全管理机构审批等），是否明确对重要活动进行逐级审批，由哪些部门/人员逐级审批。 |  |
| 3）应检查经逐级审批的文档，查看是否具有各级批准人的签字和审批部门的盖章。 |  |
| c）应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。 | 1）应检查审批事项的审查记录，查看是否对审批事项、审批部门、审批人的变更进行评审。 | 1）具有审查记录。  2）记录与文件要求一致。 |  |
| d）应记录审批过程并保存审批文档。 | 1）应检查关键活动的审批过程记录，查看记录的审批程序与文件要求是否一致。 | 1）具有各项活动的审批过程记录。  2）记录与文件要求一致。 |  |
| 4 | 沟通和合作 | a）应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通，定期或不定期召开协调会议，共同协作处理信息安全问题。 | 1）应访谈安全主管，询问与其它部门之间及内部各部门管理人员之间的沟通、合作机制。部门间、，安全管理职能部门内部以及信息安全领导小组或者安全管理委员会是否定期召开会议。 | 1）具有会议文件或会议记录。  2）文件或记录中有会议内容等描述。 |  |
| 2）应检查组织内部机构之间以及信息安全职能部门内部的安全工作会议文件或会议记录，查看是否具有会议内容、会议时间、参加人员和会议结果等描述。 |  |
| 3）应检查是否具有信息安全管理委员会或领导小组安全管理工作执行情况的文件或工作记录（如会议记录/纪要，信息安全工作决策文档等）。 |  |
| b）应加强与兄弟单位、公安机关、电信公司的合作与沟通。 | 1）应访谈安全主管，询问是否建立与公安机关、电信公司和兄弟单位等的沟通、合作机制。 | 1）与兄弟单位等建立了某种方式的沟通合作机制。  2）具有外联单位联系列表。  3）列表说明外联单位包含公安机关等。 |  |
| 2）应检查外联单位联系列表，查看外联单位是否包含公安机关、电信公司、兄弟公司等，是否说明外联单位的名称、联系人、合作内容和联系方式等内容。 |  |
| 5 | 审核和检查 | a）安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。 | 1）应访谈安全主管，询问是否组织人员定期对信息系统进行安全检查 查看检查内容是否包括系统日常运行、系统漏洞和数据备份等情况。 | 1）定期实施安全检查。 |  |

### 人员安全管理

| **序号** | **类别** | **测评项** | **测评实施** | **预期结果** | **说明** |
| --- | --- | --- | --- | --- | --- |
| 1 | 人员录用 | a）应指定或授权专门的部门或人员负责人员录用。 | 1）应访谈安全主管，询问由何部门/何人负责安全管理和技术人员的录用工作。 | 1）指定或授权专门的部门或人员负责录用工作。 |  |
| b）应严格规范人员录用过程，对被录用人的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核。 | 1）应访谈人事负责人，询问在人员录用时是否对被录用人的身份、背景、专业资格和资质进行审查，对技术人员的技术技能进行考核。 | 1）文档中有人员录用的要求，说明录用人员应具备的条件。  2）文档或记录中有审查内容和审查结果。  3）具有技能考核文档或记录。 |  |
| 2）应检查人员录用要求管理文档，查看是否说明录用人员应具备的条件，如学历、学位要求，技术人员应具备的专业技术水平，管理人员应具备的安全管理知识等。 |  |
| 3）应检查技能考核文档或记录，查看是否记录考核内容和考核结果等。 |  |
| c）应签署保密协议。 | 1）应访谈人事负责人，询问是否与录用后的技术人员签署保密协议。 | 1）具有保密协议。  2）协议中有保密范围、保密责任、违约责任、协议的有效期限和责任人的签字等内容。 |  |
| 2）应检查保密协议，查看是否具有保密范围、保密责任、违约责任、协议的有效期限和责任人的签字等内容。 |  |
| 2 | 人员离岗 | a）应严格规范人员离岗过程，及时终止即将离岗员工的所有访问权限。 | 1）应访谈人事负责人，询问是否及时终止离岗人员的所有访问权限。 | 1）文档有离岗管理的内容，规定了人员离岗要求。  2）具有离岗人员所有访问权限终止的记录。 |  |
| 2) 应检查人员离岗管理文档，查看是否规范人员离岗过程，并明确终止离岗人员的访问权限。 |  |
| b）应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。 | 1）应访谈人事负责人，询问是否及时取回离岗人员的各种身份证件、钥匙、徽章等以及机构提供的软硬件设备等。 | 1）具有离岗人员交还身份证件、设备等的登记记录。 |  |
| 2）应检查是否具有交还身份证件和设备等的登记记录。 |  |
| c）应办理严格的调离手续。 | 1）应访谈人事负责人，询问人员离岗是否办理调离手续。 | 1）管理文档中规定了人员调离手续。  2）具有按照离岗程序办理调离手续的记录。 |  |
| 2）应检查人员离岗管理文档，查看是否规定了调离手续和离岗要求等。 |  |
| 3）应检查保密承诺文档，查看是否具有调离人员签字。 |  |
| 3 | 人员考核 | a）应定期对各个岗位的人员进行安全技能及安全认知的考核。 | 1）应访谈安全主管，询问对各个岗位人员是否定期进行安全技能考核。 | 1）具有安全技能考核记录。  2）考核内容要求包含安全知识、安全技能等。 |  |
| 2）应检查考核记录，查看记录的考核人员是否包括各个岗位的人员，考核内容是否包含安全知识、安全技能等。查看记录日期与考核周期是否一致。 |  |
| 4 | 安全意识教育和培训 | a）应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训。 | 1）应访谈安全主管，询问是否对各类人员（普通用户、运维人员、单位领导等）进行安全教育、岗位技能和安全技术培训。 | 1）对各岗位人员进行了安全技能和意识培训。 |  |
| b）应对安全责任和惩戒措施进行书面规定并告知相关人员，对违反违背安全策略和规定的人员进行惩戒。 | 1）应访谈安全管理员、系统管理员、网络管理员和数据库管理员，考查其是否了解与工作相关的安全责任和惩戒措施等。 | 1）具有安全责任和惩戒措施管理文档。  2）文档包含具体的安全责任和惩戒措施。 |  |
| 2）应检查安全责任和惩戒措施管理文档，查看包括哪些具体的安全责任和惩戒措施。 |  |
| c）应对安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行培训。 | 1）应访谈安全主管，询问是否针对不同岗位制定不同的培训计划，并按照计划对各个岗位人员进行安全教育和培训。 | 1）具有安全教育和培训管理文档。  2）不同岗位的培训计划。  3）文档中明确了培训方式、培训对象、培训内容、培训时间和地点等，培训内容应包含信息安全基础知识、岗位操作规程等。 |  |
| 2）应检查安全教育和培训管理文档，查看是否明确规定应进行安全教育和培训。 |  |
| 3) 应检查安全培训计划文档，查看是否具有不同岗位的培训计划。查看计划是否明确了培训目的、培训方式、培训对象、培训内容、培训时间和地点等，培训内容是否包含信息安全基础知识、岗位操作规程等。 |  |
| d）应对安全教育和培训的情况和结果进行记录并归档保存。 | 1）应检查是否具有安全教育和培训的结果记录，查看记录中是否具有培训人员、培训内容、培训结果等的描述。查看记录与培训计划是否一致。 | 1）具有安全教育和培训的结果记录。  2）记录中有培训人员、培训内容、培训结果等的描述。  3）记录应与培训计划一致。 |  |
| 5 | 外部人员访问管理 | a）应确保在外部人员访问机房等重要区域前先提出书面申请，批准后由专人全程陪同或监督，并登记备案。 | 1）应检查外部人员访问相关规定，查看是否明确外部人员包括哪些人员，外部人员进入条件（对哪些重要区域的访问须提出书面申请批准后方可进入），外部人员进入的访问控制（由专人全程陪同或监督等）和外部人员的离开条件等。 | 1）具有外部人员访问管理文档。  2）文档中明确允许外部人员访问的范围，外部人员进入的条件，外部人员进入的访问控制措施等。  3）具有外部人员访问重要区域的书面申请文档。  4）文档中有批准人允许访问的批准签字等。  5）具有外部人员访问重要区域的登记记录。  6）记录中有外部人员访问重要区域的进入时间、离开时间、访问区域及陪同人等。 |  |
| 2）应检查外部人员访问重要区域批准文档，查看是否具有外部人员访问重要区域的书面申请，是否具有允许访问的批准签字等。 |  |
| 3）应检查外部人员访问重要区域的登记记录，查看记录是否描述了外部人员访问重要区域的进入时间、离开时间、访问区域、访问设备或信息及陪同人等。 |  |

### 系统建设管理

| **序号** | **类别** | **测评项** | **测评实施** | **预期结果** | **说明** |
| --- | --- | --- | --- | --- | --- |
| 1 | 系统定级 | a）应明确信息系统的边界和安全保护等级。 | 1）应访谈安全主管，询问是否明确信息系统的边界和安全保护等级。 | 1）具有定级文档。  2）定级文档中明确了信息系统边界。  3）定级文档中明确了信息系统安全保护等级。 |  |
| 2）应检查系统边界说明文档，查看文档是否明确信息系统边界和确定边界的理由。 |  |
| b）应以书面的形式说明确定信息系统为某个安全保护等级的方法和理由。 | 1）应检查系统定级文档，查看文档是否明确信息系统的安全保护等级确定的方法和理由。 | 1）具有定级文档。  2）定级文档中说明了确定信息系统安全保护等级的方法及理由。 |  |
| c）应确保信息系统的定级结果经过相关部门的批准。 | 1）应访谈安全主管，询问定级结果是否获得了相关部门（如上级主管部门）的批准。 | 1）具有相关部门对信息系统定级结果的批复文件或者定级文档中有相关部门的盖章或签字。 |  |
| 2）应检查系统定级文档，查看定级结果是否具有相关部门的批准盖章。 |  |
| 2 | 安全方案设计 | a）应根据系统的安全级别选择基本安全措施，并依据风险分析的结果补充和调整安全措施。 | 1）应访谈系统建设负责人，询问系统选择基本安全措施的依据，是否依据安全保护等级选择，是否依据风险分析的结果补充和调整安全措施。 | 1）系统建设/整改方案中有根据系统的安全级别选择基本安全措施的方法描述。  2）系统建设/整改方案中有根据风险分析结果调整安全措施的内容。 |  |
| 2）应检查系统建设/整改方案，是否根据系统的安全级别选择了基本安全措施。 |
| 3）应检查系统建设/整改方案，是否依据风险分析结果调整和补偿了安全措施。 |
| b）应以书面形式描述对系统的安全保护要求、策略和措施等内容，形成系统的安全方案。 | 1）应访谈安全主管，询问是否授权专门的部门对信息系统的安全建设进行总体规划，由何部门/何人负责。 | 1）部门岗位职责文档中说明有部门负责对信息系统的安全建设进行总体规划，或者有相关的授权文件。  2）具有系统安全建设工作计划。  3）系统安全建设工作计划中明确了近期和远期的安全建设计划。 |  |
| 2）应检查系统的安全建设工作计划，查看文件是否明确了系统的近期安全建设计划和远期安全建设计划。 |  |
| c）应根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件。 | 1）应访谈系统建设负责人，询问是否根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案等。 | 1）具有包含系统总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等方面内容的文件。  2）如是多个文件，文件内容之间相互保持一致。 |  |
| 2）应检查是否有系统总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等配套文件。 |
| 3）应检查配套文件之间是否保持一致。 |
| d）应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施。 | 1）应访谈系统建设负责人，询问是否组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略等相关配套文件进行论证和审定。 | 1）具有针对配套文件的论证和评审记录或文档，记录或文档中有相关论证意见。 |  |
| 2）应检查配套文件的论证评审记录或文档，查看是否有相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的论证意见。 |
| 3）应查看各个文件是否有机构管理层的批准。 |
| 3 | 产品采购和使用 | a）应确保安全产品的采购和使用符合国家的有关规定。 | 1）应访谈系统建设负责人，询问是否按照国家的相关规定进行采购和使用系统信息安全产品，。 | 1）抽样的安全产品具有相关凭证。 |  |
| 2）应抽样检查安全产品的相关凭证，如销售许可等，查看是否使用了符合国家有关规定产品。 |
| b）应确保密码产品的采购和使用符合国家密码主管部门的要求。 | 1）应访谈系统建设负责人，询问系统是否采用了密码产品，密码产品的使用是否符合国家密码主管部门的要求。 | 1）抽样的密码产品具有相关凭证。 |  |
| 2）应抽样检查密码产品的相关凭证，如销售许可等，查看是否使用了符合国家有关规定产品。 |
| c）应指定或授权专门的部门负责产品的采购。 | 1）应访谈系统建设负责人，询问是否具有专门的部门负责产品的采购。 | 1）部门职责文档中说明有专门的负责采购的部门，或者有相关的授权文件。 |  |
| 2）应检查部门职责文档或授权文件，是否明确产品采购职责部门。 |
| 4 | 自行软件开发 | a）应确保开发环境与实际运行环境物理分开，开发人员和测试人员分离，测试数据和测试结果受到控制。 | 1）应访谈系统建设负责人，询问系统是否自主开发软件，是否在独立的开发环境中编写、调试和完成。是否要求开发人员不能做测试工作，是否控制测试数据和测试结果。 | 1）网络拓扑图表明实际运行环境和开发环境间有效隔离。  2）人员岗位对应关系表中的开发人员与测试人员不同。  3）具有源代码、测试数据和测试结果的使用控制记录。 |  |
| 2）应检查是否具有软件开发相关文档（源代码、测试数据、测试结果等）的使用控制记录。 |
| 3）应检查网络拓扑图和实际开发环境，查看是否实际运行环境和开发环境有效隔离。 |
| b）应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则。 | 1）应检查是否具有软件开发管理制度。 | 1）具有软件开发管理制度。  2）软件开发管理制度中有相应内容。 |  |
| c）应确保提供软件设计的相关文档和使用指南，并由专人负责保管。 | 1）应访谈系统建设负责人，询问是否由专人保管软件设计的相关文档。 | 1）具有软件设计相关文档。  2）软件使用指南或操作手册等。  3）专人负责文档保管。 |  |
| 2）应检查是否具有软件设计的相关文档（应用软件设计程序文件、源代码说明文档等）和软件使用指南或操作手册和维护手册等。 |  |
| 5 | 外包软件开发 | a）应根据开发需求检测软件质量。 | 1）应访谈系统建设负责人，询问软件交付前是否依据开发协议的技术指标对软件功能和性能等进行验收检测。 | 1）具有软件验收测试结果记录。  2）软件验收测试结果记录内容包括需求说明文档中的内容。 |  |
| 2）应检查软件验收测试结果记录，并检查测试内容是否与软件需求说明文档一致。 |  |
| b）应在软件安装之前检测软件包中可能存在的恶意代码。 | 1）应访谈系统建设负责人，软件安装之前是否检测软件中的恶意代码，检测工具是否是第三方的商业产品。 | 1）具有针对软件包的恶意代码检测报告，如防病毒软件扫描结果等。 |  |
| 2）应检查是否有针对该软件包的恶意代码检测报告。 |
| c）应要求开发单位提供软件设计的相关文档和使用指南。 | 1）应访谈系统建设负责人，询问是否具有软件设计的相关文档和使用指南。 | 1）具有软件开发的相关文档，如需求分析说明书、软件设计说明书、测试文档等。  2）具有软件操作手册或使用指南。 |  |
| 2）应检查是否具有需求分析说明书、软件设计说明书、软件操作手册等开发文档。 |  |
| d）应要求开发单位提供软件源代码，并审查软件中可能存在的后门。 | 1）应访谈系统建设负责人，询问开发单位是否提供了软件源代码，对其是否经过审查明确不存在后门。 | 1）具有软件源代码。  2）具有源代码审查记录或表明不存在后门的证明文件。 |  |
| 2）应检查软件源代码审查记录，查看是否包括对可能存在后门的审查结果。 |
| 6 | 工程实施 | a）应指定或授权专门的部门或人员负责工程实施过程的管理。 | 1）应访谈系统建设负责人，询问是否指定专门部门或人员按照工程实施方案的要求对工程实施过程进行进度和质量控制。 | 1）部门职责文档中明确说明有部门或人员负责工程实施过程管理，或有相关授权文件。 |  |
| 2）应检查部门或人员岗位职责文档或授权文件，是否将工程实施过程的管理职责指定或授权了某部门或人员负责。 |
| b）应制定详细的工程实施方案控制实施过程，并要求工程实施单位能正式地执行安全工程过程。 | 1）应检查工程实施方案，查看其是否规定工程时间限制、进度、控制、质量控制等方面内容，工程实施过程是否按照实施方案形成各种文档，如阶段性工程进程汇报报告。 | 1）具有工程实施方案。  2）工程实施方案包括相关控制内容。  3）具有按照工程实施方案进行各类控制的过程文档和阶段性文档。 |  |
| 7 | 测试验收 | a）应对系统进行安全性测试。 | 1）应访谈系统建设负责人，询问在信息系统正式运行前，是否委托第三方测试机构根据设计方案或合同要求对信息系统进行独立的安全性测试。 | 1）具有系统安全性测试报告。  2）测试报告有第三方测试单位的签字或盖章。 |  |
| 2）应检查是否具有第三方测试机构出示的系统安全性测试验收报告。 |  |
| b）应在测试验收前根据设计方案或合同要求等制订测试验收方案，测试验收过程中详细记录测试验收结果，形成测试验收报告。 | 1）应检查工程测试验收方案，查看其是否对参与验收部门、人员、现场操作过程等进行要求。查看测试记录是否详细记录了测试时间、人员、操作过程、测试结果等方面内容。查看测试报告是否提出存在问题及改进意见等。 | 1）具有测试验收方案。  2）测试验收方案与设计方案或合同要求内容一致。  3）测试验收方案中有参与测试的部门、人员、测试验收内容、现场操作过程等内容。  4）具有测试验收报告。  5）测试验收报告或测试验收记录中详细记录了验收结果。 |  |
| c）应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。 | 1）应访谈系统建设负责人，询问是否根据设计方案或合同要求组织相关部门和人员对测试报告进行符合性审定。 | 1）具有对系统测试验收报告进行审定的意见。 |  |
| 2）应检查是否具有相关部门和人员对系统测试验收报告进行审定的意见,是否有相关部门或人员的签字或盖章。 |
| 8 | 系统交付 | a）应制定详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点。 | 1）应访谈系统建设负责人，询问是否根据交付清单对所交接的设备、文档、软件等进行清点，交付清单是否满足合同的有关要求。 | 1）具有系统交付清单。 |  |
| 2）应检查是否具有系统交付清单。 |  |
| b）应对负责系统运行维护的技术人员进行相应的技能培训。 | 1）应访谈系统建设负责人，询问目前的信息系统是否由内部人员独立运行维护，如果是，系统建设实施方是否对运维技术人员进行过技能培训。 | 1）具有系统交付时的技术培训记录。  2）培训记录包括培训内容、培训时间和参与人员等内容。 |  |
| 2）应检查是否有系统交付技术培训记录，查看是否包括培训内容、培训时间和参与人员等。 |
| c）应确保提供系统建设过程中的文档和指导用户进行系统运行维护的文档。 | 1）应检查是否具有系统建设文档（如系统建设方案）、指导用户进行系统运维的文档（如服务器操作规程书）以及系统培训手册等文档。 | 1）具有系统建设过程中的文档（如系统设计方案等）。  2）具有指导用户进行系统运维的文档（如用户操作手册等）。 |  |
| 9 | 安全服务商选择 | a）应确保安全服务商的选择符合国家的有关规定。 | 1）应访谈系统建设负责人，询问对信息系统进行安全规划、设计、实施、维护、测评等服务的安全服务单位是否符合国家有关规定。 | 1）安全服务商具有符合国家规定的资质文件。 |  |
| 2）应检查选择的安全服务商的安全资质文件。 |
| b）应与选定的安全服务商签订与安全相关的协议，明确约定相关责任。 | 1）应检查是否具有与产品供应商、软件开发商、系统集成商、系统运维商和等级测评机构等相关安全服务商签订的协议。 | 1）具有与所有安全服务商签订的安全责任合同书或保密协议文档。  2）文档中有保密范围、安全责任、违约责任、协议的有效期限和责任人的签字等内容。 |  |
| c）应确保选定的安全服务商提供技术培训和服务承诺，必要的与其签订服务合同。 | 1）应访谈系统建设负责人，询问是否要求选定的安全服务商提供一定的技术培训和服务。 | 1）具有与所有安全服务商签订的服务承诺或服务合同文档。  2）文档中有后期的技术培训、技术支持和服务等相关内容。 |  |
| 2）应检查与安全服务商签订的服务合同或安全责任合同书，查看是否明确了后期的技术支持和服务承诺等内容。 |

### 系统运维管理

| **序号** | **类别** | **测评项** | **测评实施** | **预期结果** | **说明** |
| --- | --- | --- | --- | --- | --- |
| 1 | 环境管理 | a）应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理。 | 1）应访谈物理安全负责人，询问是否指定专人或部门对机房的基本设施（如空调、供配电设备等）进行定期维护，由何部门/何人负责。 | 1）指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理。  2）具有对空调、温湿度控制等机房设施定期维护保养的记录。 |  |
| 2）应检查机房基础设施的维护记录，查看是否记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容。 |  |
| b）应指定部门负责机房安全，并配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理。 | 1）应访谈物理安全负责人，询问是否指定部门和人员负责机房安全管理工作。 | 1）文件明确指定部门并配备人员负责机房的安全。 |  |
| 2）应检查部门或人员岗位职责文档，查看是否明确机房安全的责任部门及人员。。 |
| c）应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定。 | 1）应检查机房安全管理制度，查看其内容是否覆盖机房物理访问、物品带进、带出机房和机房环境安全等方面。 | 1）具有机房安全管理制度。  2）制度内容包括机房物理访问、物品带进、带出机房和机房环境安全等方面。 |  |
| d）应加强对办公环境的保密性管理，规范办公环境人员行为，包括工作人员调离办公室应立即交还该办公室钥匙、不在办公区接待来访人员、工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸档文件等。 | 1）应访谈物理安全负责人，询问是否对办公环境保密性进行管理。 | 1）文档明确规范办公环境内人员的行为。  2）工作人员离开座位确保终端计算机退出登录状态。  3）桌面上没有包含敏感信息的纸档文件。 |  |
| 2）应检查办公环境管理文档，查看是否对办公人员的相关行为进行规范。 |  |
| 2 | 资产管理 | a）应编制并保存与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。 | 1）应检查资产清单，查看其内容是否覆盖资产责任人、所属级别、所处位置、所处部门等方面。 | 1）具有资产清单。  2）内容包括资产责任部门、责任人、所处位置和重要程度。 |  |
| b）应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门, 并规范资产管理和使用的行为。 | 1）应访谈安全主管，询问是否指定资产管理的责任部门或人员。 | 1）具有资产安全管理方面的制度。  2）制度中明确信息资产管理的责任部门、责任人。  3）制度内容包括资产使用、借用、维护。 |  |
| 2）应检查资产管理制度，查看其内容是否覆盖资产使用、维护等方面。 |  |
| 3 | 介质管理 | a）应确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理。 | 1）应访谈资产管理员，询问介质存放于何种环境中，是否对存放环境实施专人管理。 | 1）具有介质存放在安全的环境（防潮、防盗、防火、防磁，专用存储空间）。  2）具有介质存放、使用管理记录。  3）专人管理。 |  |
| 2）应检查介质使用管理记录，查看其是否记录介质归档和使用等情况。 |
| b）应对介质归档和查询等进行登记记录，并根据存档介质的目录清单定期盘点。 | 2）应检查介质安全管理制度中是否包括在介质物理传输过程中的对人员选择、打包、交付等情况进行控制的内容。对介质归档和查询等是否有登记记录。是否有并根据存档介质的目录清单进行定期盘点的记录。 | 1）介质安全管理制度中包括在介质物理传输过程中对人员选择、打包、交付等情况进行控制的内容。  2）具有介质归档和查询的记录。  3）具有存档介质定期盘点的记录。 |  |
| c）应对存储介质的使用过程、送出维修以及销毁等进行严格的管理，对带出工作环境的存储介质进行内容加密和监控管理，对送出维修或销毁的介质应首先清除介质中的敏感数据，对保密性较高的存储介质未经批准不得自行销毁。 | 1）应访谈资产管理员，询问对送出维修或销毁的介质如何管理，销毁前是否对数据进行净化处理。 | 1）介质安全管理制度中包括对存储介质的使用过程、送出维修以及销毁等进行严格管理的方法和对带出工作环境的存储介质进行内容加密和监控管理的方法。  2）对带出工作环境的存储介质进行内容加密并有领导批准。  3）对保密性较高的介质销毁前有领导批准。  4）具有送修记录。  5）具有带出记录。  6）具有销毁记录。 |  |
| 2）应检查介质安全管理制度，查看是否包括对存储介质的使用过程、送出维修以及销毁等进行严格管理的方法和对带出工作环境的存储介质进行内容加密和监控管理的方法。对带出工作环境的存储介质是否进行内容加密并有领导批准。对保密性较高的介质销毁前是否有领导批准。是否有存储介质的送修、带出和销毁记录。 |
| d）应根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同。 | 1）应访谈资产管理员，询问是否对某些重要介质实行异地存储，异地存储环境是否与本地环境相同。 | 1）具有介质存放在安全的异地环境（防潮、防盗、防火、防磁，专用存储空间）。  2）专人管理。 |  |
| 2）应检查介质本地存放的实际环境条件是否是安全的。 |  |
| e）应对重要介质中的数据和软件进行分类和标识管理。 | 1）应访谈资产管理员，询问对重要介质中的数据和软件是否进行保密性处理，对介质是否根据重要性不同进行分类标识。 | 1）重要介质中的数据采取加密存储。  2）介质上具有分类的标识或标签。  3）标识或标签与介质管理制度的要求一致。 |  |
| 2）应检查介质，查看是否对其进行了分类，并具有不同标识。 |  |
| 4 | 设备管理 | a）应对信息系统相关的各种设备（包括备份和冗余设备）、线路等指定专人或专门的部门定期进行维护管理。 | 1）应访谈资产管理员，询问是否对各类设施、设备指定专人或专门部门进行定期维护。 | 1）文件明确专门的部门或人员对各种设备、线路进行定期维护。 |  |
| 2）应检查部门或人员岗位职责文档，是否明确设备维护管理的责任部门。 |
| b）应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理。 | 1）应访谈资产管理员，询问是否对设备选用的各个环节（选型、采购、发放等）进行规范化管理。 | 1）具有设备安全管理制度。  2）制度内容包括对各种软硬件设备的选型、采购、发放和领用的申报、审批和专人负责的规定。 |  |
| 2）应检查设备安全管理制度，查看其是否对设备选型、采购、发放以及带离机构等环节的申报和审批作出规定。 |  |
| c）应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作。 | 1）应检查设备操作手册，查看其内容是否覆盖设备启动、停止、加电、断电等操作，对象是否覆盖终端计算机、工作站、便携机、系统和网络等设备。 | 1）操作手册中对象覆盖终端计算机、工作站、便携机、系统和网络等设备。  2）具有主要设备（包括备份和冗余设备）的启动、停止、加电/断电等操作的操作手册 |  |
|  |
| d）应确保信息处理设备必须经过审批才能带离机房或办公地点。 | 1）应访谈资产管理员，询问对带离机房的设备是否经过审批，由何人审批。 | 1）具有信息处理设备带离机房或办公地点的审批记录。 |  |
| 2）应检查是否具有信息处理设备带离机房或办公地点的审批记录。 |
| 5 | 网络安全管理 | a）应指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作。 | 1）应访谈安全主管，询问是否指定专人负责维护网络安全管理工作。 | 1）人员岗位信息表中指定了专人负责网络管理。 |  |
| 2）应检查相关部门或人员岗位职责文档，查看是否明确网络安全管理的责任人。 |
| b）应建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定。 | 1）应检查网络安全管理制度，查看其内容是否覆盖网络安全配置（包括网络设备的安全策略、授权访问、最小服务、升级与打补丁）、审计日志保存时间、升级与打补丁等方面。 | 1）具有网络安全管理制度，至少包括网络安全配置、系统升级、权限控制、日志管理、口令策略等。 |  |
| c）应根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份。 | 1）应访谈网络管理员，询问是否对网络设备进行过升级，更新前对现有的重要文件是否进行备份。 | 1）具有网络设备升级更新的工作记录。 |  |
| 2）应检查网络设备运维维护工作记录，是否对网络设备进行升级更新，并在更新前备份现有配置数据。 |
| d）应定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞进行及时的修补。 | 1）应访谈安全管理员，询问是否对网络进行过漏洞扫描，并对发现的漏洞进行及时修补。 | 1）具有漏洞扫描报告，且时间间隔与安全管理制度中规定的扫描周期一致。 |  |
| 2）应检查是否具有网络漏洞扫描报告。 |  |
| e）应实现设备的最小服务配置，并对配置文件进行定期离线备份。 | 1）应访谈安全管理员，询问对设备的安全配置是否遵循最小服务原则，是否对配置文件进行备份。 | 1）配置文件中只启用了必要的网络服务（参照技术检查结果）。  2）具有网络设备配置数据的离线备份。 |  |
| 2）检查网络设备是否实现了最小服务配置，是否具有网络设备配置文件的备份文件。 |
| f）应保证所有与外部系统的连接均得到授权和批准。 | 1）应访谈安全管理员，询问系统网络的外联种类（互联网、合作伙伴企业网、上级部门网络等）是否都得到授权与批准，由何人/何部门批准。是否定期检查违规联网的行为。 | 1）具有授权和批准与外部系统的连接的文档。 |  |
| 2）应检查是否具有内部网络外联的授权批准书。 |  |
| 6 | 系统安全管理 | a）应根据业务需求和系统安全分析确定系统的访问控制策略。 | 1）应访谈系统管理员，询问是否根据业务需求和系统安全分析确定系统的访问控制策略。 | 1）具有系统安全访问控制策略说明文档。  2）文档内容完备。 |  |
| 2）应检查是否具有系统安全访问控制策略说明文档，是否规定了根据业务需求和系统安全分析制定系统的访问控制策略，控制分配文件及服务的访问权限。 |
| b）应定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补。 | 1）应访谈系统管理员，询问是否对系统进行过漏洞扫描，发现漏洞是否进行了及时修补。 | 1）具有系统漏扫策略文档，文档中规定了扫描周期、对象等。  2）扫描报告和策略中的扫描周期应一致。  3）具有漏洞记录表及修复结果记录表或系统加固报告。 |  |
| 2）应检查系统漏洞扫描报告，查看其内容是否描述了系统存在的漏洞、严重级别、原因分析和改进意见等方面。 |  |
| c）应安装系统的最新补丁程序，在安装系统补丁前，首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装。 | 1）应访谈系统管理员，询问在安装系统补丁程序前是否经过测试，并对重要文件进行备份。 | 1）具有补丁测试记录和系统安装操作记录。  2）安装较新系统补丁（参考技术检查结果）。 |  |
| 2）应检查是否有补丁测试记录和系统补丁安装操作记录。 |
| d）应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出具体规定。 | 1）应检查系统安全管理制度，查看其内容是否覆盖系统安全配置（包括系统的安全策略、授权访问、最小服务、升级与打补丁）、系统账户（用户责任、义务、风险、权限审批、权限分配、账户注销等）、审计日志以及配置文件的生成、备份、变更审批、符合性检查等方面。 | 1）具有系统安全管理制度。  2）制度中系统安全策略、安全配置、日志管理和日常操作流程等内容完备。 |  |
| e）应依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作。 | 1）应检查系统操作手册，查看其内容是否覆盖操作步骤、维护记录、参数配置等方面。 | 1）具有系统操作规程。  2）系统操作规程完备。 |  |
| f）应定期对运行日志和审计数据进行分析，以便及时发现异常行为。 | 1）应访谈审计员，询问是否定期对系统审计日志进行分析。 | 1）具有定期的日志分析报告。 |  |
| 2）应检查是否有定期对系统运行日志和审计数据的分析报告。 |
| 7 | 恶意代码防范管理 | a）应提高所有用户的防病毒意识，及时告知防病毒软件版本，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查。 | 1）应访谈系统运维负责人，询问是否对员工进行基本恶意代码防范意识的教育，如告知应及时升级软件版本。 | 1）具有相关的培训文档。 |  |
| 2）应检查是否有对员工的恶意代码防范教育的相关培训文档，文档内容涵盖相关内容。 |
| b）应指定专人对网络和主机进行恶意代码检测并保存检测记录。 | 1）应访谈系统运维负责人，询问是否指定专人对恶意代码进行检测，并保存记录。 | 1）具有恶意代码检测记录。 |  |
| 2）应检查是否具有对网络和主机进行恶意代码检测的记录。 |
| c）应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定。 | 1）应检查恶意代码防范管理文档，查看其内容是否覆盖防恶意代码软件的授权使用、恶意代码库升级、定期汇报等方面。 | 1）具有恶意代码防范方面的管理制度。  2）内容完备。 |  |
| 8 | 密码管理 | a）应建立密码使用管理制度，使用符合国家密码管理规定的密码技术和产品。 | 1）应访谈安全管理员，询问密码技术和产品的使用是否遵照国家密码管理规定。 | 1）密码技术和产品有国家密码管理的相关资质和证明。  2）具有完整的密码管理制度。 |  |
| 2）应检查是否具有密码使用管理制度。 |  |
| 9 | 变更管理 | a）应确认系统中将发生的变更，并制定变更方案。 | 1）应访谈系统运维负责人，询问是否制定变更方案指导系统执行变更。 | 1）具有系统变更方案。  2）变更方案内容和规定对变更类型、变更原因、变更过程、变更前评估等方面进行了说明。 |  |
| 2）应检查系统变更方案，查看其是否对变更类型、变更原因、变更过程、变更前评估等方面进行规定。 |  |
| b）应建立变更管理制度，重要系统变更前，应向主管领导申请，变更和变更方案经过评审、审批后方可实施变更，并在实施后将变更情况向相关人员通告。 | 1）应检查变更管理制度，查看其是否覆盖变更前审批、变更过程记录、变更后通报等方面内容。 | 1）具有变更管理制度。  2）具有变更方案评审记录。  3）具有变更申请和批准的相关记录。 |  |
| 2）应检查是否具有变更方案评审记录和变更过程记录文档。 |  |
| 3）应检查重要系统的变更申请书，查看其是否具有主管领导的批准。 |  |
| 10 | 备份与恢复管理 | a）应识别需要定期备份的重要业务信息、系统数据及软件系统等。 | 1）应访谈系统管理员、数据库管理员和网络管理员，询问是否识别需定期备份的业务信息、系统数据及软件系统。 | 1）具有需要定期备份的重要业务信息、系统数据、软件系统的列表或清单。 |  |
| 2）应检查是否具有定期备份的重要业务信息、系统数据、软件系统的列表或清单。 |
| b）应建立备份与恢复管理相关的安全管理制度，对备份信息的备份方式、备份频度、存储介质和保存期等进行规范。 | 1）应检查是否具有规定备份方式、频度、介质、保存期的安全管理制度。 | 1）具有数据备份与恢复管理制度。  2）制度内容应包括备份方式、备份频度、存储介质和保存期、等方面内容。 |  |
| c）应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略应指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法。 | 1）应检查数据备份和恢复策略文档，查看其内容是否覆盖数据的存放场所、文件命名规则、介质替换频率、数据离站传输方法等方面。 | 1）具有数据备份与恢复策略。  2）策略内容应包括备份数据放置场所、文件命名规则、介质替换频率和将数据离站运输的方法等方面内容。 |  |
| 11 | 安全事件处置 | a）应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点。 | 1）应访谈系统运维负责人，询问是否告知用户在发现安全弱点和可疑事件时应进行及时报告。 | 1）具有对发现的安全弱点和可疑事件形成的对应的报告或相关文档。  2）报告或相关文档对安全弱点和可疑事件描述清晰并详细。 |  |
| 2）应检查是否有系统运维过程中发现的安全弱点和可疑事件对应的报告或相关文档，内容是否详实。 |
| b）应制定安全事件报告和处置管理制度，明确安全事件的类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责。 | 1）应检查安全事件报告和处置管理制度，查看其是否明确与安全事件有关的工作职责，包括报告单位（人）、接报单位（人）和处置单位等职责。 | 1）具有安全事件报告和处置管理制度。  2）安全事件报告和处置管理制度内容明确了安全事件类型，规定了安全事件的现场处理、事件报告和后期恢复的管理职责及流程。 |  |
| c）应根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分。 | 1）应访谈系统运维负责人，询问是否了解本系统已发生的和需要防止发生的安全事件，对识别出的安全事件是否根据其对系统的影响程度划分不同等级。 | 1）相关报告和文档内容有对安全事件进行分级（安全事件根据其对系统的影响程度划分不同等级，主要有哪几类等），并有相关处置方法等内容。  2）安全事件定级文档明确了安全事件的定义、安全事件级别划分的原则、级别描述等方面内容。 |  |
| 2）应检查安全事件定级文档，查看其内容是否明确安全事件的定义、安全事件等级划分的原则、等级描述等方面内容。 |  |
| d）应制定安全事件报告和响应处理程序，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等。 | 1）应检查事件报告和响应处理程序，查看其内容是否包括事件的报告流程、响应处理方法等。 | 1）具有各级安全事件响应流程。 |  |
| e）应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存。 | 1）应检查安全事件记录分析文档，查看其是否记录引发安全事件的系统弱点，是否分析不同安全事件发生的原因。 | 1）具有安全事件处理记录和分析文档。  2）文档有事件原因、处理过程、补救措施等内容。  3）处理过程与管理规定处理一致。 |  |
| f）对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序。 | 1）应访谈工作人员，询问其不同安全事件的报告流程。 | 1）具有重大安全事件（系统中断、信息泄密）的不同报告和处理程序文档。  2）文档内容明确具体报告方式、报告内容、报告人等方面内容。 |  |
| 2）应检查安全事件报告和处理程序文档，查看其是否根据不同安全事件制定不同的处理和报告程序，是否明确具体报告方式、报告内容、报告人等方面内容。 |  |
| 13 | 应急预案管理 | a）应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容。 | 1）应检查应急响应预案框架文档，查看其内容是否覆盖启动计划的条件、应急处理流程、系统恢复流程和事后教育等内容。 | 1）具有应急预案框架。  2）应急预案框架包括应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等方面内容。  3）根据应急预案框架制定的各不同事件的专项预案。 |  |
| 2）应检查是否具有不同事件的应急预案。 |  |
| b）应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障。 | 1）应访谈系统运维负责人，询问是否具有应急响应小组，是否具备应急设备并能正常工作，应急预案执行所需资金是否做过预算并能够落实。 | 1）具体应急预案框架中包括应急小组人员名单、应急设备清单、第三方技术支持人员名单和财务概算等内容。 |  |
| 2）应检查应急预案框架，查看是否包括人员名单、应急设备（软硬件）清单、第三方技术支持人员名单、财务概算等。 |
| c）应对系统相关的人员进行应急预案培训，对应急预案的培训应至少每年举办一次。 | 1）应访谈系统运维负责人，询问是否对系统相关人员进行应急预案培训。 | 1）具有应急预案培训记录。  2）培训记录内容包括培训内容、培训日期等。 |  |
| 2）应检查是否具有应急预案培训记录。 |  |