变更记录：

序号	变更原因	变更内容	编制（变更）人/时间	批准人/时间	备注
1	新建	全部，版本A/0	葛方隽/2022.9	吕萍/2022.9	

安全物理环境（S3A3G3）作业指导书					
控制点	**安全要求**	**要求解读**	**测评方法**	**预期结果或主要证据**	**符合情况**
物理位置选择	[一般]a)机房场地应选择在具有防震、防风和防雨等能力的建筑内。	机房场地所在的建筑物要具有防震、防风和防雨等的能力	1)核查是否没有雨水渗漏的痕迹 2)核查是否没有可灵活开启的窗户，若有窗户，是否做了封闭、上锁等防护措施 3)核查屋顶、墙体、门窗和地面等是否有破损开裂的情况	1)机房具有验收文档 2)天花板、窗台下无水渗漏的现象 3)机房无窗户，或有窗户且做了防护措施 4)现场观测屋顶、墙体、门窗和地面等无开裂的情况	符合情况：没有雨水渗漏的痕迹；没有可灵活开启的窗户，若有窗户，做了封闭、上锁等防护措施 ；屋顶、墙体、门窗和地面等无破损开裂的情况 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。
物理位置选择	[重要]b)机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。	机房场地要避免设置在建筑物的顶层或地下室。如果因为某些原因无法避免时，设置在建筑物顶层或地下室的机房需要加强防水和防潮措施	1)核查机房是否在顶层或地下室 2)若是，核查机房是否采取了防水和防潮措施	1)非建筑物顶层或地下室 2)在顶层或地下室的，做了严格的防水防潮措施	符合情况：机房不在顶层或地下室；若在顶层或地下室，机房采取了防水和防潮措施。 不符合情况：机房在顶层或地下室，且未采取了防水和防潮措施。
物理位置选择	[关键]c)机房应避开火灾危险程度高的区域，周围100米内不得有加油站、燃气站等危险建筑。（F3）	机房应避开火灾危险程度高的区域	1)核查机房周围100米内是否有加油站。 2)核查机房周围100米内是否有燃气站。	1)机房周围100米内无加油站、燃气站等危险建筑	符合情况：机房周围100米内无加油站、燃气站等危险建筑 不符合情况：机房周围100米内有加油站、燃气站等危险建筑
物理访问控制	[关键]a)机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。	为防止非授权人员进入机房，需要安装电子门禁系统对机房及机房内区域的出入人员实施访问控制，避免由于非授权人员的擅自进入，造成系统运行中断、设备丢失或损坏、数据被窃取或篡改，并可利用系统实现对人员进入情况的记录	1)核查出入口是否配置电子门禁系统 2)核查电子门禁系统是否开启并正常运行 3)核查电子门禁系统是否可以鉴别、记录进入的人员信息	1)机房出入口配备电子门禁，可使用门禁卡、指纹开启 2)电子门禁系统工作正常，可对进出人员进行鉴别 3）如果电子门禁不能鉴别人员，需要人员出入登记表，包括姓名、单位、联系方式、事由、时间等内容	符合情况：配置电子门禁系统；电子门禁正常运行；可以鉴别、记录进入的人员信息。 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。
物理访问控制	[关键]b)应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或 安装等过渡区域。（F3）	机房要进行区域划分，区域之间要设置物理隔离装置。重要区域前要设置交付或 安装等过渡区域。	1)核查机房是否进行区域划分。 2)若已划分区域，则核查机房区域之间是否设置物理隔离装置。 3)核查在重要区域前是否设置交付或安装等过渡区域。	1)机房内进行区域划分 2)区域之间设置物理隔离装置 2)重要区域前设置交付或安装等过渡区域。	符合情况：机房进行区域划分，区域之间设置物理隔离装置，重要区域前设置过渡区。 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。

防盗窃和防破坏	[一般]a)应将设备或主要部件进行固定，并设置明显的不易除去的标识。	对于安放在机房内用于保障系统正常运行的设备或主要部件需要进行固定，并设置明显的不易除去的标记用于识别	1)核查机房内设备或主要部件是否固定 2)核查机房内设备或主要部件上是否设置了明显且不易除去的标记	1)机房内设备均放置在机柜或机架，并已固定 2)设备或主要部件均设置了不易除去的标识、标志，如使用粘贴方式则不能有翘起	符合情况：机房内设备或主要部件固定放置；设置了明显且不易除去的标记。 部分符合情况：满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。
防盗窃和防破坏	[一般]b)应将通信线缆铺设在隐蔽安全处。	机房内通信线缆需要铺设在隐蔽安全处，防止线缆受损	核查机房内通信线缆是否铺设在隐蔽安全处	机房通信线缆铺设在线槽或桥架里	符合情况：机房内通信线缆铺设在隐蔽安全处 。 部分符合情况：机房内通信线缆部分铺设在隐蔽安全处 。 不符合情况：机房内通信线缆未铺设在隐蔽安全处 。
防盗窃和防破坏	[关键]c)应设置机房防盗报警系统或设置有专人值守的视频监控系统，非7*24小时人员值守和巡查的 机房，主要出入口应安装红外线探测设备等光电防盗设备，一旦发现有破坏性入侵即时显示 入侵部位，并驱动声光报警装置。（F3）	机房需要安装防盗报警系统，或在安装视频监控系统的同时安排专人进行值守，非7*24小时人员值守和巡查的机房，主要出入口要安装红外线探测设备等光电防盗设备，防止盗窃和恶意破坏行为的发生。	1)核查是否配置防盗报警系统或专人值守的视频监控系统 2)若非7*24小时人员值守和巡查的机房，核查是否安装红外线探测设备等光电防盗设备，当发现有破坏性入侵即时显示入侵部位，并驱动声光报警装置。 3)核查防盗报警系统或视频监控系统是否开启并正常运行	1) 机房内配置了防盗报警系统或专人值守的视频监控系统 2） 非24小时值守的，机房出入口配备红外线探测设备等光电防盗设备，一旦发现有破坏性入侵即时显示 入侵部位，并驱动声光报警装置。 3） 现场观测时监控系统正常工作	符合情况：配置防盗报警系统或专人值守的视频监控系统；防盗报警系统或视频监控系统开启并正常运行。 部分符合情况：满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。
防盗窃和防破坏	[关键]d)应建立机房视频监控系统和动环监控系统，并对监控内容进行记录，对机房风冷水电设备、 消防设施、门禁系统等重要设施实行连续24小时全面监控，视频监控记录和门禁系统出入记 录至少保存3个月。（F3）	需要部署机房视频监控系统和动环监控系统，并对监控内容进行记录，对机房风冷水电设备、 消防设施、门禁系统等重要设施实行连续24小时全面监控，视频监控记录和门禁系统出入记 录至少保存3个月。	1)核查机房是否部署视频监控系统和动环监控系统。 2)核查是否对机房风冷水电设备、消防设施、门禁系统等重要设施实行连续24小时全面监控。 3)核查视频监控系统和动环监控系统是否正常运行，视频监控记录和门禁系统出入记录是否保存3个月。	1) 机房内配置了视频监控系统和动环监控系统 2）对机房风冷水电设备、消防设施、门禁系统等重要设施实行连续24小时全面监控， 3）视频监控记录和门禁系统出入记 录至少保存3个月。	符合情况：机房内配置了视频监控系统和动环监控系统。对机房风冷水电设备、 消防设施、门禁系统等重要设施实行连续24小时全面监控。视频监控记录和门禁系统出入记 录至少保存3个月。 部分符合情况：满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。
防雷击	[重要]a)应将各类机柜、设施和设备等通过接地系统安全接地。	在机房内对机柜、各类设施和设备采取接地措施，防止雷击对电子设备产生 损害	核查机房内机柜、设施和设备等是否进行接地处理，通常黄绿色相间的电线为接地用线	机房内所有机柜、设施和设备等均已采取了接地的控制措施	符合情况：机柜、设施和设备等进行接地处理。 部分符合情况：部分机柜、设施和设备等进行接地处理。 不符合情况：机柜、设施和设备等未进行接地处理。

防雷击	[重要]b)应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。	在机房内安装防雷保安器或过压保护等装置,防止感应雷对电子设备产生损害	1)核查机房内是否设置防感应雷措施	1)机房内设置了防感应雷措施，如设置了防雷感应器、防浪涌插座等 2)防雷装置通过了国家有关部门的技术检测	符合情况：设置了防感应雷措施。 不符合情况：未设置防感应雷措施
防雷击	[关键]c)机房应通过相关防雷验收，并定期对防雷设施进行维护和防雷检测。（F3）	机房需要通过相关防雷验收，并定期对防雷设施进行维护和防雷检测。	1)核查机房是否通过相关防雷验收。 2)核查是否定期对防雷设施进行维护和防雷检测。 3)核查是否有相关防雷验收、防雷检测和设施维护记录和报告。	1)机房通过相关防雷验收，并定期对防雷设施进行维护和防雷检测。 2)具有防雷验收文档和维护记录	符合情况：机房通过相关防雷验收，并定期对防雷设施进行维护和防雷检测。具有防雷验收文档和维护记录 部分符合情况：满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。
防火	[关键]a)机房应设置火灾自动消防系统，能够通过在机房内、基本工作房间内、活动地板下、吊顶里及易燃物附近部位设置烟感、温感等多种方式进行自动检测火情、自动报警，并自动灭火。（F3）	机房内需要设置火灾自动消防系统，可在发生火灾时进行自动检测、报警和灭火，如采用自动气体消防系统、自动喷淋消防系统等	1）核查机房内是否设置火灾自动消防系统 2)核查火灾自动消防系统是否可以自动检测火情、自动报警并自动灭火	1)机房内设置火灾自动消防系统 2)现场观测时火灾自动消防系统工作正常	符合情况：设置火灾自动消防系统；可以自动检测火情、自动报警并自动灭火。 部分符合情况：满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。
防火	[一般]b)机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。	机房内需要采用具有耐火等级的建筑材料，防止火灾的发生和火势蔓延	核查机房验收文档是否明确所用建筑材料的耐火等级	机房所有材料为耐火材料，如使用墙体、防火玻璃等，但使用金属栅栏的不能算符合	符合情况：机房采用具有耐火等级的建筑材料进行建设。 部分符合情况：机房内部分房间采用具有耐火等级的建筑材料进行建设。 不符合情况：机房未采用具有耐火等级的建筑材料进行建设。
防火	[重要]c)应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。	机房内需要进行区域划分并设置隔离防火措施，防止水灾发生后火势蔓延	1)核查是否进行了区域划分 2)核查各区域间是否采取了防火隔离措施	1)机房进行了区域划分，如过渡区、主机房 2)区域间部署了防火隔离装置	符合情况：进行了区域划分；区域间采取了防火隔离措施。 部分符合情况：满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。

防火	[关键]d)机房应备有一定数量的对电子设备影响小的手持式灭火器，消防报警系统应具有与空调系统、 新风系统、门禁系统联动的功能，一般工作状态为手动触发。 (F3)	机房需要备有一定数量的对电子设备影响小的手持式灭火器，消防报警系统应具有与空调系统、 新风系统、门禁系统联动的功能，一般工作状态为手动触发。	1)核查是否机房内配备有对电子设备影响小的手持式灭火器，如手持式干粉灭火器等。 2)核查消防报警系统是否与空调系统、 新风系统、门禁系统进行联动，一般工作状态下是否为手动触发。	1)机房内配备有对电子设备影响小的手持式灭火器，如手持式干粉灭火器等。 2)消防报警系统与空调系统、 新风系统、门禁系统进行联动，一般工作状态下是否为手动触发。	符合情况：机房内配备有对电子设备影响小的手持式灭火器。消防报警系统与空调系统、新风系统、门禁系统进行联动，一般工作状态下是否为手动触发。 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。
防火	[关键]e)机房内部通道设置、装修装饰材料、设备线缆等应满足消防要求，并对机房进行消防验收， 纸张、磁带和胶卷等易燃物品要放置于防火柜内。 (F3)	机房内部通道设置、装修装饰材料、设备线缆等需要满足消防要求，需要对机房进行消防验收， 纸张、磁带和胶卷等易燃物品要放置于防火柜内。	1)核查机房内部通道设置、装修装饰材料、设备线缆等是否满足消防要求，是否采用防火材料。 2)核查机房是否进行消防验收，是否具备消防验收材料。 3)核查机房内纸张、磁带和胶卷等易燃物品是否放置防火柜内。	1)机房内部通道设置、装修装饰材料、设备线缆等满足消防要求，采用防火材料。 2)机房进行消防验收，具备消防验收材料。 3)机房内纸张、磁带和胶卷等易燃物品放置防火柜内。	符合情况：机房内部通道设置、装修装饰材料、设备线缆等满足消防要求，采用防火材料。机房进行消防验收，具备消防验收材料。机房内纸张、磁带和胶卷等易燃物品放置防火柜内。 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。
防火	[关键]f)主机房宜采用管网式洁净气体灭火系统，也可采用高压细水雾灭火系统，应同时设置两种火 灾探测器，且消防报警系统应与空调系统、新风系统、门禁系统、灭火系统联动，凡设置洁 净气体灭火系统的主机房，应配置专用空气呼吸器或氧气呼吸器。 (F3)	主机房需要采用管网式洁净气体灭火系统，也可采用高压细水雾灭火系统，需要同时设置两种火灾探测器，且消防报警系统应与空调系统、新风系统、门禁系统、灭火系统联动，凡设置洁净气体灭火系统的主机房，应配置专用空气呼吸器或氧气呼吸器。	1)核查机房是否有设置相关气体灭火系统和高压细水雾灭火系统。 2)核查消防报警系统是否与空调系统、新风系统、门禁系统、灭火系统联动。 3)若采用气体灭火，则核查机房内是否配置专用空气呼吸器或氧气呼吸器。	1)机房有设置相关气体灭火系统和高压细水雾灭火系统。 2)消防报警系统与空调系统、新风系统、门禁系统、灭火系统联动。 3)若采用气体灭火，机房内配置专用空气呼吸器或氧气呼吸器。	符合情况：机房有设置相关气体灭火系统和高压细水雾灭火系统。消防报警系统与空调系统、新风系统、门禁系统、灭火系统联动。若采用气体灭火，机房内配置专用空气呼吸器或氧气呼吸器。 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。
防火	[关键]g)应定期检查消防设施，每年至少组织各运维相关部门联合开展一次针对机房的消防培训和演 练。 (F3)	需要定期检查消防设施，每年至少组织各运维相关部门联合开展一次针对机房的消防培训和演 练。	1)核查是否定期检查消防设施。 2)核查是否每年至少组织各运维相关部门联合开展一次针对机房的消防培训和演练。 3)核查是否具备设施检查记录和消防培训和演练记录。	1)定期检查消防设施。 2)每年至少组织各运维相关部门联合开展一次针对机房的消防培训和演练。 3)具备设施检查记录和消防培训和演练记录。	符合情况：定期检查消防设施。每年至少组织各运维相关部门联合开展一次针对机房的消防培训和演练。具备设施检查记录和消防培训和演练记录。 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。

防火	[关键]h)机房应设置消防逃生通道，同时应保证机房内各分区到各消防通道的道路通畅，方便人员逃 生时使用，在机房通道上应设置显著的消防标志。（F3）	机房需要设置消防逃生通道，同时保证机房内各分区到各消防通道的道路通畅，方便人员逃生时使用，在机房通道上应设置显著的消防标志。	1)核查机房内是否设置消防逃生通道。 2)核查逃生通道是否通畅。 3)核查逃生通道上是否设置显著的消防标志。	1)机房内设置消防逃生通道。 2)逃生通道通畅。 3)逃生通道上设置显著的消防标志。	符合情况：机房内设置消防逃生通道。逃生通道通畅。逃生通道上设置显著的消防标志。 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。
防水和防潮	[重要]a)应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。	机房内需要采取防渗漏措施，防止窗户、屋顶和墙壁存在水渗透情况	核查窗户、屋顶和墙壁是否采取了防渗漏的措施	机房采取了防雨水渗透的措施，如: 1）封锁了窗户并采取了防水，或者设置双层固定式玻璃窗，并设置雨棚 2）在屋顶铺设防水层； 3）机房墙壁设置彩钢板或采用防水涂层；	符合情况：窗户、屋顶和墙壁采取了防渗漏的措施。 不符合情况：窗户、屋顶和墙壁未采取防渗漏的措施
防水和防潮	[一般]b)应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。	机房内需要采取防结露和排水措施，防止水蒸气结露和地面产生积水	1)核查是否采取了排水措施，防止地面产生积水	1)机房内配备了专用的精密空调来防止水蒸气结露的控制措施 2)机房内部署了漏水检测装置，可以对漏水进行监控报警	符合情况：采取了排水措施，防止地面产生积水 不符合情况：未采取排水措施，防止地面产生积水
防水和防潮	[关键]c)为便于地下积水的转移，漏水隐患区域地面周围应设排水沟或地漏等排水设施，当采用吊顶 上布置空调风口时，风口位置不宜设置在设备正上方以避免水蒸气结露和渗透。（F3）	漏水隐患区域地面周围需要设排水沟或地漏等排水设施，当采用吊顶上布置空调风口时，风口位置不宜设置在设备正上方以避免水蒸气结露和渗透。	1)核查机房内漏水隐患区域地面周围是否设排水沟或地漏等排水设施。 2)若采用吊顶上布置空调风口时，核查出风口是否设置在设备正上方。	1)机房内漏水隐患区域地面周围设排水沟或地漏等排水设施。 2)若采用吊顶上布置空调风口时，出风口未设置在设备正上方。	符合情况：机房内漏水隐患区域地面周围设排水沟或地漏等排水设施。若采用吊顶上布置空调风口时，出风口未设置在设备正上方。 部分符合情况： 满足上述其中一点，但未完全满足所有条
防水和防潮	[重要]d)应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。	机房内需要布设对水敏感的检测装置，对渗水、漏水情况进行检测和报警	1)核查是否安装了对漏水的检测装置	1)机房内部署了漏水检测装置，如漏水检测绳等 2)检测和报警工作正常	符合情况：安装了对漏水的检测装置；可以进行检测和报警。 部分符合情况：安装了对漏水的检测装置，但不可以进行检测和报警。 不符合情况：未安装对漏水的
防水和防潮	[关键]e)应对温湿度调节设备安装漏水报警装置，并设置防水堤，还应注意冷却塔、泵、水箱等供水 设备的防冻、防火措施。（F3）	对温湿度调节设备安装漏水报警装置，并设置防水堤，还应注意冷却塔、泵、水箱等供水设备的防冻、防火措施。	1)核查机房内针对于精密空调排水口是否安装有漏水报警装置，是否设置防水提。 2)核查针对冷却塔、泵、水箱等供水设备是否设置有防冻、防火措施。	1)机房内针对于精密空调排水口安装有漏水报警装置，设置防水提。 2)针对冷却塔、泵、水箱等供水设备设置有防冻、防火措施。	符合情况：机房内针对于精密空调排水口安装有漏水报警装置，设置防水提。针对冷却塔、泵、水箱等供水设备设置有防冻、防火措施。 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足

防静电	[重要]a)应采用防静电地板或地面并采用必要的接地防静电措施。	机房内需要安装防静电地板或在地面采取必要的接地措施,防止静电的产生	1)核查是否安装了防静电地板 2)核查是否采用了防静电接地措施	1)机房部署了防静电地板 2)机房采用了接地的防静电措施	符合情况：安装了防静电地板；采用来防静电接地措施。 不符合情况：未安装防静电地板；未采用防静电接地措施。
防静电	[重要]b)应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。	机房内需要配备静电消除器E佩戴防静电手环等消除静电的设备。	核查机房内是否配备了静电消除器、佩戴防静电手环。	机房配备了防静电设备	符合情况：配备了静电消除器、佩戴防静电手环。 不符合情况：未配备静电消除器、未佩戴防静电手环。
防静电	[关键]c)主机房和辅助区内的工作台面宜采用导静电或静电耗散材料。（F3）	主机房和辅助区内的工作台面需要采用导静电或静电耗散材料。	1)核查主机房和辅助区内是否设置工作台。 2)若有，核查工作台面是否采用导静电或静电耗散材料。	1)主机房和辅助区内设置工作台。 2)工作台面采用导静电或静电耗散材料。	符合情况：主机房和辅助区内设置工作台。工作台面采用导静电或静电耗散材料。 部分符合情况：满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。
温湿度控制	[重要]a)应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。	机房内需要安装温、湿度自动调节装置，如空调、除湿机、通风机等，使机房内温、湿度的变化在适宜设备运行所允许的范围之内。通常机房内适宜的温度范围是18~27℃， 空气湿度范围是35~75%	1)核查机房内是否配备了专用空调 2)核查机房内温湿度是否在设备运行所允许的范围之内	1)机房内配备了专用的精密空调 2)机房内温湿度设置在20-25℃,湿度为: 40%-60%	符合情况：配备了专用空调；机房内温湿度在设备运行所允许的范围之内。 部分符合情况：配备了专用空调；但机房内温湿度未在设备运行所允许的范围之内。 不符合情况：配备了专用空调；机房内温湿度在设备运行所允许的范围之内。
温湿度控制	[关键]b)机房应采用专用温湿度调节设备，并应满足机房监控系统的要求。（F3）	机房需要采用专用温湿度调节设备，并满足机房监控系统的要求。	1)核查机房内是否部署专用的温湿度调节设备，如精密空调等。 2)核查专用的温湿度调节设备是否正常运行。	1)机房内部署专用的温湿度调节设备，如精密空调等。 2)专用的温湿度调节设备正常运行。	符合情况：机房内部署专用的温湿度调节设备，如精密空调等。专用的温湿度调节设备正常运行。 部分符合情况：满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。
温湿度控制	[关键]c)温湿度调节设备的工作能力应满足机房负载要求，并应保有一定的余量。（F3）	温湿度调节设备的工作能力需要满足机房负载要求，并应保有一定的余量。	1)核查专用的温湿度调节设备是否满足机房负载需求。	1)专用的温湿度调节设备满足机房负载需求。	符合情况：专用的温湿度调节设备满足机房负载需求。 不符合情况：专用的温湿度调节设备不满足机房负载需求。
电力供应	[重要]a)应在机房供电线路上配置稳压器和过电压防护设备。	机房供电线路上需要安装电流稳压器和电压过载保护装置,防止电力波动对电子设备造成损害	核查供电线路上是否配置了稳压器和过电压防护设备	1)机房的计算机系统供电线路上设置了稳压器和过电压防护设备 2)现场观测时稳压器和过电压防护设备可正常工作	符合情况：供电线路上配置了稳压器和过电压防护设备。 部分符合情况：部分供电线路上配置了稳压器和过电压防护设备。 不符合情况：供电线路上未配

电力供应	[关键]b)应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。	机房供电需要配备不间断电源(UPS)或备用供电系统，如备用发电机或使用第三方提供的备用供电服务，防止电力中断对设备运转和系统运行造成损害	1)核查是否配备不间断电源(UPS)等备用供电系统	1)机房配备了UPS后备电源系统 2)UPS能够满足短期断电时的供电要求（当有柴油发电机作为后备电源时，电池最少备用时间为7min；否则不少于30min。）	符合情况：配备不间断电源(UPS)等备用供电系统。 不符合情况：未配备不间断电源(UPS)等备用供电系统
电力供应	[关键]c)应设置冗余或并行的电力电缆线路为计算机系统供电。	机房供电需要使用冗余或并行的电力电缆线路，防止电力中断对设备运转和系统运行造成损害	核查是否设置了冗余或并行的电力电缆线路为计算机系统供电	为机房配备了冗余的供电线路，如市电双路接入	符合情况：设置了冗余或并行的电力电缆线路为计算机系统供电。 不符合情况：未设置冗余或并行的电力电缆线路为计算机系统供电
电力供应	[关键]d)应提供应急供电设施，以备供电系统临时停电时启用，并确保应急供电设施能在UPS供电时间 内到位，每年需进行应急供电设施的带负载模拟演练，并定期对备用电力供应设备及应急供 电设施进行检修和维护，确保其能正常使用。（F3）	提供需要急供电设施，以备供电系统临时停电时启用，并确保急供电设施能在UPS供电时间内到位，每年需进行应急供电设施的带负载模拟演练，并定期对备用电力供应设备及应急供 电设施进行检修和维护，确保其能正常使用。	1)核查是否配备紧急供电设施，如柴油发电机等。 2)核查供电设施的切换时间是否满足要求，是否可以在UPS供电时间内到位。 3)核查是否每年进行应急供电设施的带负载模拟演练。 4)核查是否具有模拟演练记录和设施检修和维护记录。	1)配备紧急供电设施，如柴油发电机等。 2)供电设施的切换时间满足要求，可以在UPS供电时间内到位。 3)每年进行应急供电设施的带负载模拟演练。 4)具有模拟演练记录和设施检修和维护记录。	符合情况：机房配备紧急供电设施，如柴油发电机等。 供电设施的切换时间满足要求，可以在UPS供电时间内到位。每年进行应急供电设施的带负载模拟演练。具有模拟演练记录和设施检修和维护记录。 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。
电力供应	[关键]e)UPS供电系统的冗余方式应采用N+1、N+2、2N、2(N+1) 等方式，未建立备用发电机应急供电 系统的单位，UPS后备时间至少1小时，已建立备用发电机应急供电系统的单位，UPS后备时间 应满足至少15分钟以上。（F3）	UPS供电系统的冗余方式需要采用N+1、N+2、2N、2(N+1) 等方式，未建立备用发电机应急供电 系统的单位，UPS后备时间至少1小时，已建立备用发电机应急供电系统的单位，UPS后备时间需要满足至少15分钟以上。	1)核查UPS供电系统是否采用冗余方式部署。 2)若没有备用发电机的机房，核查UPS后备时间是否满足至少1小时的要求。 3)若配备备用发电机的机房，核查UPS后备时间是否满足至少15分钟的要求。	1)UPS供电系统采用冗余方式部署。 2)若没有备用发电机的机房，UPS后备时间满足至少1小时的要求。 3)若配备备用发电机的机房，UPS后备时间满足至少15分钟的要求。	符合情况：UPS供电系统采用冗余方式部署。若没有备用发电机的机房，UPS后备时间满足至少1小时的要求。若配备备用发电机的机房，UPS后备时间满足至少15分钟的要求。 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。
电力供应	[关键]f)机房内要求采用机房专用插座，市电、UPS电源插座分开，满足负荷使用要求。（F3）	机房内要求采用机房专用插座，市电、UPS电源插座分开，满足负荷使用要求。	1)核查机房内是否采用机房专用插座，如pdu等。 2)核查机房内市电、UPS电源插座是否分开。	1)机房内采用机房专用插座，如pdu等。 2)机房内市电、UPS电源插座分开。	符合情况：机房内采用机房专用插座，如pdu等。机房内市电、UPS电源插座分开。 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。

电力供应	[关键]g)计算机系统应选用铜芯电缆，避免铜、铝混用，若不能避免时，应采用铜铝过渡头连接。（F3）	计算机系统需要选用铜芯电缆，避免铜、铝混用，若不能避免时，应采用铜铝过渡头连接。	1)核查机房内计算机系统是否选用铜芯电缆，避免铜、铝混用。 2)若不能避免的，是否采用铜铝过渡头连接。	1)机房内计算机系统选用铜芯电缆，避免铜、铝混用。 2)若不能避免的，采用铜铝过渡头连接。	符合情况：机房内计算机系统选用铜芯电缆，避免铜、铝混用。 不符合情况：机房内计算机系统未选用铜芯电缆，避免铜、铝混用。
电力供应	[关键]h)机房应设置应急照明和安全出口指示灯，供配电（箱）和分电盘内各种开关、手柄、按钮 应标志清晰，防止误操作。（F3）	机房需要设置应急照明和安全出口指示灯，供配电（箱）和分电盘内各种开关、手柄、按钮 标志清晰。	1)核查机房内是否设置应急照明和安全出口指示灯。 2)核查机房内供配电（箱）和分电盘内各种开关、手柄、按钮标志是否清晰。	1)机房内设置应急照明和安全出口指示灯。 2)机房内供配电（箱）和分电盘内各种开关、手柄、按钮标志清晰。	符合情况：机房内设置应急照明和安全出口指示灯。机房内供配电（箱）和分电盘内各种开关、手柄、按钮标志清晰。 部分符合情况：满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。
电力供应	[关键]i)机房重要区域、重要设备应提供UPS单独供电。（F3）	机房重要区域、重要设备需要提供UPS单独供电。	1)核查机房重要区域、重要设备是否提供UPS单独供电。	1)机房重要区域、重要设备提供UPS单独供电。	符合情况：机房重要区域、重要设备提供UPS单独供电。 不符合情况：机房重要区域、
电磁防护	[一般]a)电源线和通信线缆应隔离铺设，避免互相干扰。	机房内电源线和通信线缆需要隔离铺设在不同的管道或桥架内,防止电磁辐射和干扰对设备运转和系统运行产生的影响	核查机房内电源线缆和通信线缆是否隔离铺设	机房内电源线缆和通信线缆隔离铺设，如通过线槽或桥架进行了隔离	符合情况：电源线缆和通信线缆隔离铺设。 部分符合情况： 不符合情况：电源线缆和通信线缆未隔离铺设。
电磁防护	[重要]b)应对关键设备实施电磁屏蔽。	机房内关键设备需要安放在电磁屏蔽机柜内或电磁屏蔽区域内,防止电磁辐 射和干扰对设备运转和系统运行产生的影响	核查机房内是否为关键设备配备了电磁屏蔽装置	为关键设备采取了电磁屏蔽措施，如配备了屏蔽机柜或屏蔽机房，关键设备如加密机	符合情况：为关键设备配备了电磁屏蔽装置。 不符合情况：关键设备未配备电磁屏蔽装置。

安全通信网络（S3A3G3）作业指导书					
安全控制点	**检测项**	**要求解读**	**测评方法**	**预期结果或主要证据**	**符合情况**
网络架构	[关键]a)应保证网络设备的业务处理能力满足业务高峰期需要，如：业务处理能力能满足业务高峰期 需要的 50%以上。（F3）	为了保证主要网络设备具备足够处理能力，应定期检查设备资源占用情况，确保设备的业务处理能力具备冗余空间。	1)应访谈网络管理员业务高峰时期为何时，核查边界设备和主要网络设备的处理能力是否满足业务高峰期需要，询问采用何种手段对主要网络设备的运行状态进行监控。 一般来说，在业务高峰期主要网络设备的CPU内存最大使用率不宜超过70%，也可以通过综合网管系统查看主要网络设备的CPU、 内存的使用情况。 2)应访谈或核查是否因设备处理能力不足而出现过宕机情况，可核查综合网管系统告警日志或设备运行时间等，或者访谈是否因设备处理能力不足而进行设备升级。 查看设备在线时长，如设备在线时间在近期有重启可询问原因。 3)应核查设备在一段时间内的性能峰值，结合设备自身的承载性能，分析是否能够满足业务处理能力需要的50%以上	1)设备CPU和内存使用率峰值不大于70%; 2)未出现宕机情况，网管平台未出现宕机告警日志，设备运行时间较长: 3)业务高峰流量不超过设备处理能力的70%	符合情况：主要网络设备CPU和内存使用率峰值不超过70%，未出现宕机情况，业务高峰期流量不超过设备70%。 部分符合情况：预期结果1,2,3满足一部分为部分符合。 不符合情况：主要网络设备CPU和内存使用率峰值超过70%，业务高峰期流量超过设备承受能力70%。
网络架构	[重要]b)应保证网络各个部分的带宽满足业务高峰期需要。	为了保证业务服务的连续性，应保证网络各个部分的带宽满足业务高峰期需要。如果存在带宽无法满足业务高峰期需要的情况，则需要在主要网络设备上进行带宽配置，保证关键业务应用的带宽需求	1)应访谈管理员高峰时段的流量使用情况，是否部署流量控制设备对关键业务系统的流量带宽进行控制，或在相关设备上启用QoS配置，对网络各个部分进行带宽分配，从而保证业务高峰期业务服务的连续性 2)应该查综合网管系统在业务商峰时段的带宽占用情况，分析是否满足业务需求。如果无法满足业务高蜂期需要，则需要在主要网络设备上进行带宽配置 3)测试验证网络各个部分的带宽是否满足业务高峰期需求	1)在各个关键节点部署流量监控系统，能够监测网络中的实时流量，部署流量控制设备，在关键节点设备品置QoS策略，对关健业务系统的流量带宽进行控制 2)节点设备配置了流量监管和流量整形策略; 3) 各通信链路高峰流量均不大其带宽的70%	符合情况：采取了流量限制措施或各各个关键节点通信线路高峰流量不大其带宽70%。 部分符合情况：预期结果1,2,3满足一部分为部分符合。 不符合情况：各个关键通信线路高峰期流量均大于其带宽70%。
网络架构	[重要]c)应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址。	根据实际情况和区域安全防护要求，应在主要网络设备上进行VLAN划分。VLAN 是一种通过将局域网内的设备逻辑地而不是物理 地划分成不同子网从而实现虚拟工作组的新技术。不同VLAN内的报文在传输时是相互隔离的,即一个VLAN内的用户不能和其它VLAN内的用户直接通信，如果不同VLAN要进行通信，则需要通过路由器或三层交换机等三层设备实现	应访谈网络管理员，是否依据部门的工作职能、等级保护对象的重要程度和应用系统的级别等实际情况和区域安全防护要求划分了不同的VLAN,并核查相关网络设备配置信息，验证划分的网络区域是否与划分原则一致。	划分不同的网络区域，按照方便管理和控制的原则为各网络区域分配地址，不同网络区域之间应采取边界防护措施:	符合情况：划分有不同的网络区域并按照方便管理和控制的原则分配网络地址，并采取控制措施。 部分符合情况：无部分符合情况。 不符合情况：未划分不同的网络区域，未根据业务情况划分不同的网络地址，所有都部署在统一网段内，且未采取控制措施。

网络架构	[重要]d)应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。	为了保证等级保护对象的安全，应避免将重要网段部署在网络边界处且直接连接外部等级保护对象，防止来自外部等级保护对象的攻击。同时，应在重要网段和其它网段之间配置安全策略进行访问控制	1)应核查网络拓扑图是否与实际网络运行环境一致 2)应核查重要网络区域是否未部署在网络边界处；网络区域边界处是否部署了安全防护措施 3)应核查重要网络区域与其他网络区域之间，例如应用系统区、数据库系统区等重要网络区域边界是否采取可靠的技术隔离手段，是否部署了网闸、防火墙和设备访问控制列表(ACL)等	1)网络拓扑图与实际网络运行环境一致 2）重要网络区域未部署在网络边界处 3)在重要网络区域与其他网络区域之间部署了网闸、防火墙等安全设备实现了技术隔离	符合情况：网络拓扑与实际运行一致，重要网络区域没有部署在边界，且已经采取措施实现隔离。 部分符合情况：预期结果1,2,3满足一部分为部分符合。 不符合情况：网络拓扑图与实际不一致，重要网络区域部署在边界，且未采取访问控制措施。
网络架构	[关键]e)应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性，双线路设计 时，宜由不同的电信运营商提供。（F3）	本要求虽然放在“安全通信网络”分类中，实际是要求整个网络架构设计需要冗余。为了避免网络设备或通信线路出现故障时引起系统中断，应采用冗余技术设计网络拓扑结构，以确保在通信线路或设备故障时提供备用方案，有效增强网络的可靠性。双线路设计 时，宜由不同的电信运营商提供。	1)应核查系统的出口路由器、 核心交换机、安全设备等关键设备是否有硬件冗余和通信线路冗余，保证系统的高可用性。 2)双线路设计时，核查是否采用不同的电信运营商。	采用HSRP、VRRP 等冗余技术设计网络架构，确保在通信线路或设备故障时网络不中断，有效增强网络的可靠性	符合情况：采用HSRP，VRRP等进行冗余技术设计网络架构，且通信线路采用冗余方式设计。 部分符合情况：部分关键设备未采取冗余方式设计。 不符合情况：所有关键设备均未采取冗余方式设计。
通信传输	[关键]a)应采用校验技术或密码技术保证通信过程中数据的完整性性，并按照国家密码管理部门与行业 有关要求使用密码算法。（F3）	为了防止数据在通信过程中被修改或破坏，应采用校验技术或密码技术保证通信过程中数据的完整性，这些数据包括鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。校验技术或密码技术需要使用符合国家密码管理部门与行业要求的密码算法。	1)应核查是否在数据传输过程中使用校验技术或密码技术来保证其完整性 2)应测试验证设备或组件是否保证通信过程中数据的完整性。例如使用 File ChecksumIntegrity Verifier 、SigCheck 等工具对数据进行完整性校验 3)使用的密码算法是否符合国家密码管理部门与行业的要求	1)对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息数据等采用校验技术或密码技术保证通信过程中数据的完整性; 2) File ChecksumIntegrity Verifier 计算数据的散列值，验证数据的完整性	符合情况：在数据传输过程中采取了校验技术或密码技术保证其完整性。使用的密码算法 符合国家密码管理部门和行业要求。 部分符合情况：部分关键数据采用了校验技术或密码技术。 不符合情况：未采取措施在数据传输过程中采取校验技术和密码技术保证其完整性。
通信传输	[关键]b)应采用密码技术保证通信过程中数据的保密性，并按照国家密码管理部门与行业有关要求使 用密码算法。（F3）	根据实际情况和安全防护要求，为了防止信息被窃听，应采取技术手段对通信过程中的敏感信息字段或整个报文加密，可采用对称加密、非对称加密等方式实现数据的保密性。校验技术或密码技术需要使用符合国家密码管理部门与行业要求的密码算法。	1)应核查是否在通信过程中采取保密措施，具体采用哪些技术措施 2)应测试验证在通信过程中是否对敏感信息字段或整个报文进行加密，可使用Sniffer、Wireshark 等测试工具通过流量镜像等方式抓取网络中的数据,验证数据是否加密 3)使用的密码算法是否符合国家密码管理部门与行业的要求。	1)对鉴别数据、重要业务数据，重要审计数据、重要配置数据、重要视频数据和重要个人信息数据等采用密码技术保证通信过程中数据的保密性 2)Sniffer. Wireshak可以监视到信息的传送，但是显示的是加密报文	符合情况：在数据传输过程中采取了校验技术或密码技术保证其保密性。使用的密码算法 符合国家密码管理部门和行业要求。 部分符合情况：部分关键数据采用了校验技术或密码技术。 不符合情况：未采取措施在数据传输过程中采取校验技术和密码技术保证其保密性。

可信验证	[一般]a)可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	通信设备可能包括交换机、路由器或其他通信设备等，通过设备的启动过程和运行过程中对预装软件(包括系统引导程序、系统程序、相关应用程序和重要配置参数)的完整性验证或检测，确保对系统引导程序、系统程序、重要配置参数和关键应用程序的篡改行为能被发现，并报警便于后续的处置动作	1)应核查是否基于可信根对设备的系统引导程序、系统程序、重要配置参数和关键应用程序等进行可信验证 2)应核查是否在应用程序的关键执行环节进行动态可信验证 3)应测试验证当检测到设备的可信性受到破坏后是否进行报警 4)应测试验证结果是否以审计记录的形式送至安全管理中心 (2.3)	1)通信设备、交换机、路由器或其他通信设备具有可信根芯片或硬件 2)启动过程基于可信根对系统引导程序、系统程序，重要配置参数和关键应用程序等进行可信验证度量 3)在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心 4)安全管理中心可以接收设备的验证结果记录 (2.3)	符合情况：通信设备例如交换机、路由器均部署了可信芯片或硬件进行可信验证，均基于可信根对引导程序、系统程序，重要配置参数和关键应用程序进行可信验证度量，在检测到可信性破坏后进行报警，并将验证结果送至安全管理中心，并验证。 部分符合情况：预期结果1，2，3，4点满足一部分为部分符合。 不符合情况：未采取措施通信设备例如交换机、路由器均部署了可信芯片或硬件进行可信验证，均基于可信根对引导程序、系统程序，重要配置参数和关键应用程序进行可信验证度量，在检测到可信性破坏后进行报警，并将验证结果送至安全管理中心，并验证。

安全区域边界（S3A3G3）作业指导书					
安全控制点	**检测项**	**要求解读**	**测评方法**	**预期结果或主要证据**	**符合情况**
边界防护	[关键]a)应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	为了保障数据通过受控边界，应明确网络边界设备，并明确边界设备物理端口，网络外连链路仅能通过指定的设备端口进行数据通信	1)应核查网络拓扑图与实际的网络链路是否一致，是否明确了网络边界，且明确边界设备端口。 2)应核查路由配置信息及边界设备配置信息，确认是否指定物理端口进行跨越边界的网络通信。 3)应采用其他技术手段核查是否不存在其他未受控端口进行跨越边界的网络通信,例如检测无线访问情况，可使用无线嗅探器、无线入侵检测/防御系统、手持式无线信号检测系统等相关工具进行检测	1)查看网络拓扑图，并比对实际的网络链路，确认网络边界设备及链路接入端口无误 2)通过相关命令显示设备端口、Vlan信息 3)通过网络管理系统的自动拓扑发现功能，监控是否存在非授权的网络出口链路;通过无线嗅探器排查无线网络的使用情况，确认无非授权WiFi	符合情况： 1)网络拓扑与实际链路情况一致 2）边界路由，边界访问控制设备的配置信息准确无误 3）不存在非授权的网络出口链路;通过无线嗅探器排查无线网络的使用情况，无非授权WiFi 部分符合情况：满足1），2），3）其中一条或者两条 不符合情况：无网络拓扑，边界设备配置信息有误，存在非授权wifi
边界防护	[重要]b)应能够对非授权设备私自联到内部网络的行为进行检查或限制。	设备的“非授权接入”可能会破坏原有的边界设计策略，可以采用技术手段和管理措施对“非授权接入”行为进行检查。技术手段包括部署内网安全管理系统，关闭网络设备未使用的端口，绑定IP/MAC地址等	1)应访谈网络管理员，询问采用何种技术手段或管理措施对非授权设备私自联到内部网络的行为进行管控，并在网络管理员的配合下验证其有效性 2)应核查所有路由器和交换机等设备闲置端口是否均已关闭。以Cisco I0S为例，输入命令"show ip interfaces brief” 3)如通过部署内网安全管理系统实现系统准入，应检查各终端设备是否统一进行了部署，是否存在不可控特殊权限接入设备 4）如果采用了IP/MAC地址绑定的方式进行准入控制，应核查接入层网络设备是否配置了IP/MAC地址	1)非使用的端口均已关闭; 2)网络中部署的终端管理系统已启用，且各终端设备均已有效部署，无特权设备 3)IP/MAC地址绑定结果。	符合情况：1）采取技术手段或管理措施对非授权设备私自联到内部网络的行为进行管控 2）所有路由交换设备的闲置端口已手动关闭 3)部署了准入系统或进行MAC绑定，权限覆盖到所有终端 部分符合情况：满足1），2），3）其中一条或者两条 不符合情况：对入网设备无任何限制措施
边界防护	[重要]c)应能够对内部用户非授权联到外部网络的行为进行检查或限制。	内网用户设备上的外部连接端口的“非授权外联“行为也可能破坏原有的过界设计策略，可以通成内网安全管理系统的非授权外联管控功能或者防非法外联系统实现“非授权外联”行为的控制，由于内网安全管理系统可实现包括非授权外连管控在内的众多的管理功能，建议c采用该项措施。通过对用户非授权建立网络连接访问非可信网络的行为进行管控，从而减少安全风险的引入	1)应核查是否采用内网安全管理系统或其它技术手段，对内部用户非授权连接到外部网络的行为进行限制或检查 2)应核查是否限制终端设备相关端口的使用，如禁用双网卡、USB接口、Modem、无线网络等，防止内部用户非授权外连行为	1)网络中部署有终端安全管理系统，或非授权外联管控系统 2)网络中各类型终端设备均已正确部署了终端安全管理系统或外联管控系统，并启用了相关策略，如禁止更改网络配置，禁用双网卡、USB接口.、Mode、无线网络等	符合情况：1）采取技术手段或管理措施对非授权设备私自外联行为进行管控 2）限制了终端设备的D多余组件的使用，如双网卡，USB接口等 部分符合情况：满足1），2）其中一条或者两条 不符合情况：未对终端的外联行为进行任何限制措施

边界防护	[重要]d)应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。	为了防止未经授权的无线网络接入行为，无线网络应单独组网并通过无线接入网关等受控的边界防护设备接入到内部有线网络。同时，应部署无线网络管控措施，对分非授权无线网络进行检测、屏蔽	1)应访谈网络管理员是否有授权的无线网络，是否单独组网后接入到有线网络 2)应核查无线网络部署方式，是否部署无线接入网关，无线网络控制器等设备。应检查该类型设备配置是否合理，如无线网络设备信道使用是否合理，用户口令是否具备足够强度、 是否使用WPA2加密方式等 3)应核查网络中是否部署了对非授权无线设备管控措施，能够对非授权无线设备进行检查、屏蔽。如使用无线嗅探器、无线入侵检测/防御系统、手持式无线信号检测系统等相关工具进行检测、限制	1)授权的无限网络通过无线接入网管，并通过防火墙等访问控制设备接入到有限网络。无线网络使用了1信道，防止设备间互相干扰;使用WPA2进行加密;且用户密码具备复杂度要求，如:口令长度8位以上，由数字、字母、大小写及特殊字符组成 2)通过无线嗅探器未发现非授权无线设备	符合情况：1）具备授权的无线网络 2）部署了接入网关，AC控制器，且采用安全的无线加密方案 3）能够对非授权无线设备进行检查、屏蔽 部分符合情况：满足1），2），3）其中一条或者两条 不符合情况：无线网络可以直接接入，无任何管控措施
访问控制	[关键]a)应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。	应在网络边界或区域之间部署网闸，防火墙、路由器、交换机和无线接入网关等提供访问控制功能的设备或相关组件，想据访问控制策略设置有效的访问控制规则，访问控制规则采用白名单机制	1)应核查在网络边界或区域之间是否部署访问控制设备，是否启用访问控制策略 2)应核查设备的访问控制策略是否为白名单机制，仅允许授权的用户访问网络资源，禁止其他所有的网络访问行为 3)应该检查配置的访问控制策略是否实际应用到相应的接口的进或出方向。	1、边界部署了访问控制设备如（防火墙、网闸、边界路由等）设备; 2、边界设备是否配置了访问控制策略，访问控制策略配置是否有效; 3、访问控制策略调用到相应的端口、route-map、出入方向等。	符合情况：1）边界部署了访问控制设备 2）访问控制策略颗粒度满足要求且真实有效 3）访问控制策略应用到实际出入方向 部分符合情况：满足1），2），3）中的一条或两条 不符合情况：边界未部署访问控制设备或者访问控制策略无
访问控制	[重要]b)应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。	根据实际业务需求配置访问控制策略，仅开放业务必须的端口，禁止配置全通策略，保证边界访问控制设备安全策略的有效性。不同访问控制策略之间的逻辑关系应合理，访问控制策略之间不存在相互冲突，重叠或包含的情况;同时，应保障访问控制规则数量最小化。	1)应访谈安全管理员访问控制策略配置情况,核查相关安全设备的访问控制策略与业务及管理需求的一致性，结合策略命中数分析策略是否有效 2)应检查访问控制策略中是否已禁止了全通策略或端口、地址限制范围过大的策略。 3)应核查设备的不同访问控制策略之间的逻辑关系是否合理。	1、访问控制策略相对精简，不存在无效的访问控制策略; 2、应删除默认的any to any全通策略，根据业务和资源访问需求逐条进行策略配置; 3、根据整体边界情况配置访问控制策略，不应出现同方向或者同网段出现访问控制策略逻辑不一致	符合情况：1）访问控制策略精简，不存在多余或无效的访问控制策略 2）不存在默认的访问控制策略any to any 3）边界访问控制策略出入方向逻辑一致 部分符合情况：满足1) 不符合情况：不存在或者边界访问控制策略无效，或存在默认全通的策略
访问控制	[重要]c)应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出。	应对网络中网闸、防火墙、路由器、交换机和无线接入网关等提供访问控制功能的设备或相关组件进行检查，访问控制策略应明确源地址、目的地址，源端口、目的端口和协议，以允许/拒绝数据包进出	应核查设备中访问控制策略是否明确设定了源地址、目的地址、源端口、目的端只和协议等相关配置参数。 以Ciso IOS为例 拒绝所有从172.16.4.0到172.16.3.0的ftp通信流量通过F0/0接口，输入命令：”show running-config“,检查配置文件中访问控制列表配置项	根据源地址、目的地址，源端口、目的端口和协议等设置相应访问控制策略，根据访问控制策略允许或拒绝数据通信	符合情况：1）访问控制策略具备明确的源目地址，端口协议等配置参数 部分符合情况：\ 不符合情况：访问控制策略颗粒度不够，没有明确的源目地址、端口等参数

访问控制	[关键]d)应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级。（F3）	防火墙能够根据数据包的源地址、目标地址、协议类型、源端口、目标端口等对数据包进行控制，而且能够记录通过防火墙的连接状态，直接对包里的数据进行处理。防火墙还应具有完备的状态检测表来追踪连接会话状态，并结合前后数据包的关系进行综合判断，然后决定是否允许该数据包通过，通过连接状态进行更迅速更安全地过滤。控制粒度为端口级。	应核查状态检测防火墙访问控制策略中是否明确设定了源地址、目的地址、源端口、目的端口和协议以Cisco IOS为例，输入命令: show running0-config.	边界设备的访问控制策略要根据业务的实际情况进行配置，如特定端口、特定源地址、目的地址或者协议等。访问控制策略要清晰明确，避免具体业务出现大段放行的访问控制策略。	符合情况：边界设备的访问控制策略要根据业务的实际情况进行配置，如特定端口、特定源地址、目的地址或者协议等部分符合情况\ 不符合情况：边界设备未根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力
访问控制	[重要]e)应对进出网络的数据流实现基于应用协议和应用内容的访问控制。	在网络边界采用下-代防火墙或相关安全组件,实现基于应用协议和应用内容的访问控制	1)应核查在关键网络节点处是否部署访问控制设备 2)应检查访问控制设备是否配置了相关策略，对应用协议、应用内容进行访问控制，并对策略有效性进行测试	防火墙配置应用访问控制策略，从应用协议、应用内容进行访问控制，对QQ聊天工具、优酷视频以及Web服务、FTP服务等进行管控	符合情况：配置基于应用协议的访问控制策略，从应用协议、应用内容进行访问控制，对QQ聊天工具、优酷视频以及Web服务、FTP服务等进行管控部分符合情况\ 不符合情况：未对应用层协议和内容进行访问控制
访问控制	[关键]f)应对网络设备系统自带的服务端口进行梳理，关掉不必要的系统服务端口，并建立相应的端 口开放审批制度。（F3）	对网络设备系统自带的服务端口进行梳理，关掉不必要的系统服务端口，并建立相应的端 口开放审批制度。	1)应核查在网络设备是否已关闭空闲端口。 2)核查是否建立端口开发审批制度。	1)网络设备已关闭空闲端口。 2)建立端口开发审批制度。	符合情况：1设备空闲端口已关闭,2已建立端口开发审批制度。 部分符合情况：满足1），2），其中一条 不符合情况：未关闭网络设备空闲端口。未建立端口开发审批制度。
访问控制	[关键]g)应定期检查并锁定或撤销网络设备中不必要的用户账号。（F3）	定期检查并锁定或撤销网络设备中不必要的用户账号。	1)应与管理员访谈核对，核查网络设备是否存在不必要的用户账号。	定期检查并锁定或撤销网络设备中不必要的用户账号。	符合情况：定期检查并锁定或撤销网络设备中不必要的用户账号。 部分符合情况：/ 不符合情况：未定期检查并锁定或撤销网络设备中不必要的

入侵防范	[重要]a)应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为。	要维护系统安全，必须进行主动监视，以检查是否发生了入侵和攻击。监视入侵和安全事件既包括被动任务也也包括主动任务。很多入侵都是在发生攻击之后，通过检查日志文件才检测到的。这种攻击之后的检测通常被称为被动入侵检测;只有通过检查日志文件，攻击才得以根据日志信息进行复查和再现。其他入侵尝试可以在攻击发生的同时检测到，这种方法称为”主动“入侵检测，它会查找已知的攻击模式或命令，并阻止这些命令的执行。 完整的入侵防范应首先实现对事件的特征分析功能，以发现潜在的攻击行为，应能发现目前主流的各种攻击行为，如端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等。 目前对入侵防范的实现主要是通过在网络边界部署包含入侵防范功能的安全设备，如抗APT攻击系统、网络回溯系统、威胁情报检测系统、抗DDoS攻击系统、入侵检测系统(IDS)，入侵防御系统(IPS)、包含入侵防范模块的多功能安全网关(UTM)等。 为了有效检测，防止或限制从外部发起的网络攻击行为，应在网络边界、核心等关键网络节点处部署IPS等系统，或在防火墙、UTM启用入侵防护功能	1)应核查相关系统或设备是否能够检测从外部发起的网络攻击行为 2)应核查相关系统或设备的规则库版本是否已经更新到最新版本 3)应核查相关系统或设备配置信息或安全策略是否能够覆盖网络所有关键节点 4) 应测试验证相关系统或设备的安全策略是否有效	1)相关系统或设备有检测到外部发起攻击行为的信息; 2)相关系统或设备的规则库进行了更新，更新时间与测评时间较为接近 3)配置信息、安全策略中制定的规则覆盖系统关键节点的IP地址等 4)监测到的攻击日志信息与安全第略相符	符合情况：关键节点网络有入侵攻击检测设备，并配置了相应策略，且策略有效 部分符合情况：\ 不符合情况：未在关键节点部署入侵攻击检测产品或等效措施
入侵防范	[重要]b)应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为。	为了有效检测、防止或限制从内部发起的网络攻击行为，应在网络边界、核心等关键网络节点处部署IPS等系统，或在防火墙、UTM启用入侵防护功能	1)应核查相关系统或设备是否能够检测到从内部发起的网络攻击行为 2)应核查相关系统或设备的规则库版本是否已经更新到最新版本 3)应核查相关系统或设备配置信息或安全策略是否能够覆盖网络所有关键节点 4)应测试验证相关系统或设备的安全策略是否有效	1)相关系统或设备有检测到外部发起攻击行为的信息; 2)相关系统或设备的规则库进行了更新，更新时间与测评时间较为接近 3)配置信息、安全策略中制定的规则覆盖系统关键节点的IP地址等 4)监测到的攻击日志信息与安全策略相符的	符合情况：1)相关系统或设备有检测到外部发起攻击行为的信息; 2)相关系统或设备的规则库进行了更新，更新时间与测评时间较为接近 3)配置信息、安全策略中制定的规则覆盖系统关键节点的IP地址等 4)监测到的攻击日志信息与安全策略相符的 部分符合情况：满足1）和2），3）其中一条 不符合情况：未部署入侵检测设备对关键网络节点受到的内

入侵防范	[关键]c)应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。	部署网络回溯系统或抗APT攻击系统等实现对新型网络攻击行为进行检测和分析	1)应核查是否部署回溯系统或抗APT攻击系统，实现对新型网络攻击行为进行检测和分析 2)应核查相关系统或设备的的规则库版本是否已经更新到最新版本 3)应测试验证是否对网络行为进行分析，实现对网络攻击特别是未知的新型网络攻击的检测和分析	1)系统内部署网络回溯系统或抗APT攻击系统，系统内包含对新型网络攻击的检测和分析功能 2)网络回溯系统或抗APT攻击系统的规则库进行了更新，更新时间与测评时间较为接近 3)经测试验证系统可对网络行为进行分析，且能够对未知新型网络攻击检测和分析	符合情况：1)系统内部署网络回溯系统或抗APT攻击系统，系统内包含对新型网络攻击的检测和分析功能 2)网络回溯系统或抗APT攻击系统的规则库进行了更新，更新时间与测评时间较为接近 3)经测试验证系统可对网络行为进行分析，且能够对未知新型网络攻击检测和分析 部分符合情况：满足1）和2），3）其中一条或者两条 不符合情况：未部署对网络攻击行为进行检测和分析的产品或设备
入侵防范	[一般]d)当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。	为了保证系统受到攻击时能够及时准确的记录攻击行为并进行安全应急响应，当检测到攻击行为时，应对攻击源IP、攻击类型、攻击目标和攻击时间等信息进行日志记录。通过这些日志记录，可以对攻击行为进行审计分析。当发生严重入侵事件时，应能够及时向有关人员报警，报警方式包括短信、邮件等。	1)访谈网络管理员和查看网络拓扑结构，查看在网络边界处是否部署了包含入侵防范功能的设备。如果部署了相应设备，则检查设备的日志记录,查看是否记录了攻击源IP、攻击类型、攻击目的和攻击时间等信息，查看设备采用何种方式进行报警 2)应测试验证相关系统或设备的报警策略是否有效	1)相关具有入侵防范功能的设备日志记录了攻击源IP、攻击类型、攻击目标、攻击时间等信息 2)设备的报警功能已开启且处于正常使用状态	符合情况：1)相关具有入侵防范功能的设备日志记录了攻击源IP、攻击类型、攻击目标、攻击时间等信息 2)设备的报警功能已开启且处于正常使用状态 部分符合情况：满足1），2）其中一条 不符合情况：无法对攻击行为的类型，IP，时间等攻击信息
入侵防范	[关键]e)应采取技术手段对高级持续威胁进行监测、发现。（F3）	需要采取技术手段对高级持续威胁进行监测、发现。如沙箱、蜜罐、态势感知等。	1)应核查是否部署技术手段对高级持续威胁进行监测、发现，并查看其监测记录。	采取技术手段对高级持续威胁进行监测、发现。	符合情况：采取技术手段对高级持续威胁进行监测、发现。 部分符合情况：\ 不符合情况：未采取技术手段对高级持续威胁进行监测、发现。
入侵防范	[关键]f)应建立诱捕、欺骗攻击者的安全防护手段，对攻击者的行为进行捕获和分析。（F3）	需要建立诱捕、欺骗攻击者的安全防护手段，对攻击者的行为进行捕获和分析。如沙箱、蜜罐、态势感知等。	1)应核查是否部署诱捕、欺骗攻击者的安全防护手段，对攻击者的行为进行捕获和分析。并查看其分析记录。	建立诱捕、欺骗攻击者的安全防护手段，对攻击者的行为进行捕获和分析。	符合情况：建立诱捕、欺骗攻击者的安全防护手段，对攻击者的行为进行捕获和分析。 部分符合情况：\ 不符合情况：未建立诱捕、欺骗攻击者的安全防护手段，对攻击者的行为进行捕获和分析

恶意代码和垃圾邮件防范	[重要]a)应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	计算机病毒、木马和蠕虫的泛滥使得防范恶意代码的破坏显得尤为重要。恶意代码是指怀有恶意目的可执行程序。目前恶意代码主要都是通过网页、邮件等网络载体进行传播。因此在网络边界处部署防恶意代码产品进行恶意代码防范是最为直接和高效的办法。 防恶意代码产品目前生要包括防病毒网关，包含防病毒模块的多功能安全网关等产品。其至少应具备的功能包括:对恶意代码的分析检查能力，对恶意代码的清除或阻断能力，以及发现恶意代码后记录日志和审计，并包含对恶意代码特征库的升级和检测系统的更新能力。 恶意代码具有特征变化快的特点。因此对于恶意代码检测重要的特征库更新，以及监测系统自身的更新，都非常重要。 产品应具备通过多种方式实现恶意代码特征库和检测系统更新的能力，如自动远程更新、手动远程更	1)应访谈网络管理员和检查网络拓结构，查看在网络边界处是否部署了防恶意代码产品。如果部署了相关产品，则查看是否启用了恶意代码检测并查看白志记录中是否有相关阻断信息 2)应访谈网络管理员，是否对防恶意代码产品的特征库进升级及具体的升级方式，并登录相应的防恶意代码产品，核查其特征库升级情况，当前是否为最新版本 3)应测试验证相关系统或设备的安全策略是否有效	1)在网络边界处及部署防恶意代码产品或组件，防恶意代码的功能正常开启且具有对恶意代码检测和清除的功能 2)防恶意代码的特征库进行了升级，且升级时间与测评时间较为接近	符合情况：1)在网络边界处及部署防恶意代码产品或组件，防恶意代码的功能正常开启且具有对恶意代码检测和清除的功能 2)防恶意代码的特征库进行了升级，且升级时间与测评时间较为接近 部分符合情况：满足1），2）其中一条 不符合情况：未部署防恶意代码设备
恶意代码和垃圾邮件防范	[重要]b)应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。	垃圾邮件是指电子邮件使用者事先未提出要求或同意接收的电子邮件,应部署相应设备或系统对垃圾邮件进行识别和处理，包括部署透明的防垃圾邮件网关。基于转发的防垃圾邮件系统、安装于邮件服务器的防垃圾邮件软件，以及与邮件服务器一体的防垃圾邮件的邮件服务器等，并保证规则库已经更新到最新	1)应核查在关键网络节点处是否部署了防垃圾邮件设备或系统 2)应核查防垃圾邮件产品运行是否正常，防垃投邮件规则库是否已经更新到最新。 3)应测试验证相关系统或设备的安全策略是否有效	1）在网络关键节点处部署了防垃投邮件设备的产品或组件，防垃级邮件设备的功能正常开启 2)防垃报邮件防护机制的进行了升级和更新，且升级时间与测评时间较为接近 3)测试结果显示系统或设备能够对垃圾邮件成功的阻断	符合情况：1）在网络关键节点处部署了防垃投邮件设备的产品或组件，防垃级邮件设备的功能正常开启 2)防垃报邮件防护机制的进行了升级和更新，且升级时间与测评时间较为接近 3)测试结果显示系统或设备能够对垃圾邮件成功的阻断 部分符合情况：满足1），2），3）其中一条或者两条 不符合情况：未部署垃圾邮件防护产品、且未进行定期更新
安全审计	[重要]a)应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。	为了对重要用户行为和重要安全事件进行审计,需要在网络边界部署相关系统，启用重要网络节点日志功能，将系统日志信息输出至各种管理端口、内部缓存或者日志服务器	1)核查是否部署了综合安全审计系统或类似功能的系统平台 2)核查安全审计范围是否覆盖到每个用户并对重要的用户行为和重要安全事件进行了审计	1)在网络边界处、重要网络节点处部署了审计设备 2）审计的范围能够覆盖到每个用户，且审计记录包合了重要的用户行为和重要安全事件	符合情况：1)在网络边界处、重要网络节点处部署了审计设备 2）审计的范围能够覆盖到每个用户，且审计记录包合了重要的用户行为和重要安全事件 部分符合情况：\ 不符合情况：未部署审计平台且无法收集审计信息
安全审计	[关键]b)应记录无线网络接入行为，形成日志进行留存，保存时间不少于 6 个月。（F3）	需要记录无线网络接入行为，形成日志进行留存，保存时间不少于 6 个月。	1)核查系统是否涉及无线网络接入场景。 2)若系统涉及无线网络接入，则核查是否有无线接入行为记录，记录是否保存6个月以上。	1记录无线网络接入行为，形成日志进行留存，2保存时间不少于 6 个月。	符合情况：1）记录无线网络接入行为，形成日志进行留存，2)记录保存时间不少于 6 个月。 部分符合情况：满足1），2）其中一条 不符合情况：未记录无线网络

安全审计	[一般]c)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	审计记录包含内容是否全面将直接影响审计的有效性，网络边界处和重要网络节点的日志审计内容应记录事件的时间、类型、用户、事件类型、事件是否成功等必要信息	核查审计记录信意是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。 -般来说，对于主流路由器和交换机设备，可以实现对系统错误、网络和接口的变化、登录失败、ACL匹配等进行审计，审计内容向括了时间、类型、用户等相关信息。因此，只要这些路由器和交换机设备启用审计功能就能符合该项要求。但对于防火墙等安全设备来说，由于其访问控制策略命中日志需要手动启用，因此应重点核查其访问控制策命中日志是否启用	审计记录包含了事件的日期和时间、用户、事件类型、事件是否成功等信息	符合情况：审计记录包含了事件的日期和时间、用户、事件类型、事件是否成功等信息 部分符合情况：审计记录覆盖一部分但覆盖补全 不符合情况：未开启审计功能模块或审计记录无法进行查看
安全审计	[关键]d)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等，审计记录保存时 间不少于 6 个月。（F3）	审计记录能够帮助管理人员及时发现系统运行状况和网络攻击行为，因此需要对审计记录实施技术上和管理上的保护，防止未授权修改、删除和破坏。可以设置专门的日志服务器来接收设备发送出的报警信息。非授权用户(审计员除外)无权删除本地和日志服务器上的审计记录	1)核查是否采取了技术措施对审计记录进行保护 2)核查审计记录的备份机制和备份策略是否合理	1)审计系统开启了日志外发功能，日志转发至日志服务器 2)审计记录存储超过6个月以上	符合情况：1)审计系统开启了日志外发功能，日志转发至日志服务器 2)审计记录存储超过6个月以上部分符合情况：\ 不符合情况：审计记录无法进行有效保护且存储时间达不到要求
安全审计	[重要]e)应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。	对于远程访问用户，应在相关设备上提供用户认证功能。通过配置用户、用户组，并结合访问控制规则可以实现对认证成功的用户允许访问受控资源。此外，还需对内部用户访问互联网的行为进行审计分析	核查是否对远程访问用户及互联风访问用户行为单独进行审计分析，并核查审计分析的记录是否包含了用于管理远程访同行为、访问互联网用户行为必要的信息	在网络边界处的审计系统对远程访问的用户行为进行了审计,审计系统对访问互联网的行为进行了单独的审计	符合情况：在网络边界处的审计系统对远程访问的用户行为进行了审计,审计系统对访问互联网的行为进行了单独的审计部分符合情况\ 不符合情况：无法对远程访问的用户行为进行审计。
安全审计	[关键]f)所有的审计手段需要具备统一的时间戳，保持审计的时间标记一致。（F3）	所有的审计手段需要具备统一的时间戳，保持审计的时间标记一致。	1)核查系统是否部署时钟同步服务器，如ntp服务器。 2)核查系统审计记录的时间标记是否一致。	1系统是否部署时钟同步服务器， 2所有设备审计记录的时间标记一致。	符合情况：1)系统部署时钟同步服务器， 2)所有设备审计记录的时间标记一致。 部分符合情况：满足1），2)其中一条 不符合情况：系统未部署时钟同步服务器

可信验证	[一般]a)可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	边界设备可能包括网闸、防火墙、交换机、路由器或其他边界防护设备等，通过设备的启动过程和运行过程中对预装软件(包括系统引导程序、系统程序、相关应用程序和重要配置参数)的完整性验证或检测，确保对系统引导程序、系统程序、重要配置参数和关键应用程序的篡改行为能被发现，并报警便于后续的处置动作	1)应核查是否基于可信根对设备的系统引导程序、系统程序、重要配置参数和关键应用程序等进行可信验证 2)应核查是否应用程序的关键执行环节进行动态可信验证3)应测试验证当检测到设备的可信性受到破坏后是否进行报警 4)应测试验证结果是否以审计记录形式送至安全管理中心 (3.6)	1)边界设备（网闸、防火墙、交换机、路由器或其他边界防护设备）具有可信根芯片或硬件 2)启动过程基于可信根对系统引导程序、系统程序、重要配置参数和关键应用程序等进行可信验证度量 3)在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心 4) 安全管理中心可以接收设备的验证结果记录 (3.6)	符合情况：1)边界设备（网闸、防火墙、交换机、路由器或其他边界防护设备）具有可信根芯片或硬件 2)启动过程基于可信根对系统引导程序、系统程序、重要配置参数和关键应用程序等进行可信验证度量 3)在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心 4) 安全管理中心可以接收设备的验证结果记录 部分符合情况：满足1），2），3）、4）其中一条或者多条 不符合情况：不具备可信验证产品或者服务

安全计算环境-网络设备-H3C（S3A3G3）作业指导书					
安全控制点	检测项	要求解读	测评方法	预期结果或主要证据	符合情况
身份鉴别	[关键]a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，应实现身份鉴别信息防窃取和防重用。静态口令应在8位以上，由字母、数字、符号等混合组成并每半年更换口令，不允许新设定的口令与前次旧口令相同。应用系统用户口令应在满足口令复杂度要求的基础上定期更换。（F3）	一般来说，用户登录路由器的方式包括:利用控制台端口(Console)通过串口进行本地登录连接。利用辅助端口(AUX)通过Modem进行远程拨号连接登录或者利用虚拟终端（VTY）通过TCP/IP网络进行TelnetT登录等。无论是哪一种登录方式，都需要对用户身份进行鉴别，口令是路由器用来防止非受权访问的常用手段，是路由器本身安全的一部分，因此需要加强对路由器口令的管理,包括口令的设置和存储，最好的口令存储方法是保存在TACACS+或RADIUS认证服务器上。管理员应当依据需要为路由器相应的端口加上身份签别最基本的安全控制。 路由器不允许配置用户名相同的用户，同时要防止多人共用一个账户，实行分账户管理，每名管理员设置一个单独的账户，避免出现问题后不能及时进行追查。 为避免身份鉴别信息被冒用，可以通过采用令牌、认证服务器等措施，加强身份鉴别信息的保护。如果仅仅基于口令的身份鉴别，应当保证口令复杂度和定期更改的要求。 使用“service password-encryption"命令对存储在配置文件中的所有口令和类似数据进行加密，避免通过读取配置文件而获取口令的明文	1)应核查用户在登录时是否采用了身份签别措施 2)应核查用户列表，测试用户身份标识是否具有唯一性 以华为路由器为例，输入“display current-configuration"即【dis cu】命令；检查是否存在如下配置: # telnet server enable【登录通道】 # user-interface vty 0 15 authentication-mode scheme user-role network-admin user-role network-operator # local-user user1【用户名】class manage service-type telnet【用户登录方式】 authorization-attribute user-role level-9【用户权限】 password-control aging 1【口令老化时间1天】	1）采取一种或以上身份鉴别措施； 2）身份标识具有唯一性； 3）用户口令8位以上由数字字母符号组成； 4）定期（90天以内）更换用户口令。	符合情况：采用了一种及以上的身份鉴别方式，身份标识具备唯一性，用户口令8位及以上，口令组成由大小写字母、数字和字符组成，口令每90天进行一次更换。 部分符合情况：预期结果1,2,3,4满足一部分为部分符合。 不符合情况：未采取身份鉴别方式，用户口令8位以下，且口令组成未采用大小写字母、数字和特殊字符，未定期进行口令更换。
身份鉴别	[关键]b)应具有登录失败处理功能，应配置并启用结束会话、限制登录间隔、限制非法登录次数和当登录连接超时自动退出等相关措施。（F3）	可以通过配置结束会话、限制管理员的最大登录失败次数、网络连接超时自动退出等多种措施实现登录失败处理功能。例如，设置管理员最大登录失败次数，一旦该管理员的登录失败次数超过设定数值，系统将对其进行登录锁定，从而防止非法用户通过暴力破解的方式登录到防火墙	1)应核查是否配置并启用了登录失败处理功能，核查是否配置并启用了限制非法登录达到一定次数后实现账户锁定功能 2)应核查是否配置并启用了远程登录连接超时并自动退出功能	1）启用并配置了登录失败处理功能； 2）非法登录达到一定次数后将账户锁定； 3）配置了连接超时自动退出功能，超时时间不大于30分钟。	符合情况：启用了登录失败处理功能，且非法登录达到一定次数后进行限制，配置了连接自动退出功能。 部分符合情况：预期结果1,2,3满足一部分为部分符合。 不符合情况：未配置登录失败处理功能，未配置非法登录限制措施，未配置登录连接自动超时退出功能
身份鉴别	[关键]c)当进行远程管理时，应对管理终端进行身份标识和鉴别，采用密码技术防止鉴别信息在网络传输过程中被窃听。（F3）	当对网络设备进行远程管理时，为避免口令传输过程中别窃取，不应当使用明文传送的Telnet服务，而应当采用SSH、ITTPS等加密协议等方式进行交互式管理	1、直接对设备进行远程管理时，华为H3C:输入【diSplay curent-configuration】命令，查看是否存在如下类似配置: local-user test password cipher 456%&ET service-type ssh level 3 ssh user test authentication type password User-interface vty 0 4 Protocol inbound ssh 如果service-type后的参数为明文传输协议则不符合要求。 2、网络设备通过堡垒机进行远程管	1）采用SSH、HTTPS等加密或其他的安全方式进行远程管理。	符合情况：采用SSH或HTTPS的加密方式进行远程管理。 部分符合情况：无部分符合情况。 不符合情况：采用telnet、http的方式进行远程管理。

身份鉴别	[关键]d)应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	采用双因子鉴别是防止欺骗的有效方法，双因子鉴别不仅要求访问者知道一些鉴别信息，还需要访问者拥有鉴别特征，例如采用令牌、智能卡等	1、核查系统是否采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户身份进行鉴别	1）同时采用两种或两种以上组合的鉴别方式对用户身份进行鉴别，且其中一种方式采用密码技术。	符合情况：同时采用两种或两种以上的身份鉴别方式，且其中一种鉴别方式采用了密码技术。 部分符合情况：采用了两种及两种以上的身份鉴别方式，但未包含密码技术。 不符合情况：未同时采用两种或两种以上的身份鉴别方式
访问控制	[重要]a)应对登录的用户分配账户和权限。	为了确保交换机的安全，需要对登录的用户分配账户，并合理配置账户权限。例如，相关管理人员具有与职位相对应的账户和权限	1)访谈网络管理员、安全管理员、系统管理员或核查用户账户和权限设置情况 华为H3C交换机输入【diSplay curent-configuration】查看设备中存在的账号，与管理员核对一下配置中的账号对应的管理人员和权限设置情况； # user-interface vty 0 15 authentication-mode scheme user-role network-operator 【network-operator为默认权限名】 # role name network-operator rule 1 permit read write execute feature aaa rule 2 permit read write execute feature device ---------- 进一步查看用户权限【dispaly role name network-operator（权限名称）】	1）各帐户权限设置与实际业务需求一致。	符合情况：对登录的用户分配了不同的账户，且分配了不同的权限。 部分符合情况：无部分符合情况。 不符合情况：未对登录的用户分配不同的账户，且未分配相关的权限。
访问控制	[关键]b)应重命名或删除默认账户，修改默认账户或预设账户的默认口令。（F3）	对于路由器的默认账户，由于他们的某些权限与实际要求可能存在差异，从而造成安全隐患，因此这些默认账户应被禁用，并且应不存在默认账户admin.huawei及默认口令	1、使用默认账户和默认口令无法登录路由器 2、华为H3C交换机不存在默认账户admin, huawei 华为H3C交换机输入“display local-user”确认存在的用户	1）重命名默认账户、禁用或删除默认账户； 2）修改了默认帐户的默认口令。	符合情况：已重命名或删除默认账户，且已修改默认账户的默认口令。 部分符合情况：预期结果1,2为一部分符合为部分符合。 不符合情况：未重命名或删除默认账户，且使用默认口令登录
访问控制	[关键]c)应用系统应对首次登录的用户提示修改默认账户或预设账户的默认口令。（F3）	应用系统应对首次登录的用户提示修改默认账户或预设账户的默认口令。	此项不适合，该项要求一般在应用系统上实现	此项不适合，该项要求一般在应用系统上实现	此项不适合，该项要求一般在应用系统上实现
访问控制	[重要]d)应及时删除或停用多余的、过期的账户，避免共享账户的存在。	路由器中如果存在多余的、过期的账户，可能会被攻击者利用其进行非法操作的风险，因此应及时清理路由器中的账户，删除或停用多余的账户	1、华为/H3C:输入display current-configuration命令，查看每条如下类似命令所配置的用户名是否确实必要: local-user xxxxx privilege level x 2、与管理员确认账号的使用人员，分析是否存在共享账户、过期多余账户。	1）不存在多余或过期账户； 2）管理员用户与账户之间一一对应。	符合情况：通过display current-configuration未发现多余、过期账户存在，且管理员用户与账户之间一一对应，无共享账户存在。 部分符合情况：预期结果1,2为一部分符合为部分符合。 不符合情况：设备存在多余、过期账户，且存在共享账户

访问控制	[一般]e)应授予管理用户所需的最小权限，实现管理用户的权限分离。	根据管理用户的角色对权限进行细致的划分，有利于各岗位细致协调工作，同时仅授予管理用户所需的最小权限，避免出现权限的漏洞使得一些高级用户拥有过大的权限。例如，进行角色划分，分为网络管理员、安全管理员、系统管理员三个角色，并设置对应的权限	1、访谈管理员，进行角色划分，分为网络管理员，安全管理员、系统管理员三个角色，并设置对应的权限 2、华为/H3C交换机;输入display current-configuration命令,存在如下类似配置: local-user userl service-type telnet user privilede level 2 # local-user user2 service-type ftp user privilede level 3 3.网络管理员、安全管理员、系统管理员对应的账户为其工作任务所	1）合理角色划分，管理用户的权限是否已进行分离（如管理员、审计员、操作员）； 2）各用户权限为其工作任务所需的最小权限。	符合情况：创建有系统管理员、审计管理员、安全管理员等账户通过LEVEL进行等级划分，并赋予去角色权限，各账户仅分配最小的权限。 部分符合情况：预期结果1,2为一部分符合为部分符合。 不符合情况：未创建系统管理员、审计管理员、安全管理员等账户角色，各账户均具备相同的管理员权限。
访问控制	[关键]f)应严格限制默认账户或预设账户的权限，如默认账户和预设账户的权限应为空权限或某单一功能专用权限等。（F3）	严格限制默认账户或预设账户的权限，如默认账户和预设账户的权限应为空权限或某单一功能专用权限等。	1)应核查限制默认账户或预设账户的权限分配和限制措施	对默认账户或预设账户的权限进行限制	符合情况：对默认账户或预设账户的权限进行限制 部分符合情况：/ 不符合情况：未对默认账户或预设账户的权限进行限制
访问控制	[一般]g)应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。	此项不适合，条款主要针对主机和数据库的测评，网络设备主要用户为运维管理人员，无其他用户	1)应核查是否由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。	由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。	符合情况：由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。 部分符合情况：/ 不符合情况：未由授权主体配置访问控制策略，访问控制策略规定主
访问控制	[一般]h)访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级。	此项不适合，条款主要针对主机和数据库的测评，网络设备主要用户为运维管理人员，无其他用户	1)应核查访问控制的粒度是否达到主体为用户级或进程级，客体为文件、数据库表级。	访问控制的粒度达到主体为用户级或进程级，客体为文件、数据库表级。	符合情况：访问控制的粒度达到主体为用户级或进程级，客体为文件、数据库表级。 部分符合情况：/ 不符合情况：访问控制的粒度未达到主体为用户级或进程级，客体未达到
访问控制	[一般]i)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	敏感标记是强制访问控制的依据，主客体都有,它存在的形式无所谓，可能是整形的数字，也可能是字母，总之它表示主客体的安全级别。敏感标记由安全管理员进行设置，通过对重要信息资源设置敏感标记，决定主体以何种权限对客体进行操作，实现强制访问控制	1)应核查是否对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	符合情况：对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。 部分符合情况：/ 不符合情况：未对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问

安全审计	[重要]a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。	为了对网络设备的运行状况、网络流量、管理记录等进行检测和记录，需要启用系统日志功能。系统日志中的每个信息都被分配了一个严重级别，并伴随一些指示性问题或事件的描述信息。 交换机的系统日志信息通常输出至各种管理端口、内部缓存或者日志服务器,在缺省情况下，控制台端口上的日志功能处于启用状态	1、华为/H3C:网络设备设置日志服务器，并使用Syslog方式或者SNMP方式将日志发送到日志服务器， 通过输入”display current-configuration“命令，存在如下类似配置： Info-center enable Info-center loghost source vlan-interface 3 Info-center loghost 192.10.12.1 facility local 1 Info-center source default channel 2 log level warning Snmp-agent snmp-agent trap enable standard authentication snmp-agent target-host trap address udp-domain 10.1.1.1 params	1）开启了日志审计功能； 2）审计范围覆盖到每个用户； 3）对重要的用户行为和重要安全事件进行了审计。	符合情况：设备已开启log日志功能，审计范围能覆盖到每个用户，并对每个重要安全事件进行审计。 部分符合情况：预期结果1,2,3为一部分符合为部分符合。 不符合情况：设备未开启日志功能，未能审计到每个用户行为以及重要安全事件。
安全审计	[一般]b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	对于交换机设备，日志审计内容需要记录时间、类型、用户、事件类型、事件是否成功等相关信息	1、华为/H3C:网络设备配置的日志策略，通过输入”display logging“或“display logbuffer”命令，存在如下类似配置： %Jan 31 00:38:22:216 2019 Spine ACL/6/PFILTER_STATIS_INFO: -MDC=1-Chassis=1-Slot=1; GigabitEthernet1/1/0/42 (inbound): Packet-filter 3333 rule 2 permit icmp source 192.168.1.10 0 logging counting 7 packet(s).	1）审计记录包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； 2）系统时间正确。	符合情况：审计记录能覆盖到具体的日期和时间、用户、事件类型、事件是否成功及审计相关信息，系统时间正确。 部分符合情况：预期结果1,2为一部分符合为部分符合。 不符合情况：未开启审计功能，审计记录未包含日期和时间、用户、事件类型、事件是否成功及其他审
安全审计	[关键]c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等，审计记录保存 时间应不少于 6 个月。（F3）	审计记录能修帮助管理人员及时发现系统运行状况和网络攻击行为，因此需要对审计记录实施技术上和管理上的保护，历正未授权修改、删除和破坏	1、华为/H3C:网络设备配置的日志策略，通过输入”display current-configuration“命令，存在如下类似配置： Info-center enable Info-center loghost source vlan-interface 3 Info-center loghost 192.10.12.1 facility local 1 Info-center source default channel 2 log level warning Snmp-agent snmp-agent trap enable standard authentication snmp-agent target-host trap address udp-domain 10.1.1.1 params	1）部署了综合安全审计系统； 2）采取技术措施对审计记录进行保护； 3）定期备份设备审计记录。	符合情况：部署有第三方日志审计系统，设备日志上传至第三方审计平台进行保护，日志保存时间长达6个月。 部分符合情况：预期结果1,2,3为一部分符合为部分符合。 不符合情况：未部署第三方日志审计系统，未对审计记录进行保护，日志保存时间不满足6个月。
安全审计	[一般]d)应对审计进程进行保护，防止未经授权的中断。	保护好审计进程，当安全事件发生时能够及时记录事件发生的详细内容	应测试通过非审计员的其他账户来中断审计进程，验证审计进程是否受到保护	1）非审计员的其他账户不能中断审计进程。	符合情况：非审计管理员的其他账户不能中断审计进程。 部分符合情况：无部分符合情况。 不符合情况：非审计管理员的其他账户能中断审计进程。

安全审计	[关键]e)对于从互联网客户端登录的应用系统，应在用户登录时提供用户上一次非常用设备成功登录的日期、时间、方法、位置等信息。（F3）	对于从互联网客户端登录的应用系统，在用户登录时提供用户上一次非常用设备成功登录的日期、时间、方法、位置等信息。	此项不适合，该项要求一般在应用层面上核查	此项不适合，该项要求一般在应用层面上核查	此项不适合，该项要求一般在应用层面上核查
安全审计	[关键]f)审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的一致性与正确性。（F3）	审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的一致性与正确性。	1)应核查系统是否部署时钟同步服务器。	系统部署时钟同步服务器。	符合情况：系统部署时钟同步服务器。 部分符合情况：无部分符合情况。 不符合情况：系统未部署时钟同步服务器。
入侵防范	[重要]a)应遵循最小安装的原则，仅安装需要的组件和应用程序。	遵循最小安装原则，仅安装需要的组件和应用程序，能够极大的降低遭受攻击的可能性。及时更新系统补丁，避免遭受由于系统漏洞带来的风险	1)应核查设备是否遵循最小安装的原则，仅安装需要的组件和应用程序。	遵循最小安装的原则，仅安装需要的组件和应用程序。	符合情况：设备遵循最小安装的原则，仅安装需要的组件和应用程序。 部分符合情况：无部分符合情况。 不符合情况：设备未遵循最小安装的原则，安装了多余组件或程序
入侵防范	[关键]b)应关闭不需要的系统服务、默认共享和高危端口。	关闭不需要的系统服务、默认共享和高危端口，可以有效降低系统遭受攻击的可能性	输入diplay current-configuration命令，根据实际网络环境参考已经关闭不必要服务,例如： p http shutdown	1）已关闭非必要的系统服务。	符合情况：已关闭不需要的系统服务、默认共享和高危端口等。 部分符合情况：无部分符合情况。 不符合情况：存在多余系统服务ftp，telnet等，存在高危端口和共享端口等。
入侵防范	[重要]c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。	为了保证安全，需要对通过VTY访问网络设备的登录地址进行限制，避免未授权的访问，可以利用ip access-class 限制访问VTY的IP地址范围。同时，由于VTYs的数目有一定的限制，当所有的VTYs用完，就不能再建立远程的网络连接了。这就有可能被利用进行Dos (拒绝服务攻击)	检查配置信息中存在类似如下配置信息: acl number 2001 rule 10 permit source 10.1.100.0.0.0.255 user-interface vty 0 4 acl 2001 inbound authentication-mode scheme user privilege level 1	1）仅允许管理主机远程登录设备。	符合情况：通过策略限制设备仅通过某地址或地址段可进行远程管理。 部分符合情况：无部分符合情况。 不符合情况：未采取措施对远程管理设备的地址进行限制。
入侵防范	[关键]d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。	本条款要求应用系统应对数据的有效性进行验证，主要验证那些通过人机接口(如程序的界面)输入或通过通信接口输入的数据格式或长度是否符合系统设定要求，防止个别用户输入畸形数据而导致系统出错(如SQL注入攻击等),人而影响系统的正常使用甚至危害系统的安全	此项不适合，该项要求一般在应用层面上核查	此项不适合，该项要求一般在应用层面上核查	此项不适合，该项要求一般在应用层面上核查

入侵防范	[关键]e)应能通过使用漏洞扫描工具、人工漏洞排查分析等漏洞检查手段，及时发现可能存在的已知 漏洞，并在经过充分测试评估后，及时修补漏洞。（F3）	核查漏扫修补报告，管理员定期进行漏洞扫描。发现漏洞在经过充分测试评估后及时修补漏洞	1)应进行漏洞扫描，核查是否不存在高风险漏洞 2)应访谈系统管理员，核查是否在经过充分测试评估后及时修补漏洞	1）管理员定期进行漏洞扫描，发现漏洞，在经过充分测试评估后及时修补漏洞。	符合情况：定期对设备进行漏洞扫描，且针对发现的漏洞经过测试评估后及时进行修补。 部分符合情况：无部分符合情况。 不符合情况：未定期对设备进行漏洞扫描，且未进对发现的漏洞进行测评评估后及时进行修补。
入侵防范	[重要]f)应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。	要维护系统安全，必须进行主动监视，一般是在网络边界、 核心等重要节点处部署IDS. IPS等系统，或在防火墙、UTM房用入侵检测功能，以检查息是否发生了入侵和攻击	1)应核查防火墙是否有入侵检测功能，查看入侵检测功能是否正确启用 2)应核查在发生严重入侵事件时是否提供报警，报警方式般包括短信、邮件等	1设备具有入侵检测功能， 2在发生严重入侵事件时提供报警，报警方式般包括短信、邮件等	符合情况：具有入侵检测功能的设备在发生严重入侵事件时提供报警，报警方式般包括短信、邮件等 部分符合情况：无部分符合情况。 不符合情况：具有入侵检测功能的设备在发生严重入侵事件时无法提供报警。
入侵防范	[关键]g)所有安全计算环境设备应全部专用化，生产设备不得进行与业务不相关的操作。（F3）	所有安全计算环境设备全部专用化，生产设备不得进行与业务不相关的操作。	1)应核查设备是否全部专用化，	所有安全计算环境设备全部专用化，生产设备不得进行与业务不相关的操作。	符合情况：所有安全计算环境设备全部专用化，生产设备不得进行与业务不相关的操作。 部分符合情况：无部分符合情况。 不符合情况：安全计算环境设备未专用化，生产设备进行与业务相关的操作。
入侵防范	[关键]h)应能够有效屏蔽系统技术错误信息，不得将系统产生的错误信息直接或间接反馈到前台界面。（F3）	能够有效屏蔽系统技术错误信息，不得将系统产生的错误信息直接或间接反馈到前台界面。	此项不适合，该项要求一般在应用层面上核查	此项不适合，该项要求一般在应用层面上核查	此项不适合，该项要求一般在应用层面上核查
恶意代码防范	[关键]a)应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断并定期统一进行升级和更新防恶意代码库。（F3）	无论是Windows主机还是Linux主机，都面临木马、蠕虫等病毒的破坏。因此一般的主机为防范病毒，均会安装反病毒软件，或者采用可信验证机制对系统程序、应用程序等进行可信执行验证	此项不适合，该项要求一般在服务器上实现	此项不适合，该项要求一般在服务器上实现	此项不适合，该项要求一般在服务器上实现
恶意代码防范	[关键]b)应建立病毒监控中心，对网络内计算机感染病毒的情况进行监控。（F3）	建立病毒监控中心，对网络内计算机感染病毒的情况进行监控。	此项不适合，该项要求一般在服务器上实现	此项不适合，该项要求一般在服务器上实现	此项不适合，该项要求一般在服务器上实现

可信验证	[一般]a)可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	设备应作为通信设备或边界设备对待	1)应核查是否基于可信根对设备的系统引导程序、系统程序、重要配置参数和关键应用程序等进行可信验证 2)应核查是否在应用程序的关键执行环节进行动态可信验证 3)应测试验证当检测到设备的可信性受到破坏后是否进行报警 4)应测试验证结果是否以审计记录的形式送至安全管理中心 (2.3)	1)计算设备具有可信根芯片或硬件 2)启动过程基于可信根对系统引导程序、系统程序，重要配置参数和关键应用程序等进行可信验证度量 3)在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心 4)安全管理中心可以接收设备的验证结果记录 (2.3)	符合情况：计算设备均部署了可信芯片或硬件进行可信验证，均基于可信根对引导程序、系统程序，重要配置参数和关键应用程序进行可信验证度量，在检测到可信性破坏后进行报警，并将验证结果送至安全管理中心，并验证。 部分符合情况：预期结果1，2，3，4点满足一部分为部分符合。 不符合情况：未采取措施计算设备部署了可信芯片或硬件进行可信验证，均基于可信根对引导程序、系统程序，重要配置参数和关键应用程序进行可信验证度量，在检测到可信性破坏后进行报警，并将验证结果送至安全管理中心，并验证。
数据完整性	[重要]a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。	采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。	1)应核查设备涉及哪几种数据类型 2)涉及传输的数据采用什么方式保证数据的完整性	1）系统提供对鉴别数据、重要审计数据、重要配置数据等在传输过程中的完整性保护措施 2）系统检测到鉴别数据、重要审计数据、重要配置数据等在传输过程中的完整性受到被坏后采取了技术措施进行处理，如重传或其他方式	符合：系统通过校验技术或密码技术保证所有重要数据在传输过程中的完整性， 部分符合：系统通过校验技术或密码技术保证部分数据在传输过程中的完整性， 不符合：系统未采用校验技术或密码技术无法保证重要数据在传输过程中的完整性，
数据完整性	[关键]b)应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。	采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。	1)应核查设备涉及哪几种数据类型 2)涉及存储的数据采用什么方式保证数据的完整性	1)系统采用校验技术或密码技术保证了鉴别数据、重要审计数据、重要配置数据等在存储过程中的完整性 2)系统可检测到鉴别数据、重要审计数据、重要配置数据等被修改的行为，并具备恢复措施	符合：系统通过校验技术或密码技术保证所有重要数据在存储过程中的完整性， 部分符合：系统通过校验技术或密码技术保证部分数据在存储过程中的完整性， 不符合：系统未采用校验技术或密码技术无法保证重要数据在存储过程中的完整性，
数据保密性	[关键]a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。	采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。	1)应核查设备涉及哪几种数据类型 2)涉及传输的数据采用什么方式保证数据的保密性	1）系统提供对鉴别数据、重要审计数据、重要配置数据等在传输过程中的保密性保护措施 2）系统检测到鉴别数据、重要审计数据、重要配置数据等在传输过程中的保密性受到被坏后采取了技术措施进行处理，如重传或其他方式	符合：系统通过校验技术或密码技术保证所有重要数据在存储过程中的保密性， 部分符合：系统通过校验技术或密码技术保证部分数据在存储过程中的保密性， 不符合：系统未采用校验技术或密码技术无法保证重要数据在存储过程中的保密性

数据保密性	[关键]b)应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于系统鉴别数据、重要业务数据和个人金融信息中的客户鉴别信息以及与账号结合使用可鉴别用户身份的鉴别辅助 信息等个人敏感信息，对于其他直接反应特定自然人某些情况的信息，宜使用密码技术保护 其存储过程中的保密性。（F3）	采用密码技术保证重要数据在存储过程中的保密性，包括但不限于系统鉴别数据、重要业务数据和个人金融信息中的客户鉴别信息以及与账号结合使用可鉴别用户身份的鉴别辅助 信息等个人敏感信息，对于其他直接反应特定自然人某些情况的信息，宜使用密码技术保护 其存储过程中的保密性。	1)应核查设备涉及哪几种数据类型 2)涉及存储的数据采用什么方式保证数据的保密性	1)系统采用校验技术或密码技术保证了鉴别数据、重要审计数据、重要配置数据等在存储过程中的保密性 2)系统可检测到鉴别数据、重要审计数据、重要配置数据等被修改的行为，并具备恢复措施	符合：系统通过校验技术或密码技术保证所有重要数据在存储过程中的保密性， 部分符合：系统通过校验技术或密码技术保证部分数据在存储过程中的保密性， 不符合：系统未采用校验技术或密码技术无法保证重要数据在存储过程中的保密性
数据备份恢复	[关键]a)应提供重要数据的本地数据备份与恢复功能，采取实时备份与异步备份或增量备份与完全备 份的方式，增量数据备份每天一次，完全数据备份可根据系统的业务连续性保障相关指（如 RPO，RTO）以及系统数据的重要程度、行业监管要求，制定备份策略。备份介质场外存放， 数据保存期限依照国家相关规定。（F3）	提供重要数据的本地数据备份与恢复功能，采取实时备份与异步备份或增量备份与完全备 份的方式，增量数据备份每天一次，完全数据备份可根据系统的业务连续性保障相关指（如 RPO，RTO）以及系统数据的重要程度、行业监管要求，制定备份策略。备份介质场外存放， 数据保存期限依照国家相关规定。	1)应核查设备的备份恢复策略	系统数据采取实时备份与异步备份或增量备份与完全备 份的方式，增量数据备份每天一次，	符合：系统配置数据采取实时备份与异步备份或增量备份与完全备份的方式，增量数据备份每天一次， 部分符合：/ 不符合：未对系统配置数据进行备份处理。
数据备份恢复	[重要]b)应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地。	提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地。	1)应核查设备的数据异地备份策略	系统数据进行异地实时备份，	符合：系统数据进行异地实时备份， 部分符合：/ 不符合：系统未部署异地实时备份环境。
数据备份恢复	[关键]c)应提供重要数据处理系统的热冗余，保证系统的高可用性。	提供重要数据处理系统的热冗余，保证系统的高可用性。	1)应核查设备的部署方式，是否采用热冗余方式进行部署	设备的部署方式采用热冗余方式进行部署	符合：设备采用热冗余方式进行部署 部分符合：无部分符合 不符合：设备未采用热冗余方式进行部署
数据备份恢复	[关键]d)对于同城应用级灾难备份中心，应与生产中心直线距离至少达到30km，可以接管所有核心业 务的运行；对于异地应用级灾难备份中心，应与生产中心直线距离至少达到100km。（F3）	于同城应用级灾难备份中心，应与生产中心直线距离至少达到30km，可以接管所有核心业 务的运行；对于异地应用级灾难备份中心，应与生产中心直线距离至少达到100km。	1)应核查系统是否部署灾难备份中心，生产中心与灾备中心的直线距离是否满足要求。	系统部署灾难备份中心，生产中心与灾备中心的直线距离满足要求。	符合：系统部署灾难备份中心，生产中心与灾备中心的直线距离满足要求。 部分符合：无部分符合 不符合：系统未部署灾难备份中心
数据备份恢复	[关键]e)为满足灾难恢复策略的要求，应对技术方案中关键技术应用的可行性进行验证测试，并记录 和保存验证测试结果。（F3）	为满足灾难恢复策略的要求，应对技术方案中关键技术应用的可行性进行验证测试，并记录 和保存验证测试结果。	1)应核查是否对关键技术应用的可行性进行验证测试。 2)核查是否具备验证测试记录	对关键技术应用的可行性进行验证测试，并保存有相关验证测试记录	符合：对关键技术应用的可行性进行验证测试，并保存有相关验证测试记录 部分符合：无部分符合 不符合：未对关键技术应用的可行性进行验证测试
数据备份恢复	[关键]f)数据备份应至少保存两个副本，且至少一份副本异地存放，完全数据备份至少保证以一个星 期为周期的数据冗余。（F3）	数据备份应至少保存两个副本，且至少一份副本异地存放，完全数据备份至少保证以一个星 期为周期的数据冗余。	1)应核查数据备份是否至少保存两个副本，且至少一份副本异地存放， 2)核查是否具备数据备份记录	数据备份至少保存两个副本，且至少一份副本异地存放，并具备数据备份记录	符合：1数据备份至少保存两个副本， 2至少一份副本异地存放，3具备数据备份记录 部分符合：预期结果1,2，3为一部分符合为部分符合。 不符合：数据备份未保存两个副本
数据备份恢复	[关键]g)异地灾难备份中心应配备恢复所需的运行环境，并处于就绪状态或运行状态，“就绪状态” 指备份中心的所需资（相关软硬件以及数据等资源）已完全满足但设备CPU还没有运行，“运行状态”指备份中心除所需资源完全满足要求外，CPU也在运行状态。（F3）	异地灾难备份中心应配备恢复所需的运行环境，并处于就绪状态或运行状态，“就绪状态” 指备份中心的所需资（相关软硬件以及数据等资源）已完全满足但设备CPU还没有运行，“运行状态”指备份中心除所需资源完全满足要求外，CPU也在运行状态。	1)应核查异地灾难备份中心是否配备恢复所需的运行环境，是否处于就绪状态或运行状态，	异地灾难备份中心配备恢复所需的运行环境，处于就绪状态或运行状态，	符合：1异地灾难备份中心配备恢复所需的运行环境，2处于就绪状态或运行状态， 部分符合：预期结果1,2为一部分符合为部分符合。 不符合：异地灾难备份中心未配备恢复所需的运行环境，未处于就绪状态或运行状态

剩余信息保护	[关键]a)应保证操作系统、数据库系统和应用系统用户鉴别信息所在的存储空间被释放或重新分配前得到完全清除，无论这些信息是存放在硬盘上还是内存中。（F3）	保证操作系统、数据库系统和应用系统用户鉴别信息所在的存储空间被释放或重新分配前得到完全清除，无论这些信息是存放在硬盘上还是内存中。	1)应核查操作系统、数据库系统和应用系统用户鉴别信息所在的存储空间被释放或重新分配前是否得到完全清除，	此项不适合，该项要求一般在服务器、数据库和应用系统上实现	此项不适合，该项要求一般在服务器、数据库和应用系统上实现
剩余信息保护	[关键]b)应保证操作系统、数据库系统和应用系统用户存有敏感数据的存储空间被释放或重新分配前得到完全清除，无论这些信息是存放在硬盘上还是内存中。（F3）	保证操作系统、数据库系统和应用系统用户存有敏感数据的存储空间被释放或重新分配前得到完全清除，无论这些信息是存放在硬盘上还是内存中。	1)应核查操作系统、数据库系统和应用系统用户存有敏感数据的存储空间被释放或重新分配前是否得到完全清除，	此项不适合，该项要求一般在服务器、数据库和应用系统上实现	此项不适合，该项要求一般在服务器、数据库和应用系统上实现
个人信息保护	[关键]a)金融机构在收集、使用个人金融信息时，应遵循合法、正当、必要的原则，应以隐私政策等 方式公开收集、使用规则，向个人金融信息主体明示收集、使用信息的目的、方式和范围， 并获得个人信息主体的同意。（F3）	金融机构在收集、使用个人金融信息时，遵循合法、正当、必要的原则，应以隐私政策等 方式公开收集、使用规则，向个人金融信息主体明示收集、使用信息的目的、方式和范围， 并获得个人信息主体的同意。	1)应核查在收集、使用个人金融信息时，是否遵循合法、正当、必要的原则，是否以隐私政策等 方式公开收集、使用规则，向个人金融信息主体明示收集、使用信息的目的、方式和范围， 并获得个人信息主体的同意，	此项不适合，该项要求一般在数据库和应用系统上实现	此项不适合，该项要求一般在数据库和应用系统上实现
个人信息保护	[关键]b)应仅采集和保存业务必需的用户个人金融信息。（F3）	仅采集和保存业务必需的用户个人金融信息。	1)应核查是否仅采集和保存业务必需的用户个人金融信息。	此项不适合，该项要求一般在数据库和应用系统上实现	此项不适合，该项要求一般在数据库和应用系统上实现
个人信息保护	[关键]c)应根据“业务需要”和“最小权限”原则，进行个人金融信息相关权限管理，严格控制和分 配相关操作权限，应禁止未授权访问和非法使用用户个人金融信息。（F3）	根据“业务需要”和“最小权限”原则，进行个人金融信息相关权限管理，严格控制和分 配相关操作权限，应禁止未授权访问和非法使用用户个人金融信息。	1)应核查是否根据“业务需要”和“最小权限”原则，进行个人金融信息相关权限管理，	此项不适合，该项要求一般在数据库和应用系统上实现	此项不适合，该项要求一般在数据库和应用系统上实现
个人信息保护	[关键]d)金融机构应依据 JR/T 0171—2020 对个人金融信息收集、传输、存储、使用、删除、销毁等 处理的整个过程进行管理与控制，并对个人金融信息生命周期过程进行安全检查与评估。（F3）	金融机构应依据 JR/T 0171—2020 对个人金融信息收集、传输、存储、使用、删除、销毁等 处理的整个过程进行管理与控制，并对个人金融信息生命周期过程进行安全检查与评估。	1)应核查是否依据 JR/T 0171—2020 对个人金融信息收集、传输、存储、使用、删除、销毁等 处理的整个过程进行管理与控制，	此项不适合，该项要求一般在数据库和应用系统上实现	此项不适合，该项要求一般在数据库和应用系统上实现
个人信息保护	[关键]e)金融机构应依据国家与行业主管部门要求，对通过计算机屏幕、客户端软件、银行卡受理设 备、ATM 设备、自助终端设备、纸（如受理终端打印出的支付交易凭条等交易凭证）等界面 展示的个人金融信息，应采取字段屏蔽（或截词）等处理措施，降低个人金融信息在展示环 节的泄露风险。（F3）	金融机构依据国家与行业主管部门要求，对通过计算机屏幕、客户端软件、银行卡受理设 备、ATM 设备、自助终端设备、纸（如受理终端打印出的支付交易凭条等交易凭证）等界面 展示的个人金融信息，应采取字段屏蔽（或截词）等处理措施，降低个人金融信息在展示环 节的泄露风险。	1)应核查是否依据国家与行业主管部门要求，对通过计算机屏幕、客户端软件、银行卡受理设 备、ATM 设备、自助终端设备、纸（如受理终端打印出的支付交易凭条等交易凭证）等界面 展示的个人金融信息，采取字段屏蔽（或截词）等处理措施，	此项不适合，该项要求一般在数据库和应用系统上实现	此项不适合，该项要求一般在数据库和应用系统上实现
个人信息保护	[关键]f)应向个人金融信息主体告知共享、转让个人金融信息的目的、数据接收方的身份和数据安全 保护能力，并事先征得个人金融信息主体明示同意，共享、转让经去标识化处理的个人金融 信息，且确保数据接收方无法重新识别个人金融信息主体的除外。（F3）	向个人金融信息主体告知共享、转让个人金融信息的目的、数据接收方的身份和数据安全 保护能力，并事先征得个人金融信息主体明示同意，共享、转让经去标识化处理的个人金融 信息，且确保数据接收方无法重新识别个人金融信息主体的除外。	1)应核查是否向个人金融信息主体告知共享、转让个人金融信息的目的、数据接收方的身份和数据安全保护能力，	此项不适合，该项要求一般在数据库和应用系统上实现	此项不适合，该项要求一般在数据库和应用系统上实现
个人信息保护	[关键]g)开发环境、测试环境不应使用真实的个人金融信息，应使用虚构的或经过去标识化处理的个 人金融信息，账号、卡号、协议号、支付指令等测试确需除外。（F3）	开发环境、测试环境不应使用真实的个人金融信息，应使用虚构的或经过去标识化处理的个 人金融信息，账号、卡号、协议号、支付指令等测试确需除外。	1)应核查开发环境、测试环境是否使用真实的个人金融信息，是否使用虚构的或经过去标识化处理的个人金融信息，账号、卡号、协议号、支付指令等测试确需除外。	此项不适合，该项要求一般在数据库和应用系统上实现	此项不适合，该项要求一般在数据库和应用系统上实现

安全计算环境-安全设备-防火墙（S3A3G3）作业指导书					
安全控制点	检测项	要求解读	测评方法	预期结果或主要证据	符合情况
身份鉴别	[关键]a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，应实现身份鉴别信息防窃取和 防重用。静态口令应在8位以上，由字母、数字、符号等混合组成并每半年更换口令，不允许新设定的口令与前次旧口令相同。应用系统用户口令应在满足口令复杂度要求的基础上定 期更换。（F3）	为了安全起见，防火墙器只有经过授权的合法用户才能访问，一般来说，用户登录防火墙的方式包括:通过浏览器以WEB方式登录，通过Console口以命令行方式登录，通过SSH方式登录。防火墙为了便于用户管理，还提供了图形界面管理工具便于用户对设备进行管理和维护。无论是采用哪一种的呢公路方式，都需要对用户身份进行鉴别。 防火墙不允许配置用户名相同的用户，同时要防止多人共用一个账户，实行分账户管理，每名管理员设置一个单独的账户，避免出现问题后不能及时进行追查。 同时为避免身份鉴别信息被冒用，应当保证口令复杂度和定期更改的要求	1)以天融信防火墙为例，核查用户在登录时是否来用里身份鉴别措施。 通过浏览器以WEB方式登录 打开IE浏览器，在地址输入框中输入网络卫士防火墙的URL地址，如https://xxx。回车后进入防火墙的登录界面，，提示用户输入用户名和密码 输入用户名和密码后，点击”登录“按钮，即可登录到网络卫士防火墙。登录后，用户就可通过WEB界面对防火墙进行配置管理: 1)应核查防火墙管理员账户列表，测试用户身份标识是否具有唯一性，核查是否存在多人共用账户的情况，核查是否存在空口令用户。 2)应询问管理员对身份鉴别所采取的具体措施，确认口令长度是否8位以上，是否由数字、大小写字母和特殊字符中的两种以上组成，口令是否每季度至少更改一次	1)防火墙使用口令鉴别机制对登录用户进行身份标识和鉴别 2)用户身份标识具有唯一性，不存在多人共用账户的情况，不存在空口令用户 3)口令长度8位以上，由数字、大小写字母和特殊字符中的两种以上组成，口令每季度至少更改一次	符合情况：通过用户名口令方式登录，口令长度8位以上，口令复杂度包含大写字母、小写字母、数字，口令有效期为90天; 部分符合情况：通过用户名口令方式登录，口令长度8位以上，复杂度为小写字母、数字、特殊字符，但未配置口令有效期; 不符合情况：通过用户名口令方式登录，口令长度为6位，复杂度为纯数字，未配置口令有效期，口令为弱口令。
身份鉴别	[关键]b)应具有登录失败处理功能，应配置并启用结束会话、限制登录间隔、限制非法登录次数和当登 录连接超时自动退出等相关措施。（F3）	可以通过配置结束会话、限制管理员的最大登录失败次数、网络连接超时自动退出等多种措施实现登录失败处理功能。例如，设置管理员最大登录失败次数，一旦该管理员的登录失败次数超过设定数值，系统将对其进行登录锁定，从而防止非法用户通过暴力破解的方式登录到防火墙	1)应核查是否配置并启用了登录失败处理功能，核查是否配置并启用了限制非法登录达到一定次数后实现账户锁定功能 2)应核查是否配置并启用了远程登录连接超时并自动退出功能	1)配置并启用了登录失败处理功能，配置并启用了限制非法登录达到一定次数后实现账户锁定功能。 进入管理界面。然后在左侧导航树中选择系统管理>>配置，激活“系统参数”页签，。 选中“高级属性”左侧的复选框，可以查看到“最大登录失败次数”的配置，。 2)配置并启用了远程登录连接超时并自动退出功能。 进入管理界面。然后在左侧导航树中选择系统管理>配置,激活“系统参数”页签，: 选中“高级属性”左侧的复选框，可以查看到“远程登录连接超时”的配置，	符合情况：已配置登录失败处理功能，连续登录失败5次锁定账户30分钟，会话空闲30分钟自动退出; 部分符合情况：已配置登录失败处理功能，连续登录失败5次锁定账户30分钟，但未配置连接超时自动退出措施; 不符合情况：未配置登录失败处理功能和连接超时自动退出措施。

身份鉴别	[关键]c)当进行远程管理时，应对管理终端进行身份标识和鉴别，采用密码技术防止鉴别信息在网络 传输过程中被窃听。（F3）	为避免口令传输过程中别窃取，不应当使用明文传送的Telnet、HTTP服务，而应当采用SSH、ITTPS等加密协议等方式进行交互式管理	应询问系统管理员采用何种方式对防火墙进行远程管理,核查通过WEB界面管理是否都通过SSL协议进行加密处理	通过WEB界面进行远程管理时，通过SSL协议进行加密处理	符合情况：仅采用https协议进行管理，防止鉴别信息在网络传输过程中被窃听； 不符合情况：仅采用http协议进行管理，无法防止鉴别信息在网络传输过程中被窃听。
身份鉴别	[关键]d)应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	采用双因子鉴别是防止欺骗的有效方法，双因子鉴别不仅要求访问者知道一些鉴别信息，还需要访问者拥有鉴别特征，例如采用令牌、智能卡等.目前主流防火墙多采用“本地口令+证书认证”的方式进行认证。“本地口令+证书认证”认证时，用户既要通过防火墙内部认证服务器的口令认证，也要通过证书认证才能够成功登录防火墙	进入管理界面。然后在左侧导航树中选择用户认证>>用户管理,激活“用户管理”页签， 2）右侧显示用户列表信息， 3)如果需要对用户进行两种或两种以上组合的鉴别技术，点击该用户条目右侧的“修改”图标，查看该用户的认证方式应该为“本地口令+证书认证”或者“外部口令+证书认证”。 例如，管理员希望对用户“doc”同时进行证书认证和外部服务器的口令认证，则点击用户“doc”条目右侧的“修改”图标后，用户属性的“认证方式”应该为“外部口令+证书认证”。	，通过浏览器以WEB方式登录。 查看该用户的认证方式应该为“本地口令+证书认证”或者“外部口令+证书认证”。	符合情况：通过用户名口令和谷歌验证码方式登录，验证码长度为6位，有效时间为30秒； 不符合情况：通过用户名口令方式登录，未采用两种或两种以上鉴别技术对用户进行身份鉴别。
访问控制	[重要]a)应对登录的用户分配账户和权限。	为了确保防火墙的安全，需要对登录的用户分配账户，并合理配置账户权限	进入管理界面。然后在左侧导航树中选择用户认证>>用户管理,激活“用户管理”页签，右侧显示用户列表信息，。 1)应针对每一个用户账户，核查用户账启和权限设置情况是否合理，如账户管理员和配置管理员不应具有审计员权限。 2)应核查是否已禁用或限制匿名、默认账户的访问权限	1、相关管理人员具有与职位相对应的账户和权限 2、禁用或限制匿名、默认账户的访问权限	符合情况：已对可登录用户分配账户和权限，相关管理员与职位相对应； 不符合情况：已启用匿名登录模式。
访问控制	[关键]b)应重命名或删除默认账户，修改默认账户或预设账户的默认口令。（F3）	对于防火墙的默认账户，由于他们的某些权限与实际要求可能存在差异，从而造成安全隐患，因此这些默认账户应被禁用	进入管理界面。然后在左侧导航树中选择用户认证>>用户管理,激活“用户管理”页签，右侧显示用户列表信息，如 1)应核查是否重命名或删除这些默认账户 2)应核查是否已修改默认账户的默认口令	防火墙重命名或删除默认账户，修改默认账户的默认口令	符合情况：已重命名系统默认账户a*为***，且口令修改为复杂口令； 部分符合情况：未重命名系统默认账户a**,已修改口令为复杂口令； 不符合情况：未重命名系统默认账户名，口令为设备出厂默认口令
访问控制	[关键]c)应用系统应对首次登录的用户提示修改默认账户或预设账户的默认口令。（F3）	应用系统应对首次登录的用户提示修改默认账户或预设账户的默认口令。	此项不适合，该项要求一般在应用系统上实现	此项不适合，该项要求一般在应用系统上实现	此项不适合，该项要求一般在应用系统上实现

访问控制	[重要]d)应及时删除或停用多余的、过期的账户，避免共享账户的存在。	防火墙中如果存在多余的、过期的账户，可能会被攻击者利用其进行非法操作的风险，因此应及时清理路由器中的账户，删除或停用多余的账户	进入管理界面。然后在左侧导航树中选择用户认证>>用户管理,激活“用户管理”页签，右侧显示用户列表信息， 1) 应核查防火墙用户账户列表，询问管理员各账户的具体用途，分析是否存在多余或过期账户，并核查管理员用户与账户之间是否一一对应。 2)如果因为种种原因导致某些多余的、过期的账户无法被删除，则应测试是否已经停用了这些多余的、过期的账户	防火墙用户账户列表不存在多余或过期账户，不存在共享用户	符合情况：设备中未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况； 部分符合情况：管理员用户与账户之间一一对应，未发现共享账户的情况，但a*、s*为多余账户； 不符合情况：可登录账户仅有a*，所有管理员均通过a*登录。
访问控制	[一般]e)应授予管理用户所需的最小权限，实现管理用户的权限分离。	根据管理用户的角色对权限进行细致的划分，有利于各岗位细致协调工作，同时仅授予管理用户所需的最小权限，避免出现权限的漏洞使得一些高级用户拥有过大的权限	进入管理界面。然后在左侧导航树中选择用户认证>>用户管理,激活“用户管理”页签，右侧显示用户列表信息， 1)应核查是否进行角色划分，系统中的账户分为系统管理员、安全管理员和审计管理员三类,其中，安全管理员可以制定安全策略，系统管理员可以配置安全策略，审计管理员可以查看日志 2)应查看管理用户的权限是否已进行分离，是否为其工作任务所需的最小权限，如禁止对管理用户同时赋予配置管理员和审计管理员权限	1)系统用户进行角色划分，系统中的账户分为系统管理员、安全管理员和审计管理员三类。其中，安全管理员可以制定安全策略，系统管理员可以配置安全策略，审计管理员可以查看日志 2)管理用户的权限进行了分离，并为其工作任务所费的最小权限，如禁上对管理用户同时赋予配置管理员和审计管理员权限	符合情况：已配置安全管理员s*、审计管理员a*、系统管理员s*，授予管理用户所需的最小权限； 部分符合情况：已配置安全管理员s*、系统管理员s*，但未配置审计管理员； 不符合情况：可登录账户仅有a*，未授予管理用户所需的权限分离，实现管理用户的权限分离。
访问控制	[关键]f)应严格限制默认账户或预设账户的权限，如默认账户和预设账户的权限应为空权限或某单一 功能专用权限等。 (F3)	严格限制默认账户或预设账户的权限，如默认账户和预设账户的权限应为空权限或某单一 功能专用权限等。	1)应核查限制默认账户或预设账户的权限分配和限制措施	对默认账户或预设账户的权限进行限制	符合情况：对默认账户或预设账户的权限进行限制 部分符合情况：/ 不符合情况：未对默认账户或预设账户的权限进行限制
访问控制	[一般]g)应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。	此项不适合，条款主要针对主机和数据库的测评，网络设备主要用户为运维管理人员，无其他用户	1)应核查是否由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。	由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。	符合情况：由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。 部分符合情况：/ 不符合情况：未由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。

访问控制	[一般]h)访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级。	此项不适合，条款主要针对主机和数据库的测评，网络设备主要用户为运维管理人员，无其他用户	1)应核查访问控制的粒度是否达到主体为用户级或进程级，客体为文件、数据库表级。	访问控制的粒度达到主体为用户级或进程级，客体为文件、数据库表级。	符合情况：访问控制的粒度达到主体为用户级或进程级，客体为文件、数据库表级。 部分符合情况：/ 不符合情况：访问控制的粒度未达到主体为用户级或进程级，客体未达到文件、数据库表级。
访问控制	[一般]i)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	敏感标记是强制访问控制的依据，主客体都有,它存在的形式无所谓，可能是整形的数字，也可能是字母，总之它表示主客体的安全级别。敏感标记由安全管理员进行设置，通过对重要信息资源设置敏感标记，决定主体以何种权限对客体进行操作，实现强制访问控制	1)应核查是否对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	符合情况：对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。 部分符合情况：/ 不符合情况：未对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。
安全审计	[重要]a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。	为了对防火墙的运行状况、网络流量、管理记录等进行检测和记录，需要启用系统日志功能。系统日志中的每个信息都被分配了一个严重级别，并伴随一些指示性问题或事件的描述信息。 防火墙的系统日志信息通常输出至各种管理端口、内部缓存或者日志服务器,在缺省情况下，控制台端口上的日志功能处于启用状态	进入管理界面。然后在左侧导航树中选择日志与报警>>日志设置,激活“用户管理”页签，右侧显示用户列表信息， 在右侧显示“日志设置”页面，设置正确的服务器地址、端口、以及日志级别和日志类型等信息。例如，如果希望记录0-3级的阻断策略日志，则“日志级别右侧的下拉框中应该设置为“3”,并且勾选了“阻断策略”的日志类型，	防火墙设置正确的服务器地址、端口、以及日志级别和日志类型等信息	符合情况：已开启安全审计功能，可对所有重要的用户行为和重要安全事件进行审计，审计范围覆盖系统内所有用户； 不符合情况：无审计模块，无法对重要的用户行为和安全事件进行审计。
安全审计	[一般]b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	对于防火墙来说，审计内容应包括时间、类型、用户、事件类型、事件是否成功等相关信息	进入管理界面。然后在左侧导航树中选择日志与报警>>日志设置,激活“用户管理”页签，右侧显示用户列表信息，。 登录日志服务器，并选择管理策略》日志收集源，进入日志源配置界面，查看所有日志收集源。确保日志源列表中包含了该防火墙的IP。 在日志服务器上，选择功能>>日志查询并选择“审计域”页签。根据IP地址选择防火墙后，便可对该防火墙的日志进行核查，确认是否包括日期和时间、用户、事件类型、事件是否成功等相关的信息	审计记录包括事件的日期和时间、用户事件类型、事件是否成功及其他与审计相关的信息。	符合情况：审计记录包括事件的日期和时间、用户事件类型、事件是否成功及其他与审计相关的信息。 部分符合情况：仅有用户信息、登录时间。 不符合情况：无审计模块。

安全审计	[关键]c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等，审计记录保存 时间应不少于 6 个月。（F3）	审计记录能修帮助管理人员及时发现系统运行状况和网络攻击行为，因此需要对审计记录实施技术上和管理上的保护，防止未授权修改、删除和破坏	进入管理界面。然后在左侧导航树中选择日志与报警>>日志设置,激活“用户管理”页签，右侧显示用户列表信息， 登录日志服务器，并选择管理策略》日志收集源，进入日志源配置界面，查看所有日志收集源。确保日志源列表中包含了该防火墙的IP。 收集到的日志数据会保存在日志系统的数据库中，通过对数据库进行备份操作，便可实现防火墙数据的备份和保护。 在日志服务器上，选择管理策略》》任务调度策略，然后在左侧“本地配置”分页中点击“任务调度策略”，确保存在类型为“备份数据库任务”的计划任务。这些任务会定时执行数据库的备份任务，进而达到备份防火墙日志信息的目的	防火墙日志信息定期转发至日志服务器，日志服务器上可查看到半年前的审计记录	符合情况：已对审计记录记录进行保护，审计记录实时传输至日志审计设备，并留存半年以上，能够避免受到未预期的删除、修改或覆盖； 部分符合情况：已对审计记录记录进行保护，审计记录实时传输至日志审计设备，但审计记录仅留存7天，无法够避免受到未预期的删除、修改或覆盖； 不符合情况：未对审计记录记录进行保护，审计记录仅留存7天，无法够避免受到未预期的删除、修改或覆盖。
安全审计	[一般]d)应对审计进程进行保护，防止未经授权的中断。	保护好审计进程，当安全事件发生时能够及时记录事件发生的详细内容	应测试通过非审计员的其他账户来中断审计进程，验证审计进程是否受到保护	非审计员的其他账户来不能中断审计进程，验证审计进程是否得到保护	符合情况：审计进程权限配置合理，仅授权用户可终止审计进程； 不符合情况：审计进程权限配置不合理，部分普通用户可关闭审计进程。
安全审计	[关键]e)对于从互联网客户端登录的应用系统，应在用户登录时提供用户上一次非常用设备成功登录 的日期、时间、方法、位置等信息。（F3）	对于从互联网客户端登录的应用系统，在用户登录时提供用户上一次非常用设备成功登录 的日期、时间、方法、位置等信息。	此项不适合，该项要求一般在应用层面上核查	此项不适合，该项要求一般在应用层面上核查	此项不适合，该项要求一般在应用层面上核查
安全审计	[关键]f)审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的一致性与正 确性。（F3）	审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的一致性与正 确性。	1)应核查系统是否部署时钟同步服务器。	系统部署时钟同步服务器。	符合情况：系统部署时钟同步服务器。 部分符合情况：无部分符合情况。 不符合情况：系统未部署时钟同步服务器。
入侵防范	[重要]a)应遵循最小安装的原则，仅安装需要的组件和应用程序。	遵循最小安装原则，仅安装需要的组件和应用程序，能够极大的降低遭受攻击的可能性。及时更新系统补丁，避免遭受由于系统漏洞带来的风险	1)应核查设备是否遵循最小安装的原则，仅安装需要的组件和应用程序。	遵循最小安装的原则，仅安装需要的组件和应用程序。	符合情况：设备遵循最小安装的原则，仅安装需要的组件和应用程序。 部分符合情况：无部分符合情况。 不符合情况：设备未遵循最小安装的原则，安装了多余组件或程序。

入侵防范	[关键]b)应关闭不需要的系统服务、默认共享和高危端口。	关闭不需要的系统服务、默认共享和高危端口，可以有效降低系统遭受攻击的可能性	1)应核查设备是否关闭不需要的系统服务、默认共享和高危端口。	1）已关闭非必要的系统服务。	符合情况：已关闭不需要的系统服务、默认共享和高危端口等。 部分符合情况：无部分符合情况。 不符合情况：存在多余系统服务ftp，telnet等，存在高危端口和共享端口等。
入侵防范	[重要]c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。	为了保证安全，避免未授权的访问，需要对远程管理防火墙的登录地址进行限制，可以是某一特定的IP地址，也可以来自某一子网、地址范围或地址组	进入管理界面。然后在左侧导航树中选择系统管理》配置，然后激活“开放服务”页签，。 在右侧页面中，应该存在“服务名称"为“webui”，"ssh" 或"telnet'的服务规则。	1）仅允许管理主机远程登录设备。	符合情况：通过策略限制设备仅通过某地址或地址段可进行远程管理。 部分符合情况：无部分符合情况。 不符合情况：未采取措施对远程管理设备的地址进行限制
入侵防范	[关键]d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。	本条款要求应用系统应对数据的有效性进行验证，主要验证那些通过人机接口(如程序的界面)输入或通过通信接口输入的数据格式或长度是否符合系统设定要求，防止个别用户输入畸形数据而导致系统出错(如SQL 注入攻击等),人而影响系统的正常使用甚至危害系统的安全	此项不适合，该项要求一般在应用层面上核查	此项不适合，该项要求一般在应用层面上核查	此项不适合，该项要求一般在应用层面上核查
入侵防范	[关键]e)应能通过使用漏洞扫描工具、人工漏洞排查分析等漏洞检查手段，及时发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。（F3）	核查漏扫修补报告，管理员定期进行漏洞扫描。发现漏洞在经过充分测试评估后及时修补漏洞	1)应进行漏洞扫描，核查是否不存在高风险漏洞 2)应访谈系统管理员，核查是否在经过充分测试评估后及时修补漏洞	1）管理员定期进行漏洞扫描，发现漏洞，在经过充分测试评估后及时修补漏洞。	符合情况：定期对设备进行漏洞扫描，且针对发现的漏洞经过测试评估后及时进行修补。 部分符合情况：无部分符合情况。 不符合情况：未定期对设备进行漏洞扫描，且未进对发现的漏洞进行测评评估后及时进行修补。
入侵防范	[重要]f)应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。	要维护系统安全，必须进行主动监视，一般是在网络边界、 核心等重要节点处部署IDS. IPS等系统，或在防火墙、UTM房用入侵检测功能，以检查息是否发生了入侵和攻击	1)应核查防火墙是否有入侵检测功能，查看入侵检测功能是否正确启用 2)应核查在发生严重入侵事件时是否提供报警，报警方式般包括短信、邮件等	1设备具有入侵检测功能， 2在发生严重入侵事件时提供报警，报警方式般包括短信、邮件等	符合情况：具有入侵检测功能的设备在发生严重入侵事件时提供报警，报警方式般包括短信、邮件等 部分符合情况：无部分符合情况。 不符合情况：具有入侵检测功能的设备在发生严重入侵事件时无法提供报警

入侵防范	[关键]g)所有安全计算环境设备应全部专用化，生产设备不得进行与业务不相关的操作。（F3）	所有安全计算环境设备全部专用化，生产设备不得进行与业务不相关的操作。	1)应核查设备是否全部专用化，	所有安全计算环境设备全部专用化，生产设备不得进行与业务不相关的操作。	符合情况：所有安全计算环境设备全部专用化，生产设备不得进行与业务不相关的操作。 部分符合情况：无部分符合情况。 不符合情况：安全计算环境设备未专用化，生产设备进行与业务相关的操作
入侵防范	[关键]h)应能够有效屏蔽系统技术错误信息，不得将系统产生的错误信息直接或间接反馈到前台界面。（F3）	能够有效屏蔽系统技术错误信息，不得将系统产生的错误信息直接或间接反馈到前台界面。	此项不适合，该项要求一般在应用层面上核查	此项不适合，该项要求一般在应用层面上核查	此项不适合，该项要求一般在应用层面上核查
恶意代码防范	[关键]a)应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断并定期统一进行升级和更新防恶意代码库。（F3）	无论是Windows主机还是Linux主机，都面临木马、蠕虫等病毒的破坏。因此一般的主机为防范病毒，均会安装反病毒软件，或者采用可信验证机制对系统程序、应用程序等进行可信执行验证	此项不适合，该项要求一般在服务器上实现	此项不适合，该项要求一般在服务器上实现	此项不适合，该项要求一般在服务器上实现
恶意代码防范	[关键]b)应建立病毒监控中心，对网络内计算机感染病毒的情况进行监控。（F3）	建立病毒监控中心，对网络内计算机感染病毒的情况进行监控。	此项不适合，该项要求一般在服务器上实现	此项不适合，该项要求一般在服务器上实现	此项不适合，该项要求一般在服务器上实现
可信验证	[一般]a)可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	设备应作为通信设备或边界设备对待	查看设备是否具有可信根芯片	1)计算设备具有可信根芯片或硬件 2)启动过程基于可信根对系统引导程序、系统程序，重要配置参数和关键应用程序等进行可信验证度量 3)在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心 4)安全管理中心可以接收设备的验证结果记录 (2.3)	符合情况：计算设备均部署了可信芯片或硬件进行可信验证，均基于可信根对引导程序、系统程序，重要配置参数和关键应用程序进行可信验证度量，在检测到可信性破坏后进行报警，并将验证结果送至安全管理中心，并验证。 部分符合情况：预期结果1，2，3，4点满足一部分为部分符合。 不符合情况：未采取措施计算设备部署了可信芯片或硬件进行可信验证，均基于可信根对引导程序、系统程序，重要配置参数和关键应用程序进行可信验证度量，在检测到可信性破坏后进行报警，并将验证结果送至安全管理中心，并验证。
数据完整性	[重要]a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。	采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。	1)应核查设备涉及哪几种数据类型 2)涉及传输的数据采用什么方式保证数据的完整性	1）系统提供对鉴别数据、重要审计数据、重要配置数据等在传输过程中的完整性保护措施 2）系统检测到鉴别数据、重要审计数据、重要配置数据等在传输过程中的完整性受到被坏后采取了技术措施进行处理，如重传或其他方式	符合：系统通过校验技术或密码技术保证所有重要数据在传输过程中的完整性， 部分符合：系统通过校验技术或密码技术保证部分数据在传输过程中的完整性， 不符合：系统未采用校验技术或密码技术无法保证重要数据在传输过程中的完整性，

数据完整性	[关键]b)应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。	采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。	1)应核查设备涉及哪几种数据类型 2)涉及存储的数据采用什么方式保证数据的完整性	1)系统采用校验技术或密码技术保证了鉴别数据、重要审计数据、重要配置数据等在存储过程中的完整性 2)系统可检测到鉴别数据、重要审计数据、重要配置数据等被修改的行为，并具备恢复措施	符合：系统通过校验技术或密码技术保证所有重要数据在存储过程中的完整性， 部分符合：系统通过校验技术或密码技术保证部分数据在存储过程中的完整性， 不符合：系统未采用校验技术或密码技术无法保证重要数据在存储过程中的完整性
数据保密性	[关键]a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。	采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。	1)应核查设备涉及哪几种数据类型 2)涉及传输的数据采用什么方式保证数据的保密性	1）系统提供对鉴别数据、重要审计数据、重要配置数据等在传输过程中的保密性保护措施 2）系统检测到鉴别数据、重要审计数据、重要配置数据等在传输过程中的保密性受到被坏后采取了技术措施进行处理，如重传或其他方式	符合：系统通过校验技术或密码技术保证所有重要数据在存储过程中的保密性， 部分符合：系统通过校验技术或密码技术保证部分数据在存储过程中的保密性， 不符合：系统未采用校验技术或密码技术无法保证重要数据在存储过程中的保密性，
数据保密性	[关键]b)应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于系统鉴别数据、重要业务数据和个人金融信息中的客户鉴别信息以及与账号结合使用可鉴别用户身份的鉴别辅助信息等个人敏感信息，对于其他直接反应特定自然人某些情况的信息，宜使用密码技术保护 其存储过程中的保密性。（F3）	采用密码技术保证重要数据在存储过程中的保密性，包括但不限于系统鉴别数据、重要业务数据和个人金融信息中的客户鉴别信息以及与账号结合使用可鉴别用户身份的鉴别辅助 信息等个人敏感信息，对于其他直接反应特定自然人某些情况的信息，宜使用密码技术保护 其存储过程中的保密性。	1)应核查设备涉及哪几种数据类型 2)涉及存储的数据采用什么方式保证数据的保密性	1)系统采用校验技术或密码技术保证了鉴别数据、重要审计数据、重要配置数据等在存储过程中的保密性 2)系统可检测到鉴别数据、重要审计数据、重要配置数据等被修改的行为，并具备恢复措施	符合：系统通过校验技术或密码技术保证所有重要数据在存储过程中的保密性， 部分符合：系统通过校验技术或密码技术保证部分数据在存储过程中的保密性， 不符合：系统未采用校验技术或密码技术无法保证重要数据在存储过程中的保密性
数据备份恢复	[关键]a)应提供重要数据的本地数据备份与恢复功能，采取实时备份与异步备份或增量备份与完全备 份的方式，增量数据备份每天一次，完全数据备份可根据系统的业务连续性保障相关指（如 RPO，RTO）以及系统数据的重要程度、行业监管要求，制定备份策略。备份介质场外存放， 数据保存期限依照国家相关规定。（F3）	提供重要数据的本地数据备份与恢复功能，采取实时备份与异步备份或增量备份与完全备 份的方式，增量数据备份每天一次，完全数据备份可根据系统的业务连续性保障相关指（如 RPO，RTO）以及系统数据的重要程度、行业监管要求，制定备份策略。备份介质场外存放， 数据保存期限依照国家相关规定。	1)应核查设备的备份恢复策略	系统数据采取实时备份与异步备份或增量备份与完全备 份的方式，增量数据备份每天一次，	符合：系统配置数据采取实时备份与异步备份或增量备份与完全备 份的方式，增量数据备份每天一次， 部分符合：/ 不符合：未对系统配置数据进行备份处理。
数据备份恢复	[重要]b)应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地。	提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地。	1)应核查设备的数据异地备份策略	系统数据进行异地实时备份，	符合：系统数据进行异地实时备份， 部分符合：/ 不符合：系统未部署异地实时备份环境。
数据备份恢复	[关键]c)应提供重要数据处理系统的热冗余，保证系统的高可用性。	提供重要数据处理系统的热冗余，保证系统的高可用性。	1)应核查设备的部署方式，是否采用热冗余方式进行部署	设备的部署方式采用热冗余方式进行部署	符合：设备采用热冗余方式进行部署 部分符合：无部分符合 不符合：设备未采用热冗余方式进行部署
数据备份恢复	[关键]d)对于同城应用级灾难备份中心，应与生产中心直线距离至少达到30km，可以接管所有核心业 务的运行；对于异地应用级灾难备份中心，应与生产中心直线距离至少达到100km。（F3）	于同城应用级灾难备份中心，应与生产中心直线距离至少达到30km，可以接管所有核心业 务的运行；对于异地应用级灾难备份中心，应与生产中心直线距离至少达到100km。	1)应核查系统是否部署灾难备份中心，生产中心与灾备中心的直线距离是否满足要求。	系统部署灾难备份中心，生产中心与灾备中心的直线距离满足要求。	符合：系统部署灾难备份中心，生产中心与灾备中心的直线距离满足要求。 部分符合：无部分符合 不符合：系统未部署灾难备份中心。

数据备份恢复	[关键]e)为满足灾难恢复策略的要求，应对技术方案中关键技术应用的可行性进行验证测试，并记录 和保存验证测试结果。（F3）	为满足灾难恢复策略的要求，应对技术方案中关键技术应用的可行性进行验证测试，并记录 和保存验证测试结果。	1)应核查是否对关键技术应用的可行性进行验证测试。 2)核查是否具备验证测试记录	对关键技术应用的可行性进行验证测试，并保存有相关验证测试记录	符合：对关键技术应用的可行性进行验证测试，并保存有相关验证测试记录 部分符合：无部分符合 不符合：未对关键技术应用的可行性进行验证测试
数据备份恢复	[关键]f)数据备份应至少保存两个副本，且至少一份副本异地存放，完全数据备份至少保证以一个星 期为周期的数据冗余。（F3）	数据备份应至少保存两个副本，且至少一份副本异地存放，完全数据备份至少保证以一个星 期为周期的数据冗余。	1)应核查数据备份是否至少保存两个副本，且至少一份副本异地存放， 2)核查是否具备数据备份记录	数据备份至少保存两个副本，且至少一份副本异地存放，并具备数据备份记录	符合：1数据备份至少保存两个副本， 2至少一份副本异地存放，3具备数据备份记录 部分符合：预期结果1,2，3为一部分符合为部分符合。 不符合：数据备份未保存两个副本
数据备份恢复	[关键]g)异地灾难备份中心应配备恢复所需的运行环境，并处于就绪状态或运行状态，“就绪状态”指备份中心的所需资（相关软硬件以及数据等资源）已完全满足但设备CPU还没有运行，“运行状态”指备份中心除所需资源完全满足要求外，CPU也在运行状态。（F3）	异地灾难备份中心应配备恢复所需的运行环境，并处于就绪状态或运行状态，“就绪状态”指备份中心的所需资（相关软硬件以及数据等资源）已完全满足但设备CPU还没有运行，“运行状态”指备份中心除所需资源完全满足要求外，CPU也在运行状态。	1)应核查异地灾难备份中心是否配备恢复所需的运行环境，是否处于就绪状态或运行状态，	异地灾难备份中心配备恢复所需的运行环境，处于就绪状态或运行状态，	符合：1异地灾难备份中心配备恢复所需的运行环境，2处于就绪状态或运行状态， 部分符合：预期结果1,2为一部分符合为部分符合。 不符合：异地灾难备份中心未配备恢复所需的运行环境，未处于就绪状态或运行状态
剩余信息保护	[关键]a)应保证操作系统、数据库系统和应用系统用户鉴别信息所在的存储空间被释放或重新分配前得到完全清除，无论这些信息是存放在硬盘上还是内存中。（F3）	保证操作系统、数据库系统和应用系统用户鉴别信息所在的存储空间被释放或重新分配前得到完全清除，无论这些信息是存放在硬盘上还是内存中。	1)应核查操作系统、数据库系统和应用系统用户鉴别信息所在的存储空间被释放或重新分配前是否得到完全清除，	此项不适合，该项要求一般在服务器、数据库和应用系统上实现	此项不适合，该项要求一般在服务器、数据库和应用系统上实现
剩余信息保护	[关键]b)应保证操作系统、数据库系统和应用系统用户存有敏感数据的存储空间被释放或重新分配前得到完全清除，无论这些信息是存放在硬盘上还是内存中。（F3）	保证操作系统、数据库系统和应用系统用户存有敏感数据的存储空间被释放或重新分配前得到完全清除，无论这些信息是存放在硬盘上还是内存中。	1)应核查操作系统、数据库系统和应用系统用户存有敏感数据的存储空间被释放或重新分配前是否得到完全清除，	此项不适合，该项要求一般在服务器、数据库和应用系统上实现	此项不适合，该项要求一般在服务器、数据库和应用系统上实现
个人信息保护	[关键]a)金融机构在收集、使用个人金融信息时，应遵循合法、正当、必要的原则，应以隐私政策等 方式公开收集、使用规则，向个人金融信息主体明示收集、使用信息的目的、方式和范围， 并获得个人信息主体的同意。（F3）	金融机构在收集、使用个人金融信息时，遵循合法、正当、必要的原则，应以隐私政策等 方式公开收集、使用规则，向个人金融信息主体明示收集、使用信息的目的、方式和范围， 并获得个人信息主体的同意。	1)应核查在收集、使用个人金融信息时，是否遵循合法、正当、必要的原则，是否以隐私政策等 方式公开收集、使用规则，向个人金融信息主体明示收集、使用信息的目的、方式和范围， 并获得个人信息主体的同意	此项不适合，该项要求一般在数据库和应用系统上实现	此项不适合，该项要求一般在数据库和应用系统上实现
个人信息保护	[关键]b)应仅采集和保存业务必需的用户个人金融信息。（F3）	仅采集和保存业务必需的用户个人金融信息。	1)应核查是否仅采集和保存业务必需的用户个人金融信息。	此项不适合，该项要求一般在数据库和应用系统上实现	此项不适合，该项要求一般在数据库和应用系统上实现
个人信息保护	[关键]c)应根据“业务需要”和“最小权限”原则，进行个人金融信息相关权限管理，严格控制和分 配相关操作权限，应禁止未授权访问和非法使用用户个人金融信息。（F3）	根据“业务需要”和“最小权限”原则，进行个人金融信息相关权限管理，严格控制和分 配相关操作权限，应禁止未授权访问和非法使用用户个人金融信息。	1)应核查是否根据“业务需要”和“最小权限”原则，进行个人金融信息相关权限管理，	此项不适合，该项要求一般在数据库和应用系统上实现	此项不适合，该项要求一般在数据库和应用系统上实现
个人信息保护	[关键]d)金融机构应依据 JR/T 0171—2020 对个人金融信息收集、传输、存储、使用、删除、销毁等 处理的整个过程进行管理与控制，并对个人金融信息生命周期过程进行安全检查与评估。（F3）	金融机构应依据 JR/T 0171—2020 对个人金融信息收集、传输、存储、使用、删除、销毁等 处理的整个过程进行管理与控制，并对个人金融信息生命周期过程进行安全检查与评估。	1)应核查是否依据 JR/T 0171—2020 对个人金融信息收集、传输、存储、使用、删除、销毁等 处理的整个过程进行管理与控制，	此项不适合，该项要求一般在数据库和应用系统上实现	此项不适合，该项要求一般在数据库和应用系统上实现

个人信息保护	[关键]e)金融机构应依据国家与行业主管部门要求，对通过计算机屏幕、客户端软件、银行卡受理设 备、ATM 设备、自助终端设备、纸（如受理终端打印出的支付交易凭条等交易凭证）等界面 展示的个人金融信息，应采取字段屏蔽（或截词）等处理措施，降低个人金融信息在展示环节的泄露风险。（F3）	金融机构依据国家与行业主管部门要求，对通过计算机屏幕、客户端软件、银行卡受理设 备、ATM 设备、自助终端设备、纸（如受理终端打印出的支付交易凭条等交易凭证）等界面 展示的个人金融信息，应采取字段屏蔽（或截词）等处理措施，降低个人金融信息在展示环 节的泄露风险。	1)应核查是否依据国家与行业主管部门要求，对通过计算机屏幕、客户端软件、银行卡受理设 备、ATM 设备、自助终端设备、纸（如受理终端打印出的支付交易凭条等交易凭证）等界面 展示的个人金融信息，采取字段屏蔽（或截词）等处理措施，	此项不适合，该项要求一般在数据库和应用系统上实现	此项不适合，该项要求一般在数据库和应用系统上实现
个人信息保护	[关键]f)应向个人金融信息主体告知共享、转让个人金融信息的目的、数据接收方的身份和数据安全 保护能力，并事先征得个人金融信息主体明示同意，共享、转让经去标识化处理的个人金融 信息，且确保数据接收方无法重新识别个人金融信息主体的除外。（F3）	向个人金融信息主体告知共享、转让个人金融信息的目的、数据接收方的身份和数据安全 保护能力，并事先征得个人金融信息主体明示同意，共享、转让经去标识化处理的个人金融 信息，且确保数据接收方无法重新识别个人金融信息主体的除外。	1)应核查是否向个人金融信息主体告知共享、转让个人金融信息的目的、数据接收方的身份和数据安全 保护能力，	此项不适合，该项要求一般在数据库和应用系统上实现	此项不适合，该项要求一般在数据库和应用系统上实现
个人信息保护	[关键]g)开发环境、测试环境不应使用真实的个人金融信息，应使用虚构的或经过去标识化处理的个 人金融信息，账号、卡号、协议号、支付指令等测试确需除外。（F3）	开发环境、测试环境不应使用真实的个人金融信息，应使用虚构的或经过去标识化处理的个 人金融信息，账号、卡号、协议号、支付指令等测试确需除外。	1)应核查开发环境、测试环境是否使用真实的个人金融信息，是否使用虚构的或经过去标识化处理的个 人金融信息，账号、卡号、协议号、支付指令等测试确需除外。	此项不适合，该项要求一般在数据库和应用系统上实现	此项不适合，该项要求一般在数据库和应用系统上实现

安全计算环境-服务器-操作系统（S3A3G3）作业指导书					
安全控制点	检测项	要求解读	测评方法	预期结果或主要证据	符合情况

身份鉴别	[关键]a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，应实现身份鉴别信息防窃取和防重用。静态口令应在8位以上，由字母、数字、符号等混合组成并每半年更换口令，不允许新设定的口令与前次旧口令相同。应用系统用户口令应在满足口令复杂度要求的基础上定期更换。（F3）	Linux系统的用户鉴别过程与其他UNIX系统相同：系统管理员为用户建立一个账户并为其指定一个口令,用户使用指定的口令登录后重新配置自己的自己的口令，这样用户就具备一个私有口令。etc/password文件中记录用户的属性信息，包括用户名、密码、用户标识、组标识等信息。现在Linux系统中不再直接保存在/etc/password文件中,通常将password文件中的口令字段使用一个“x”来代替，将/etc/shadow作为真正的口令文件，用于保存包括个人口令在内的数据。当然，shadow文件是不能被普通用户读取的，只有超级用户才有权读取。
		Linux中的/etc/login.defs是登录程序的配置文件，在这里我们可配置密码的最大过期天数，密码的最大长度约束等内容。如果/etc/pam.d/system-auth文件里有相同的选项，则以/etc/pam.d/system-auth里的设置为准，也就是说/etc/pam.d/system-aut的配置优先级高于/etc/login.defs。
		Linux系统具有调用PAM的应用程度认证用户。登示服务、屏保等功能，其中一个重要的文件使是etc/pam.d/system-auth 。 /etc/pam.d/system-auth 或/etc/login.defs中的配置优先级高于其他地方的配置
			1)访谈系统管理员系统用户是否已设置密码，并查看登录过程中系统账户是否使用了密码进行验证登录。
			2)以有权限的账户身份登录操作系统后，使用命令more查看/etc/shadow文件，核查系统是否存在空口令账户
			3)使用命令more查看/etc/login. defs文件，查看是否设置密码长度和定期更换要求
			#more /etc/login. defs
			使用命令more查看/etc/pam.d/system-auth文件。查看密码长度和复杂度要求
			4)检查是否存在旁路或身份鉴别措施可绕过的安全风险
			5)访谈前一次口令与当前使用口令是否相同
				1)登录需要密码
				2)不存在空口令账户
				3)得出类似反馈信息，如下:
				PASS MAX_DAYS 90 #登录密码有效期90天
				PASS MIN_DAYS 0 #登录密码最短修改时间，增加可以防止非法用户短期更改多次
				PASS MIN_LEN 7 #登录密码最小长度7位
				PASS WARN_AGE 7 #登录密码过期提前7天提示修改
				retry=3 ucredit=-1 lcredit=-1 dcredit=-2 ocredit=-1;
				4)不存在绕过的安全风险
				5)新设定口令与前一次口令不相同
					符合情况：仅可通过账户名加口令的方式进行登录，不存在空口令和弱口令账户，并已设置口令复杂度要求，且当前口令符合口令复杂度要求，并定期更换口令，新设定口令与前一次口令不同
					部分符合情况：通过账户名加口令的方式进行登录，不存在空口令和弱口令账户，但未设置口令复杂度要求，或口令未定期更换，或新口令与前次旧口令相同
					不符合情况：存在空口令或弱口令账户、可绕过身份鉴别措施进行登录

身份鉴别	[关键]b)应具有登录失败处理功能，应配置并启用结束会话、限制登录间隔、限制非法登录次数和当登录连接超时自动退出等相关措施。（F3）	Linux系统具有调用PAM的应用程度认证用户、登录服务、屏保等功能，其中一个重要的文件便/etc/pam.d/system-auth ，centos5以后版本使用pam_tally2.so模块控制用户密码认证失败的次数上限，可以实现登录次数、超时时间，解锁时间等。着只是针对某个程序的认证规则，在PAM目录(/etc/pam d)下形如sshd、login等等的对应各程序的认证规则文件中进行修改。若所有密码认证均应用规则，可直接修改system_auth文件	1)系统配置并启用了登录失败处理功能 2)以root身份登录进入Linux，查看文件内容: # cat /ete/pam.d/system -auth或根据linux版本不同在common文件中 3)查看/etc/profile中的TIMEOUT环境变量，是否配置超时锁定参数	得出类似反馈信息，如下: 1)和2)查看登录失败处理功能相关参数，/etc/pam.d/system—auth文件中存在"account required /lib/security/pam_tally.so deny=3 no_ magic root reset"; 3)记录在文件/etc/profile中设置了超时锁定参数，在profile下设置TMOUT= 300s	符合情况：已配置登录失败处理功能相关参数，且设置登录超时锁定参数 部分符合情况：已配置登录失败处理功能相关参数，但未设置登录超时锁定参数，或未配置登录失败处理功能相关参数，但已设置登录超时锁定参数 不符合情况：未配置登录失败处理功能参数，未设置登录超

身份鉴别	[关键]c)当进行远程管理时，应对管理终端进行身份标识和鉴别，采用密码技术防止鉴别信息在网络 传输过程中被窃听。（F3）	Linux提供了远程访问与管理的接口，以方便管理员进行管理操作，网络登录的方式也是多样的，例如可以使用Telnet登录，也可以使用SSH登录。但是，Telnet不安全。I因为其在教据传输过程中，账户与密码均明文传输，这是非常危险的。黑客通过一些网络对嗅探工是能够轻易地的窃取网络中明文传输的账户与密码，因此不建议通过Telnet协议对服务器进行远程管理。针对Telnet协议不安全这种情况，可以在远程登录时使用SSH协议。其原理跟Telnet类似，只是其具有更高的安全性。SSH是一个运行在传输控制层上的应用程序，与Telnet相比，它提供了强大的认证与加密功能，可以保证在远程连接过程中，其传输的数据是加密处理过的。因此保障了账户与口令的安全	访谈系统管理员，进行远程管理的方式。 1)以root身份登录进入Linux查看是否运行了sshd服务，service - status-all | grep sshd 查看相关的端口是否打开，netstat -an|grep 22 若未使用SSH方式进行远程管理，则查看是否使用了Telnet 方式进行远程管理 service - -status-all|grep running, 查看是否存在Telnet服务 2)可使用wireshark等抓包工具，查看协议是否为加密	1)使用SSH方式进行远程管理，防止鉴别信息在传输过程中被窃听,Telnet默认不符合 2)通过抓包工具，截获信息为密文，无法读取，协议为加密 3) N/A本地管理	符合情况：采用SSH方式进行远程管理，且已关闭Telnet服务 部分符合情况：采用SSH方式进行远程管理，但未关闭Telnet 不符合情况：采用Telnet进行远程管理，或采用未进行加密处理的远程管理方式
身份鉴别	[关键]d)应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	对于第三级及以上的操作系统要求采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现	访谈和核查系统管理员在登录操作系统的过程中使用了哪些身份鉴别方法，是否采用了两种或两种以上组合的鉴别技术，如口令教字证书Ukey、令牌、指纹等，是否有一种鉴别方法在鉴别过程中使用了密码技术	除口令之外，采用了另外一种鉴别机制，此机制采用了密码技术，如调用了密码机或采取SM1-SM4等算法	符合情况：采用两种或两种以上组合的鉴别技术，且其中一种鉴别技术在鉴别过程中使用了密码技术 部分符合情况：采用两种或两种以上的鉴别技术，但非密码技术 不符合情况：未采用两种或两种以上组合的鉴别技术
访问控制	[重要]a)应对登录的用户分配账户和权限。	对于Linux中一些重要的文件，应检查Linux系统主要目录的权限设置情况，Linux系统对文件的操作权限，包括4种:读(r,4)；写(w,2)；执行(x,1)；空(一，0)，文件的权限分为属主(拥有者)、属组、其它用户和用户组的权限	以有相应权限的身份登录进入Linux,使用“1s-1文件名”命令，查看重要文件和目录权限设置是否合理，如: # 1s -1 /etc/passwd #744。	重点查看以下文件和目录权限是否设置合理。 —rwx- - - - -:数字表示为700 -rwxr--r- -:数字表示为744 -rw-rw-r-x:数字表示为665 drwx-x一x:数字表示为711 drwr- - - -:数字表示为700 配置文件权限值不能大于644，对于可执行文件不能大于755	符合情况：重要文件和目录权限设置合理 部分符合情况：重要文件和目录权限设置未完全合理设置，部分文件和目录权限设置不合理 不符合情况：未对登录的用户分配账户和权限
访问控制	[关键]b)应重命名或删除默认账户，修改默认账户或预设账户的默认口令。（F3）	Linux操作系统本身安装后提供各种账号，如adm Ip sync shutdown halt mail uucp operator games gopher ftp等，但这些账户使用时并不需要，有的帐号越多，就越容易受到攻击，应禁用或者删除这些用户。 root作为重要的默认账户，一般要求禁止远程登录	1)以有相应权限的身份登录进入Linux,使用more查看/etc/shadow文件，查看文件中的用户，是否存在adm、 lp. sync、 shutdown、 halt.、mail、 uucp、 operator,、 games.、gopher ftp等默认的、无用的用户。 2)查看root账户是否能够进行远程登录	1)不存在默认无用的账户 2) 使用more查看/etc/ssh/sshd_config文件中的"PermitRootLogin"参数设置为“no“，即: PermitRootLogin no, 即不许可root远程登录	符合情况：不存在默认的、无用的可登录账户，且已禁止root用户远程登录 部分符合情况：存在默认账户，但已修改默认账户口令 不符合情况：存在默认账户，且默认账户口令也未修改
访问控制	[关键]c)应用系统应对首次登录的用户提示修改默认账户或预设账户的默认口令。（F3）	应用系统应对首次登录的用户提示修改默认账户或预设账户的默认口令。	此项不适合，该项要求一般在应用系统上实现	此项不适合，该项要求一般在应用系统上实现	此项不适合，该项要求一般在应用系统上实现
访问控制	[重要]d)应及时删除或停用多余的、过期的账户，避免共享账户的存在。	通常操作系统在运行一段时间后，因业务应用或管理员岗位的调整，出现一些多余的、过期的账户；另一方面，也会出现多个系统管理员或用户使用同一账户登录操作系统的情况，造成审计追踪时无法定位到自然人。如果存在多余的，过期的账户，可能会被攻击者利用其进行非法操作的风险，因此应及时清理系统中的账户，删除或停用多余的、过期的账户，同时避免共享账户的存在	1)应核查是否不存在多余或过期账户，如查看games、news、 ftp、 1p等系统默认账户是否被禁用，特权账号halt、shutdown是否被删除 2)应访谈网络管理员、安全管理员、系统管理员不同用户是否采用不同账户登录系统	1)禁用或删除不需要的系统默认账户，如games、news、 ftp、 1p、halt、shutdown等 2)各类管理员均使用自己分配的特定权限账户登录，不存在多余、过期账户	符合情况：无多余或过期账户，各类管理员均使用自己分配的特定权限账户登录，不存在共享账户的情况 部分符合情况：无多余或过期账户，但存在共享账户的情况 不符合情况：存在多余或过期账户

访问控制	[一般]e)应授予管理用户所需的最小权限，实现管理用户的权限分离。	根据管理用户的角色对权限进行细致的划分，有利于各岗位细致协调工作，同时仅授予管理用户所需的最小权限，避免出现权限的漏洞使得一些高级用户拥有过大的权限。Linux 系统安装后，root拥有所有权限，使用sudo授予普通用户root级权限，在sudoer.conf中进行配置	1)以有相应权限的身份登录进入Linux，使用more查看/etc/passwd文件中的非默认用户，询问各账户的权限，是否实现管理用户的权限分离 2)以有相应权限的身份登录进入Linux，使用more查看/etc/sudo.conf文件，核查root级用户的权限都授予哪些账户	1)各用户均具备最小权限,不与其他用户权限交叉。设备下可支持新建多用户角色功能 2)管理员权限仅分配root用户	符合情况：已对各不同权限的用户创建不同的账户，如安全管理员、审计管理员、系统管理员，且采用权限分配最小化原则对管理用户进行权限分配 部分符合情况：已对各不同权限的用户创建不同的账户，但各用户权限限分配不合理 不符合情况：未对不同权限的用户进行权限分离，仅采用超级管理员账户进行管理
访问控制	[关键]f)应严格限制默认账户或预设账户的权限，如默认账户和预设账户的权限应为空权限或某单一 功能专用权限等。（F3）	严格限制默认账户或预设账户的权限，如默认账户和预设账户的权限应为空权限或某单一 功能专用权限等。	1)应核查限制默认账户或预设账户的权限分配和限制措施	默认账户或预设账户为空权限或单一专用权限，不与其他用户权限交叉	符合情况：已对默认账户或预设账户的使用进行限制，并划分专用权限 不符合情况：对默认账户或预设账户的使用未进行限制，并且账户权限未进行划分
访问控制	[一般]g)应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。	操作系统的访问控制策略应由授权主体（如安全管理员）进行配置，非授权主体不得更改访问控制策略。访问控制策略规定操作系统用户对操作系统资源(如文件和目录)具有哪些权限，能进行哪些操作、通过在操作系统中配置访问控制策略，实现对操作系统各用户权限的限制	1)应核查是否由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。	1)由专门的安全员负责对访问控制权限的授权工作 2)各账户权限配置，均是基于安全员的安全策略配置进行的访问控制	符合情况：已指定授权主体（一般为安全管理员）对操作系统访问控制权限进行配置 部分符合情况：已指定专门的安全员负责对访问控制权限的授权工作，但安全策略配置不合理 不符合情况：未指定授权主体对操作系统访问控制权限进行配置
访问控制	[一般]h)访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级。	明确提出访问控制的粒度要求，重点目录的访问控制的主体可能为某个用户或某个进程，应能够控制用户或进程对文件、数据库表等客体的访问	1)应核查访问控制的粒度是否达到主体为用户级或进程级，客体为文件、数据库表级。	由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件和数据库表级进行访问。重要文件和目录权限均在合理范围内，用户可根据对文件不同的权限进行操作	符合情况：由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件和数据库表级进行访问，对于访问控制的粒度达到主体为用户级或进程级，客体为文件级、数据库表级 部分符合情况：由管理用户进行用户访问权限分配进行设置，依据访问控制策略,对各类文件和数据库表级进行访问，但访问控制的粒度未完全达到要求，部分文件或目录权限设置不合理 不符合情况：访问控制的粒度未达到主体为用户级或进程级，客体为文件、数据库表级

访问控制	[一般]i)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	敏感标记是由强认证为安全管理员进行设置的，通过对重要信息资源设置敏感标记，决定主体以何种权限对客体进行操作，实现强制访问控制。安全增强型Linux (Security Enhanced Linux)简称SELinux,是一个Linux内核模块，也是Linux的一个安全子系统。2.6及以上版本的Linux内被都团经集成了SELinux模块，在使用SELinux的操作系统中，决定一个资源是否能够被访问的因素除了用户的权限(读、写、执行)外，还需要判断每一类进程是否拥有对某一类资源的访问权限，这种权限管理机制的主体是进程，也称为强制访问控制(MAC)。在SELinux中，主体等同于进程，客体是主体访问的资源，可以是文件、目录、端口、设备等	1)应核查是否对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	1) 2) 3)4) linux服务器默认关闭SELinux服务。或采取第三方主机加固系统或对操作系统内核进行二次开发加固，并实际查看系统可视化界面。 SELINUX有三种工作模式，分别是: enforcing:强制模式。违反SELinux规则的行为将阻止并记录到日志中，表示使用SELinux。 permissive:宽容模式。违反SELinux规则的行为只会记录到日志中，一般为调试用，表示使用SELinux disabled:关闭SELinux,使用SELinux	符合情况：已对重要主体或客体设置安全标记，且已控制主体对有安全标记信息资源的访问 部分符合情况：已配置安全标记，但安全标记配置不合理等 不符合情况：未对重要主体或客体设置安全标记
安全审计	[重要]a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。	centos5以后都开始使用LASU (Linux Aduit Subsystem)来进行审计。且志系统可以记录系统的各种信息,如:安全、调试、运行信息。审计子系统专用来记录安全信息，用于对系统安全事件的追溯。如果审计子系统没有运行，Linux内核就将安全审计信息传递给日志系统。 Linux操作系统的auditd进程主要用来记录安全信息。用于对系统安全事件的追溯；而rsyslog进程用来记录系统中的各种信息，如硬件报警和软件日志。 Linux操作系统在安全审计配置文件/etc/audit/audit.rules中配置安全事件审计规则	1)以root身份登录进入Linux,查看服务进程 2)若运行了安全审计服务，则查看安全审计的守护进程是否正常 # ps -ef|grep auditd 3)若未开启系统安全审计功能，则确认是否部署了第三方安全审计工具 4)以root身份登录进入Linux查看安全事件配置：#gerep “@priv-ops" /etc/audit/filter.conf .... more/etc/audit/audit.rules	1)开启审计进程内容如下: [root@localhost april]# service auditd status auditd (pid 1656) is running... [root@localhost april]# service rsyslog statusr syslogd (pid 1681) is running... [root@localhost april]# 2)Linux服务器默认开启守护进程 3)audit.rules中记录对文件和底层调用的相关记录，记录的安全事件较为全面	符合情况：已开启安全审计功能，且审计覆盖到每个用户 部分符合情况：已开启安全审计功能，但审计未覆盖到所有用户 不符合情况：未开启安全审计功能
安全审计	[一般]b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	详细的审计记录才能实现有效的审计，审计记录应该包括事件的日期、时间、类型、主体标识、客体标识和结果等。通过记录中的详细信息，能够帮助管理员或其他相关检查人员准确的分析和定位事件。Linux用户空间审计系统由auditd、ausearch和aureport等应用程序组成，其中ausearch是查找审计事件的工具，可以用来查看系统日志	以有相应权限的身份登录进入Linux,使用命令"ausearch-ts today”，其中，-ts指定时间后的log,或命令"tail -20 /var/log/audit/audit.log“查看审计日志	审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果	符合情况：审计记录包括事件的日期和时间，用户、事件类型，事件是否成功及其他与审计相关的信息 部分符合情况：审计记录不全、记录信息不够详细 不符合情况：未开启审计功能，无审计记录
安全审计	[关键]c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等，审计记录保存 时间应不少于6个月。（F3）	非法用户进入系统后的第一件事情就是去清理系统日志和审计日志，而发现入侵的最简单最直接的方法就是去看系统记录和安全审计文件。因此，必须对审计记录进行安全保护，避免受到未预期的删除修改或覆盖等。	访谈审计记录的存储、备份和保护的措施，是否将操作系统日志定时发送到日志服务器上等，并使用sylog方式或smp方式将日志发送到日志服务器。 如果部署了日志服务器,登录日志服务器查看操作系统的日志是否在收集的范围内	操作系统日志定期备份，共定期将本地存储日志转发至日志服务器，并且日志记录保存不少于6个月	符合情况：已对审计记录进行保护，无法进行删除、修改或覆盖，且定期备份，定期将本地存储日志转发至日志服务器，且保存时间大于6个月 部分符合情况：无 不符合情况：未对审计记录进行保护、保存时间未达到6个月

安全审计	[一般]d)应对审计进程进行保护，防止未经授权的中断。	保护好审计进程，当安全事件发生时能够及时记录事件发生的详细内容。 在Linux中,Auditd是审计守护进程, syslogd是日志守护进程,保护好审计进程，当事件发生时，能够及时记录事件发生的详细内容。	1)访谈对审计进程监控和保护的措施 2)测试使用非安全审计员中断审计进程，查看审计进程的访问权限是否设置合理。 3)查看是否有第三方系统对被测操作系统的审计进程进行监控和保护	1）2）审计进程不可以非审计人员权限修改 3）部署有第三方审计工具，可实时记录审计日志，管理员不可对日志进行删除	符合情况：已通过第三方系统对审计进行进行监控和保护，审计进程无法进行未授权的中断，管理员不可对日志进行删除 部分符合情况：无 不符合情况：未对审计进行进行保护，非授权人员可中断审计进程，可随意对审计日志进行更改、删除等操作
安全审计	[关键]e)对于从互联网客户端登录的应用系统，应在用户登录时提供用户上一次非常用设备成功登录 的日期、时间、方法、位置等信息。（F3）	对于从互联网客户端登录的应用系统，在用户登录时提供用户上一次非常用设备成功登录 的日期、时间、方法、位置等信息。	此项不适合，该项要求一般在应用层面上核查	此项不适合，该项要求一般在应用层面上核查	此项不适合，该项要求一般在应用层面上核查
安全审计	[关键]f)审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的一致性与正 确性。（F3）	审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的一致性与正 确性。	1)应核查系统是否部署时钟同步服务器。	部署时钟同步的ntp服务器，审计记录产生的时间与系统范围内唯一确定的时钟产生的时间一致	符合情况：已部署ntp服务器，并且审计记录产生的时间与系统范围内唯一确定的时钟产生的时间一致 部分情况：无 不符合情况：未部署时钟同步的ntp服务器，审计记录时间无法对应
入侵防范	[重要]a)应遵循最小安装的原则，仅安装需要的组件和应用程序。	在安装Linux操件系统时，应试循最小化安装原则，即不需要的包不进行安装。安装的包越多，面临的风险起大，系统瘦身有利于提高系统的安全性。在操作系统使用过程中，为了避象由于多余组件和应用程序带来的安全风险，通常遵循最小安装原则，仅安装需要的组件和应用程序	1)访谈安装系统时是否遵循最小化安装原则，查看安装操作手册 2)使用命令“yum list installed" 查看操作系统中已安装的程序包，询问是否有目前不需要的组件和应用程序	1)系统安装遵循最小化安装原则 2)不存在业务所不需要的组件和应用程序	符合情况：系统安装遵循最小化安装原则，且不存在业务所不需要的组件和应用程序 部分符合情况：无 不符合情况：未遵循最小化安装原则，存在多余的组件或应用程序
入侵防范	[关键]b)应关闭不需要的系统服务、默认共享和高危端口。	Linux默认安装时会开启许多不必要的系统服务，为了避免由于多余的系统服务带来安全风险，通常可以将其关闭。通过查看监听端口，能够直观地发现并对比系统所运行的服务和程序,关闭高危端口,是操作系统常用的安全加固方式	1)以有相应权限的身份登录进入Linux, 使用命令"service - status-all| grep running" 查看是否已经关闭危险的网络服务 2)以有相应权限的身份登录进入Linux,使用命令"netstat -ntlp” 查看并确认是否开放的端口都为业务需要端口， 是否已经关闭非必需的端口,Linux不存在共享问题	1)关闭了系统多余服务，危险服务和进程 2)关闭了多余端口	符合情况：已关闭系统多余服务、危险服务和进程，已关闭多余端口，不存在系统默认共享 部分符合情况：已关闭系统多余服务、危险服务和进程，已关闭多余端口，但存在系统默认共享 不符合情况：存在系统多余服务、危险服务和进程、未关闭多余端口、存在系统默认共享
入侵防范	[重要]c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。	在Linux系统中存在/etc/hosts.allowr和/etc/hosts.deny两个文件,它们是tcpd服务器的配置文件，tcpd服务器可以控制外部IP对本机服务的访问。其中/etc/hosts.allow控制可以访问本机的IP地址，/ete/hosts.deny控制禁止访问本机的IP,如果两个文件的配置有冲突，以/etc/hosts. deny为准	查看在/etc/hosts.deny中是否有“ALL: ALL", 禁止所有的请求:在/etc/hosts.allow中，是否有如下配置(举例): sshd: 192.168.1.10/255. 255. 255. 0 2)是否采用了从防火墙设置了对接入终端的限制	1)使用more查看/etc/hosts.allow中是否有如下配置限制IP及其访问方式，如(举例): ssbd; 192. 168. 1.10/255.255 255.0 2)对终端接入方式，网络地址范围等条件进行限制。通过RADUS.、堡垒主机、安全城、防火墙等运维方式实现对终端入方式的限制	符合情况：已通过防火墙或其他安全设备对接入终端进行限制，如指定特定ip或对网络地址范围进行限制等 部分符合情况：通过网路地址范围对终端接入方式进行限制，但地址范围过大 不符合情况：未对终端接入方式进行限制

入侵防范	[关键]d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。	本条款要求应用系统应对数据的有效性进行验证，主要验证那些通过人机接口(如程序的界面)输入或通过通信接口输入的数据格式或长度是否符合系统设定要求，防止个别用户输入畸形数据而导致系统出错(如SQL 注入攻击等),人而影响系统的正常使用甚至危害系统的安全	此项不适合，该项要求一般在应用层面上核查	此项不适合，该项要求一般在应用层面上核查	此项不适合，该项要求一般在应用层面上核查
入侵防范	[关键]e)应能通过使用漏洞扫描工具、人工漏洞排查分析等漏洞检查手段，及时发现可能存在的已知 漏洞，并在经过充分测试评估后，及时修补漏洞。（F3）	攻击者可能利用操作系统存在的安全漏洞对系统进行攻击，应对系统进行漏洞扫描，及时发现系统中存在的已知漏洞，并在经过充分测试评估后更新系统补丁，避免遭受由系统漏洞带的风险	1)查看甲方自查的洞扫报告或通过第三方检查的漏洞报告，有无高风险漏洞 2)系统有无漏洞测试环境，补丁更新的机制和流程加何? 3)访谈补丁升级机制，查看补丁安装情况：#rpm -qa grep patch	1有运维团队定期进行漏洞扫描和人工漏洞排查计划，发现安全风险，及时补修 2)3）更断补丁时间为最近，对补丁进行控制和管理	符合情况：有定期漏洞排查分析进行漏洞扫描和人工，及时发现安全风险，并根据扫描结果及时对安全问题进行修补 部分符合情况：定期进行漏洞扫描和人工排查分析，但未及时修补漏洞 不符合情况：未定期进行漏洞扫描和人工漏洞排查
入侵防范	[重要]f)应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。	要维护真正安全的环境，只具备安全系统还远远不够。如果假设自己不会受到攻击，或认为防护措施已足以保护自己的安全，都是非常危险的。要维护系统安全，必须进行主动监视，以检查是否发生了入侵和攻击。 一般意义上，入侵威胁分为外部渗透、内部渗透和不法行为三种，入侵行为分为物理入侵、系统入侵和远程入侵三种。此项中，关注的操作系统所面对的入侵成胁可能包含了三种造成入侵威胁的入侵行为主要是系统入侵和远程入侵两种。系统入侵，指入侵者在拥有系统的一个低级账号权限下进行的破坏活动。通常，如果系统没有及时更新最近的补丁程序，那么拥有低级权限的用户就可能利用系统漏洞获取更高的管理特权。远程入侵，指入侵者通过网络渗透到一个系统中。这种情况下，入侵者通常不具备任何特殊权限，他们通过漏洞扫扫描端口扫描等技术发现攻击目标，再利用相关技术执行破坏活动	1)访谈并查看入侵检测的措施，如经常通过如下命令查看入侵的重要线索(试图Telnet.FTP等),涉及命令“#more /var/log /secure|grep refused" 2)查看是否启用了主机防火墙、TCP SYN保护机制等设置 3)访谈系统管理员是否安装了主机入侵检测软件。查看已安装的主机入侵，检查系统的配置情况，是否具备报警功能。可执行命令: find / -namie <daemonname> -print 检查是否安装了主机入侵检测软件，如Dragon Squire by Enterasys Networks，ITA by Symantec. Hostsentry by Psionic Software.Logcheck by Psiomc Software. RealSecure-agent by ISS 4)查看网络拓扑图，查看网络上是否部署了网络入侵检测系统，如IDS	1）入侵的重要路径均deny 2)开启主机防火墙相关置 3)安装有基于主机的IDS设备 4)若主机未部署主机IDS设备。可在网络链路上查香是否是IDS、IPS. 发生入侵事件时，记录报警措施等	符合情况：具备入侵检测的措施，可以检测到对重要节点进行入侵的行为，并进行报警 部分符合情况：具备入侵检测的措施，可以检测到对重要节点进行入侵的行为，但不具备报警功能 不符合情况：无入侵检测措施，无法检测到对重要节点进行入侵的行为
入侵防范	[关键]g)所有安全计算环境设备应全部专用化，生产设备不得进行与业务不相关的操作。（F3）	所有安全计算环境设备全部专用化，生产设备不得进行与业务不相关的操作。	1)应核查设备是否全部专用化，	当前设备统一由安全部门部署搭建，仅相关管理员拥有设备账户进行运维管理，并且无法进行与业务不相关的操作	符合情况：所有安全计算环境设备全部专用化，生产设备不得进行与业务不相关的操作 不符合情况：未对安全计算环境设备的使用进行限制，可以进行与业务不相关的操作。
入侵防范	[关键]h)应能够有效屏蔽系统技术错误信息，不得将系统产生的错误信息直接或间接反馈到前台界面。（F3）	能够有效屏蔽系统技术错误信息，不得将系统产生的错误信息直接或间接反馈到前台界面。	此项不适合，该项要求一般在应用层面上核查	此项不适合，该项要求一般在应用层面上核查	此项不适合，该项要求一般在应用层面上核查

恶意代码防范	[关键]a)应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断并定期统一进行升级和更新防恶意代码库。（F3）	作为Linux系统，也面临着木马和蠕虫的破坏，可以采用免受恶意代码攻击的技术措施或主动免疫可信验证机制对恶意代码进行检测	1)核查操作系统中安装了什么防病毒软件，访谈管理员病毒库是否经常更新，核查病毒库最新版本，更新日期是否超过一个星期 2)核查操作系统是否实现了可信验证机制，能够对系统程序、应用程序和重要配置文件/参数进行可信执行验途	1)部署有网络版防病毒软件，病毒库最新，支持防恶意代码的统-管理个 2)部署有主动免疫可信验证机制，可对病贵入侵进行及时阻断	符合情况：系统中已安装部署防病毒软件，可对病毒入侵进行及时阻断，且病毒库已更新到最新 部分符合情况：系统中已安装部署防病毒软件，可对病毒入侵进行及时阻断，但病毒库未及时更新 不符合情况：未安装任何防病毒软件，未采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断
恶意代码防范	[关键]b)应建立病毒监控中心，对网络内计算机感染病毒的情况进行监控。（F3）	建立病毒监控中心，对网络内计算机感染病毒的情况进行监控。	1)应核查设备是否部署了支持统一管理的防恶意代码软件，	当前部署的防恶意代码软件拥有统一查看病毒信息的界面，方便对病毒攻击设备时的情况进行监控	符合情况：防恶意代码软件已建立病毒监控中心，对主机进行实时监控 不符合情况：防恶意代码软件未部署病毒监控中心，无法将防病毒攻击的信息做监控
可信验证	[一般]a)可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	针对服务器设备，需要服务器在启动过程对预装软件(包括系统引导程序、系统程序、相关应用程序和重要配置参数)进行完整性验证或检测，确保对系统引导程序、系统程序、重要配置参数和关键应用程序的篡改行为能被发现，并报警便于后续的处置动作	1)核查服务器的启动，是否实现可信验证的检测过程，查看对那些系统引导程序、系统程序或重要配置参数进行可信验证 2)修改其中的重要系统程序之一和应用程序之一，核查是否能够检测到并进行报警 3)是否将验证结果形成审计记录送至安全管理中心	1) 服务器具有可信根芯片或硬件 2)启动过程基于可信根对系统引导程序、系统程序，重要配置参数和关键应用程序等进行可信验证度量 3)在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心 4)安全管理中心可以接收设备的验证结果记录	符合情况：服务器具有可信根芯片或硬件，可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心 部分符合情况：具有可信根芯片或硬件，但未将验证结果形成审计记录送至安全管理中心 不符合情况：无可信根芯片或硬件
数据完整性	[重要]a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。	采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。	1)应核查设备涉及哪几种数据类型 2)涉及传输的数据采用什么方式保证数据的完整性	1） 系统提供对鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性保护措施 2） 系统检测到鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性受到被坏后采取了技术措施进行处	符合：设备通过SSH协议对传输过程中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息 部分符合：系统采取措施对传输中的数据进行完整性校验；仅包括鉴别数据 不符合：设备未采取措施对传输中的数据进行完整性校验；

数据完整性	[关键]b)应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。	采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。	1)应核查设备涉及哪几种数据类型 2)涉及存储的数据采用什么方式保证数据的完整性	1)系统采用校验技术或密码技术保证了鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性 2)系统可检测到存储在数据库中的鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等被修改的行为，并具备恢复措施	符合：设备通过SHA-512技术对存储中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息 部分符合：设备通过SHA-512技术对存储中的数据进行完整性校验；仅对鉴别数据，未包括业务数据和个人信息 不符合：设备未采取措施对存储中的数据进行完整性校验；
数据保密性	[关键]a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。	采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。	1)应核查设备涉及哪几种数据类型 2)涉及传输的数据采用什么方式保证数据的保密性	1)系统管理员采用密码技术对鉴别数据、重要业务数据和重要个人信息进行了保密性处理 2）通过嗅探等方式抓取传输过程中的数据，未发现鉴别数据、重要业务数据和重要个人信息	符合：设备通过SSH协议对传输过程中的数据进行加密；包括鉴别数据、业务数据和个人信息 部分符合：设备通过SSH协议对传输过程中的数据进行加密；包括鉴别数据，未对业务数据和个人信息 不符合：设备未采取措施对传输中的数据进行加密；
数据保密性	[关键]b)应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于系统鉴别数据、重要业务数据和个人金融信息中的客户鉴别信息以及与账号结合使用可鉴别用户身份的鉴别辅助 信息等个人敏感信息，对于其他直接反应特定自然人某些情况的信息，宜使用密码技术保护 其存储过程中的保密性。（F3）	采用密码技术保证重要数据在存储过程中的保密性，包括但不限于系统鉴别数据、重要业务数据和个人金融信息中的客户鉴别信息以及与账号结合使用可鉴别用户身份的鉴别辅助 信息等个人敏感信息，对于其他直接反应特定自然人某些情况的信息，宜使用密码技术保护 其存储过程中的保密性。	1)应核查设备涉及哪几种数据类型 2)涉及存储的数据采用什么方式保证数据的保密性	1)系统采用了密码技术对存储在数据库中的鉴别数据、重要业务数据和重要 2)数据库中存储的鉴别数据、重要业务数据和重要个人信息等均加密存储	符合：设备通过SHA-512对存储中的数据进行加密；包括鉴别数据、业务数据和个人信息 部分符合：设备通过SHA-512对存储中的数据进行加密；包括鉴别数据，未对业务数据和个人信息 不符合：设备未采取措施对存储中的数据进行加密；
数据备份恢复	[关键]a)应提供重要数据的本地数据备份与恢复功能，采取实时备份与异步备份或增量备份与完全备 份的方式，增量数据备份每天一次，完全数据备份可根据系统的业务连续性保障相关指（如 RPO，RTO）以及系统数据的重要程度、行业监管要求，制定备份策略。备份介质场外存放， 数据保存期限依照国家相关规定。（F3）	提供重要数据的本地数据备份与恢复功能，采取实时备份与异步备份或增量备份与完全备 份的方式，增量数据备份每天一次，完全数据备份可根据系统的业务连续性保障相关指（如 RPO，RTO）以及系统数据的重要程度、行业监管要求，制定备份策略。备份介质场外存放， 数据保存期限依照国家相关规定。	1)应核查设备的备份恢复策略	1)提供数据的每天全量备份《(或每天增量备份，定期全量备份) 2)近期数据库的恢复测试记录显示，能够使用备份文件进行数据恢复	符合：设备通过快照形式对数据进行备份，备份策略为每周2，4，6进行备份，备份保存7天，数据每天凌晨1：00全量备份； 部分符合：提供数据备份能力、未提供数据恢复功能。 不符合：未对设备配置数据进行备份；
数据备份恢复	[重要]b)应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地。	提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地。	1)应核查设备的数据异地备份策略	提供异地实时备份功能，并通过网络将重要配置数据、重要业务数据实时备份至备份场地	符合：设备每周对配置数据进行异地备份， 部分符合：无部分符合 不符合：未提供异地实施备份功能；
数据备份恢复	[关键]c)应提供重要数据处理系统的热冗余，保证系统的高可用性。	提供重要数据处理系统的热冗余，保证系统的高可用性。	1)应核查设备的部署方式，是否采用热冗余方式进行部署	1)对重要数据，如用户数据，鉴别数据等定期进行备份，通过磁带备份到本地 2)对于重要设备，采取热备、集群、负载均衡等高可用方式	符合情况：已提供重要数据处理系统的热冗余，如热备、集群、负载均衡等高可用方式 部分符合情况：无 不符合情况：未提供重要数据处理系统的热冗余

数据备份恢复	[关键]d)对于同城应用级灾难备份中心，应与生产中心直线距离至少达到30km，可以接管所有核心业 务的运行；对于异地应用级灾难备份中心，应与生产中心直线距离至少达到100km。（F3）	于同城应用级灾难备份中心，应与生产中心直线距离至少达到30km，可以接管所有核心业 务的运行；对于异地应用级灾难备份中心，应与生产中心直线距离至少达到100km。	1)应核查系统是否部署灾难备份中心，生产中心与灾备中心的直线距离是否满足要求。	系统提供异地实时备份功能，并且同城灾备机房与生产中心的直线距离达到30KM以上，异地灾备中心与生产中心直线距离达到100KM以上	符合情况：系统提供异地实时备份功能，并且异地灾备机房与生产中心的直线距离达到100KM以上 部分符合情况：无 不符合情况：同城灾备中心与生产中心直线记录未达到30KM以上，或者异地灾难备份中心，与生产中心直线距离未达到100km以上
数据备份恢复	[关键]e)为满足灾难恢复策略的要求，应对技术方案中关键技术应用的可行性进行验证测试，并记录 和保存验证测试结果。（F3）	为满足灾难恢复策略的要求，应对技术方案中关键技术应用的可行性进行验证测试，并记录 和保存验证测试结果。	1)应核查是否对关键技术应用的可行性进行验证测试。 2)核查是否具备验证测试记录	1)对备份数据定期进行验证测试 2)对进行的验证测试留有相应的测试记录	符合情况：定期每季度对备份数据进行一次验证测试，并每次验证测试留有测试记录 部分符合情况：定期每季度对备份数据进行一次验证测试，但是没有测试记录 不符合情况：未定期对备份数据进行验证测试
数据备份恢复	[关键]f)数据备份应至少保存两个副本，且至少一份副本异地存放，完全数据备份至少保证以一个星 期为周期的数据冗余。（F3）	数据备份应至少保存两个副本，且至少一份副本异地存放，完全数据备份至少保证以一个星 期为周期的数据冗余。	1)应核查数据备份是否至少保存两个副本，且至少一份副本异地存放， 2)核查是否具备数据备份记录	1)对备份的数据至少保存两个版本，其中一份异地存放 2)对备份数据提供备份记录	符合情况：当前数据备份保存有两个副本，存在异地和本地备份等多种方式，分别保存在主机房和灾备机房，并且留存有数据备份记录 部分符合情况：当前数据备份保存有两个副本，存在异地和本地备份等多种方式，分别保存在主机房和灾备机房，但是未保存数据备份记录 不符合情况：备份数据未采用多副本的方式存储
数据备份恢复	[关键]g)异地灾难备份中心应配备恢复所需的运行环境，并处于就绪状态或运行状态，“就绪状态” 指备份中心的所需资（相关软硬件以及数据等资源）已完全满足但设备CPU还没有运行，“运行状态”指备份中心除所需资源完全满足要求外，CPU也在运行状态。（F3）	异地灾难备份中心应配备恢复所需的运行环境，并处于就绪状态或运行状态，“就绪状态” 指备份中心的所需资（相关软硬件以及数据等资源）已完全满足但设备CPU还没有运行，“运行状态”指备份中心除所需资源完全满足要求外，CPU也在运行状态。	1)应核查异地灾难备份中心是否配备恢复所需的运行环境，是否处于就绪状态或运行状态，	异地灾难备份中心已配备恢复所需的运行环境，处于就绪状态或运行状态	符合情况：异地灾难备份中心已配备恢复所需的运行环境，处于就绪状态或运行状态 部分符合情况：无 不符合情况：异地灾难备份中心未配备恢复所需的运行环境
剩余信息保护	[关键]a)应保证操作系统、数据库系统和应用系统用户鉴别信息所在的存储空间被释放或重新分配前得到完全清除，无论这些信息是存放在硬盘上还是内存中。（F3）	保证操作系统、数据库系统和应用系统用户鉴别信息所在的存储空间被释放或重新分配前得到完全清除，无论这些信息是存放在硬盘上还是内存中。	1)应核查操作系统用户鉴别信息所在的存储空间被释放或重新分配前是否得到完全清除	服务器采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。	符合情况：采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除系统中的剩余信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等。 不符合情况：未对剩余信息进

剩余信息保护	[关键]b)应保证操作系统、数据库系统和应用系统用户存有敏感数据的存储空间被释放或重新分配前得到完全清除，无论这些信息是存放在硬盘上还是内存中。（F3）	保证操作系统、数据库系统和应用系统用户存有敏感数据的存储空间被释放或重新分配前得到完全清除，无论这些信息是存放在硬盘上还是内存中。	1)应核查操作系统用户存有敏感数据的存储空间被释放或重新分配前是否得到完全清除	服务器采取了措施保证对存储介质(如硬盘或内存）中的敏感数据进行及时清除	符合情况：采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除系统中的剩余信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等。 不符合情况：未对剩余信息进
个人信息保护	[关键]a)金融机构在收集、使用个人金融信息时，应遵循合法、正当、必要的原则，应以隐私政策等 方式公开收集、使用规则，向个人金融信息主体明示收集、使用信息的目的、方式和范围， 并获得个人信息主体的同意。（F3）	金融机构在收集、使用个人金融信息时，遵循合法、正当、必要的原则，应以隐私政策等 方式公开收集、使用规则，向个人金融信息主体明示收集、使用信息的目的、方式和范围， 并获得个人信息主体的同意。	此项不适合，该项要求一般在应用、数据库层面上核查	此项不适合，该项要求一般在应用、数据库层面上核查	此项不适合，该项要求一般在应用、数据库层面上核查
个人信息保护	[关键]b)应仅采集和保存业务必需的用户个人金融信息。（F3）	仅采集和保存业务必需的用户个人金融信息。	此项不适合，该项要求一般在应用、数据库层面上核查	此项不适合，该项要求一般在应用、数据库层面上核查	此项不适合，该项要求一般在应用、数据库层面上核查
个人信息保护	[关键]c)应根据“业务需要”和“最小权限”原则，进行个人金融信息相关权限管理，严格控制和分 配相关操作权限，应禁止未授权访问和非法使用用户个人金融信息。（F3）	根据“业务需要”和“最小权限”原则，进行个人金融信息相关权限管理，严格控制和分 配相关操作权限，应禁止未授权访问和非法使用用户个人金融信息。	此项不适合，该项要求一般在应用、数据库层面上核查	此项不适合，该项要求一般在应用、数据库层面上核查	此项不适合，该项要求一般在应用、数据库层面上核查
个人信息保护	[关键]d)金融机构应依据 JR/T 0171—2020 对个人金融信息收集、传输、存储、使用、删除、销毁等 处理的整个过程进行管理与控制，并对个人金融信息生命周期过程进行安全检查与评估。（F3）	金融机构应依据 JR/T 0171—2020 对个人金融信息收集、传输、存储、使用、删除、销毁等 处理的整个过程进行管理与控制，并对个人金融信息生命周期过程进行安全检查与评估。	此项不适合，该项要求一般在应用、数据库层面上核查	此项不适合，该项要求一般在应用、数据库层面上核查	此项不适合，该项要求一般在应用、数据库层面上核查
个人信息保护	[关键]e)金融机构应依据国家与行业主管部门要求，对通过计算机屏幕、客户端软件、银行卡受理设 备、ATM 设备、自助终端设备、纸（如受理终端打印出的支付交易凭条等交易凭证）等界面 展示的个人金融信息，应采取字段屏蔽（或截词）等处理措施，降低个人金融信息在展示环 节的泄露风险。（F3）	金融机构依据国家与行业主管部门要求，对通过计算机屏幕、客户端软件、银行卡受理设 备、ATM 设备、自助终端设备、纸（如受理终端打印出的支付交易凭条等交易凭证）等界面 展示的个人金融信息，应采取字段屏蔽（或截词）等处理措施，降低个人金融信息在展示环 节的泄露风险。	此项不适合，该项要求一般在应用、数据库层面上核查	此项不适合，该项要求一般在应用、数据库层面上核查	此项不适合，该项要求一般在应用、数据库层面上核查
个人信息保护	[关键]f)应向个人金融信息主体告知共享、转让个人金融信息的目的、数据接收方的身份和数据安全 保护能力，并事先征得个人金融信息主体明示同意，共享、转让经去标识化处理的个人金融 信息，且确保数据接收方无法重新识别个人金融信息主体的除外。（F3）	向个人金融信息主体告知共享、转让个人金融信息的目的、数据接收方的身份和数据安全 保护能力，并事先征得个人金融信息主体明示同意，共享、转让经去标识化处理的个人金融 信息，且确保数据接收方无法重新识别个人金融信息主体的除外。	此项不适合，该项要求一般在应用、数据库层面上核查	此项不适合，该项要求一般在应用、数据库层面上核查	此项不适合，该项要求一般在应用、数据库层面上核查
个人信息保护	[关键]g)开发环境、测试环境不应使用真实的个人金融信息，应使用虚构的或经过去标识化处理的个 人金融信息，账号、卡号、协议号、支付指令等测试确需除外。（F3）	开发环境、测试环境不应使用真实的个人金融信息，应使用虚构的或经过去标识化处理的个 人金融信息，账号、卡号、协议号、支付指令等测试确需除外。	此项不适合，该项要求一般在应用、数据库层面上核查	此项不适合，该项要求一般在应用、数据库层面上核查	此项不适合，该项要求一般在应用、数据库层面上核查

安全计算环境-数据库（S3A3G3）作业指导书					
安全控制点	检测项	要求解读	测评方法	预期结果或主要证据	符合情况
身份鉴别	[关键]a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，应实现身份鉴别信息防窃取和 防重用。静态口令应在8位以上，由字母、数字、符号等混合组成并每半年更换口令，不允 许新设定的口令与前次旧口令相同。应用系统用户口令应在满足口令复杂度要求的基础上定 期更换。（F3）	应检查Oracle数据库的口令策略配置，查看其身份鉴别信息是否具有不易被冒用的特点，例如，口令足够长，口令复杂(如规定字符应混有大,小写字母数字和特殊字符)，口令定期更新，新旧口令的替换要求	1)访谈数据库管理员系统用户是否已设置密码，并查看登录过程中系统账户是否使用了密码进行验证登录 2)查看是否启用口令复杂度函数:select limit from dba_profiles where profile= ' DEFAULT' and resource_name=' PASSWORD_VERIFY_FUNCTION' 3)检查utlpwdmg.sql 中“-- Check for the minimum length of the password“部分中“length(password)<"后的值 4) PASSWORD_LIFE_TIME(口令过期时限) 5)访谈前一次口令与当前使用口令是否相同	1)需要登录密码 2)dba_profiles 策略中PASSWORD_VERIFY_FUNCTION'的值不为UNLLIMITED 3)utlpwdmg.sql 中“-- Check for the minimum length of the password“部分中“length(password)<"后的值为8或以上 4) dba_profiles 策略中PASSWORD_LIFE_TIME 不为UNLIMITED 5)新设定口令与前一次口令不相同	符合情况：仅可通过账户名加口令的方式进行登录，不存在空口令和弱口令账户，并已设置口令复杂度要求，且当前口令符合口令复杂度要求，并定期更换口令，新设定口令与前一次口令不同 部分符合情况：通过账户名加口令的方式进行登录，不存在空口令和弱口令账户，但未设置口令复杂度要求，当前口令不符合口令复杂度要求，或口令未定期更换，或新口令与前次旧口令相同 不符合情况：存在空口令或弱口令账户、可绕过身份鉴别措施进行登录
身份鉴别	[关键]b)应具有登录失败处理功能，应配置并启用结束会话、限制登录间隔、限制非法登录次数和当登 录连接超时自动退出等相关措施。（F3）	应检查数据库系统，查看是否已配置了鉴别失败处理功能，并设置了非法登录次数的限制值，对超过限制值的登录终止其鉴别会话或临时封闭帐号。查看是否设置网络登录连接超时，并自动退出	1)查看是否启用登录失败限制策略，执行：select limit from dba_profiles where profile= ' DEFAULT' and resource name=' FAILED_LOGIN_ATTEMPTS 2)查看是否启用登录失败锁定策略，执行：select limit from dba_profiles where profile= 'DEFAULT' and resource_ name= PASSWORD_ LOCK_TIME" 3)查看是否启用登录超时退出策略，执行：select limit from dba_profiles= 'DEFAULT and	1)dba_pofiles 策略中FAILED_LOGIN_ATTEMPTS不为UNLIMITED 2)dba_pofiles 策略中PASSWORD_LOCK_TIME 不为UNLIMITED 3)dba_pofiles策略中IDLE_ TIME不为UNLIMITED	符合情况：已配置登录失败处理功能相关参数，且设置登录超时锁定参数 部分符合情况：已配置登录失败处理功能相关参数，但未设置登录超时锁定参数，或未配置登录失败处理功能相关参数，但已设置登录超时锁定参数 不符合情况：未配置登录失败处理功能参数，未设置登录超时锁定参数
身份鉴别	[关键]c)当进行远程管理时，应对管理终端进行身份标识和鉴别，采用密码技术防止鉴别信息在网络 传输过程中被窃听。（F3）	为了防止包括鉴别信息在内的敏感信息在网络传输过程中被窃听，应限制从远程管理数据，如果业务模式需要从远程进行管理，则应提供包括SSH在内的方式对传输数据进行加密	1) 查看initsSID.ora(%ORACLE_HOME\db_1\NETWORK\ADMIN) 中 REMOTE_0S_AUTHENT的赋值 2) 查看 listene.ora(%ORACLE_HOME\db_1\NETWORK\ADMIN) 文件中的"LISTENER” -"DESCRIPTION "-"ADDRESS_LIST"-"ADDRESS"-"PROTOCOL"项目的 赋值 3)执行show parameter	1)符合，且本项为false, 则符合(为true,远程操作系统认证。 2) 应存在以下项目：PROTOCOL=TCPS (实际为TCP) 3)结果应为NONE,远程无法登录，Exclusive (唯一的数据库密码文件登录	符合情况：采用的远程管理方式启用了SSL连接特性，采取SSH隧道加密连接远程管理通信 部分符合情况：无 不符合情况：采用未进行加密处理的远程管理方式

身份鉴别	[关键]d)应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	Oracle不能集成其他身份鉴别措施，应通过对操作系统层面实现双因素，强化数据库安全	查看和询问系统管理员在登录数据库的过程中使用了哪些身份鉴别方法，是否采用了两种或两种以上组合的鉴别技术，如口令、数字证书Ukey. 令牌、指纹等，是否有一种鉴别方法使用密码技术	除口令之外，采用了另外一种鉴别机制，此机制采用了密码技术，如调用了密码机或采取SM1-SM4等算法	符合情况：已部署堡垒机，通过堡垒机管理服务器来实现双因素身份验证，且在硬件Ukey中使用了加密算法 部分符合情况：已部署堡垒机，通过堡垒机管理服务器来实现双因素身份验证，但采用加密算法 不符合情况：未部署堡垒机，未通过堡垒机管理服务器来实现双因素身份验证
访问控制	[重要]a)应对登录的用户分配账户和权限。	应检查数据库系统的安全策略，查看业务数据的管理员是否具有系统管理功能，业务数据库的操作人员是否具有删除数据库表或存储过程的权限	查看每个登录用户的角色和权限，是否是该用户所需的最小权限	MGMT_UIEW, SYS, SYSTEM, DBSNMP, SYSMAN是open的状态，其他都是锁定	符合情况：已创建不同账户，并且根据用户所需为其分配相应的权限 部分符合情况：已创建不同的用户，但未进行权限的划分 不符合情况：未对登录的用户分配账户和权限
访问控制	[关键]b)应重命名或删除默认账户，修改默认账户或预设账户的默认口令。（F3）	1)在oracle系统安装时存在部分默认口令，如 SYS：CHANGE_ON_INSTALL SYSTEM:MANAGER 2)常用口令: oracle:oracle/admin/ora92(ora+版本) sys: oracle/admin system: oralce/admin	1) 登录验证sys的口令是否为CHANGE_ON_INSTALL 2) 登录验证system的口令是否为manager 3) 登录验证dbsnmp的口令是否为dbsnmp	1)2)3)使用默认口令无法登陆数据库账户，并且修改默认账户或预设账户的默认口令	符合情况：不存在默认的、无用的可登录账户，已删除或禁用默认账户 部分符合情况：存在默认账户或预设账户，但已修改默认账户默认口令 不符合情况：存在默认账户或预设账户，且默认账户口令也未修改
访问控制	[关键]c)应用系统应对首次登录的用户提示修改默认账户或预设账户的默认口令。（F3）	应用系统应对首次登录的用户提示修改默认账户或预设账户的默认口令。	此项不适合，该项要求一般在应用系统上实现	此项不适合，该项要求一般在应用系统上实现	此项不适合，该项要求一般在应用系统上实现
访问控制	[重要]d)应及时删除或停用多余的、过期的账户，避免共享账户的存在。	应删除数据库中多余的过期的账户，如测试帐号等	1) 在sqIplus中执行命令：select username，account_ status_from dba users 2)查看返回结果中是否存在scott. out1n、 ordsys等范例数据库帐号 3)针对上述命令获得的用户帐号，查看是否存在过期账户，询问数据库管理员是否每一个账户均为正式、有效的账户 4)针对上述命令获得的用户帐号，询问是否存在多人共享账户的情况	1)不存在示例帐户 2) 应不存在acount status为“expired"的帐户;所有帐户均为必要的管理帐户或者数据库应用程序帐户(不存在测试帐户/临时账户) 3)每一个数据库帐户与实际用户应为一一对应关系 4)不存在多人共享帐户的情况	符合情况：不存在默认的、无用的可登录账户， 部分符合情况：存在默认账户，但已修改默认账户口令 不符合情况：存在默认账户，且默认账户口令也未修改
访问控制	[一般]e)应授予管理用户所需的最小权限，实现管理用户的权限分离。	在Oracle数据库中，尽量将数据库系统特权用户的权限进行分离	询问是否由不同员工分别担任操作系统管理员与数据库管理员	由不同员工分别担任操作系统管理员与数据库管理员	符合情况：已对各不同权限的用户创建不同的账户，如安全管理员、审计管理员、系统管理员，且采用权限分配最小化原则对管理用户进行权限分配 部分符合情况：已对各不同权限的用户创建不同的账户，但各用户权限限分配不合理 不符合情况：未对不同权限的用户进行权限分离，仅采用超级管

访问控制	[关键]f)应严格限制默认账户或预设账户的权限，如默认账户和预设账户的权限应为空权限或某单一功能专用权限等。（F3）	严格限制默认账户或预设账户的权限，如默认账户和预设账户的权限应为空权限或某单一功能专用权限等。	1)应核查限制默认账户或预设账户的权限分配和限制措施	默认账户或预设账户为空权限或单一专用权限，不与其他用户权限交叉	符合情况：已对默认账户或预设账户的使用进行限制，并划分专用权限 不符合情况：对默认账户或预设账户的使用未进行限制，并且账户权限未进行划分
访问控制	[一般]g)应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。	应检查数据库系统的安全策略，查看是否明确主体(如用户)以用户和/或用户组的身份规定对客体(如文件或系统设备，目录表和存取控制表等)的访问控制，覆盖范围是否包括与信息安全直接相关的主体(如用户)和客体(如文件，数据库表等)及它们之间的操作[如读、写或执行)	询问数据库管理员，数据库系统是否由特定账户进行配置访问控制策略，具体访问控制策略是什么	由特定账户进行配置访问控制策略，并根据用户角色限制账户权限	符合情况：已对各不同权限的用户创建不同的账户，如安全管理员、审计管理员、系统管理员，且采用权限分配最小化原则对管理用户进行权限分配 部分符合情况：已对各不同权限的用户创建不同的账户，但各用户权限限分配不合理 不符合情况：未对不同权限的用户进行权限分离，仅采用超级管
访问控制	[一般]h)访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级。	明确提出访问控制的粒度要求，重点目录的访问控制的主体可能为某个用户或某个进程，应能够控制用户或进程对文件、数据库表等客体的访问	询问数据库管理员，访问控制的粒度主体是否用户级或进程级，客体是否为文件、数据库表级	由管理用户进行用户访问权限分配进行设置，依据访问控制策略，对各类文件和数据库表级进行访问	符合情况：已指定授权主体（一般为安全管理员）对数据库访问控制权限进行配置，且授权主体为用户，客体未数据库表 部分符合情况：已指定专门的安全员负责对访问控制权限的授权工作，但安全策略配置不合理 不符合情况：未指定授权主体对操作系统访问控制权限进行配置
访问控制	[一般]i)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	应通过Oracle数据库或其它措施对重要的信息资源设置敏感标记，从而实现强制访问控制功能	1)检查是否安装Oracle Lable Security模块 2)查看是否创策略：SELECT policy_name,status form DBA_SA_POLICIES 3)查看是否创建级别：SELECT * form dba_sa_levels ORDER BY level_number 4)查看标签创建情况：select * from dba_sa_labels. 5)询问重要数据存储表格名称 6)查看策略与模式|表的对应关系：select * from dba_sa_tables policles, 判断是否针对重要信息资源设置敏感	1)返回的用户用户中应存在'LBACSYS' 2)存在状态为"enable'的标签策略 3) -4)返回结果不为空 5)重要资源所在的表格名称 6)返回结果应不为空，且项目包含5)的结果	符合情况：在数据库所在操作系统上，已对重要主体或客体设置安全标记，且已控制主体对有安全标记信息资源的访问 部分符合情况：在数据库所在操作系统上，已配置安全标记，但安全标记配置不合理等 不符合情况：未在数据库所在操作系统上对重要主体或客体设置安全标记
安全审计	[重要]a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。	应检查数据库系统是否开启安全审计功能，查着当前审计范围是否覆盖到每个用户	1)执行：selecet value form v$parameter where name='audit_trail', 查看是否开启审计功能 2)用不同的用户登录数据库系统并进行不同的操作，在Oracle数据库中查看日志记录是否满足要求。	1) audit_trail 结果应不为pone 2)可在Oracle数据库中查看不同的用户登录数据库系统并进行不同的操作日志记录。	符合情况：已开启安全审计功能，且审计覆盖到每个用户 部分符合情况：已开启安全审计功能，但审计未覆盖到所有用户 不符合情况：未开启安全审计功能

安全审计	[一般]b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	应检查数据库系统，查看审计策略是否覆盖系统内重要的安全相关事件，例如，用户登录系统、自主访问控制的所有操作记录、重要用户行为(如增加/删除用户，删除库表)等	1)show parameter audit_trail 2>show parameter audit_sys_operations 3)select sel,upd,del,ins,gra from dba_obj_audit _opts 4)select sel,upd,del,ins,gra from dba_stmt_audit _opts 5)select sel,upd,del,ins,gra from dba_priv_audit _opts 6)记录一条日志内容,确认其包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源(如末端标识符)、事件的结果	1)应不为none 2)应为true 3)返回对象审计选项，应不全部为“-/-” 4)返回语句审计选项，应不全部为“-/-” 5)返回特权审计选项，应不全那为“-/-” 6)默认满足	符合情况：审计记录包括事件的日期和时间，用户、事件类型，事件是否成功及其他与审计相关的信息 部分符合情况：审计记录不全、记录信息不够详细 不符合情况：未开启审计功能，无审计记录
安全审计	[关键]c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等，审计记录保存 时间应不少于 6 个月。 (F3)	应检查Oracle数据库系统， 查看是否对日志进行了权限设置，非授权人员不能对日志进行操作,另外，应防止审计日志空间不够而导致无法记录日志的情况发生	是否严格限制用户访问审计记录的权限，如采用audit vault 等	安全审计管理员定期对审计记录进行备份，对审计记录的维护和导出由专人负责，并且日志记录保存不少于6个月	符合情况：已对审计记录进行保护，无法进行删除、修改或覆盖，且定期备份，定期将本地存储日志转发至日志服务器，且保存时间大于6个月 部分符合情况：无 不符合情况：未对审计记录进行保护，保存时间未达到6个月
安全审计	[一般]d)应对审计进程进行保护，防止未经授权的中断。	对于Oracle数据库系统默认符合，但是如果采取了第三方工具，则应检查数据库系统，查看未授权用户是否能中断审计进程	1)询问是否严格限制管理员权限 2)用户可以通过alter system set audit_trail=none并重启实例关闭审计功能，查看是否成功	1)已限制管理员审计功能权限 2)测试其他人员无法对审计进程开启、关闭操作	符合情况：已通过第三方系统对审计进行进行监控和保护，审计进程无法进行未授权的中断，管理员不可对日志进行删除 部分符合情况：无 不符合情况：未对审计进行进行保护，非授权人员可中断审计进程，可随意对审计日志进行更改、删除等操作
安全审计	[关键]e)对于从互联网客户端登录的应用系统，应在用户登录时提供用户上一次非常用设备成功登录 的日期、时间、方法、位置等信息。 (F3)	对于从互联网客户端登录的应用系统，在用户登录时提供用户上一次非常用设备成功登录 的日期、时间、方法、位置等信息。	此项不适合，该项要求一般在应用层面上核查	此项不适合，该项要求一般在应用层面上核查	此项不适合，该项要求一般在应用层面上核查
安全审计	[关键]f)审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的一致性与正 确性。 (F3)	审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的一致性与正 确性。	1)应核查系统是否部署时钟同步服务器。	部署时钟同步的ntp服务器，审计记录产生的时间与系统范围内唯一确定的时钟产生的时间一致	符合情况：已部署ntp服务器，并且审计记录产生的时间与系统范围内唯一确定的时钟产生的时间一致 部分情况：无 不符合情况：未部署时钟同步的ntp服务器，审计记录时间无法对应
入侵防范	[重要]a)应遵循最小安装的原则，仅安装需要的组件和应用程序。	遵循最小安装原则，仅安装需要的组件和应用程序，能够极大的降低遭受攻击的可能性。及时更新系统补丁，避免遭受由于系统漏洞带来的风险	此项不适合，该项要求一般在服务器层面上核查	此项不适合，该项要求一般在服务器层面上核查	此项不适合，该项要求一般在服务器层面上核查
入侵防范	[关键]b)应关闭不需要的系统服务、默认共享和高危端口。	关闭不需要的系统服务、默认共享和高危端口，可以有效降低系统遭受攻击的可能性	此项不适合，该项要求一般在服务器层面上核查	此项不适合，该项要求一般在服务器层面上核查	此项不适合，该项要求一般在服务器层面上核查

入侵防范	[重要]c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。	Oracle数据库限制远程连接IP地址	查看在sqlnet. ora文件中是否配置参数：tcp.validnode_checking，tcp,invited_nodes tcp.validnode_checking=yes tcp.invited_nodes=() #运维访问的IP列表，各IP之间用逗号分隔	在sqlnet. ora文件中tcp.validnode_checking=yes tcp.invited_nodes已配置参数ip列表	符合情况：已通过防火墙或其他安全设备对接入终端进行限制，如指定特定ip或对网络地址范围进行限制等 部分符合情况：通过网路地址范围对终端接入方式进行限制，但地址范围过大 不符合情况：未对终端接入方式进行限制
入侵防范	[关键]d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。	本条款要求应用系统应对数据的有效性进行验证，主要验证那些通过人机接口(如程序的界面)输入或通过通信接口输入的数据格式或长度是否符合系统设定要求，防止个别用户输入畸形数据而导致系统出错(如SQL 注入攻击等),人而影响系统的正常使用甚至危害系统的安全	此项不适合，该项要求一般在应用层面上核查	此项不适合，该项要求一般在应用层面上核查	此项不适合，该项要求一般在应用层面上核查
入侵防范	[关键]e)应能通过使用漏洞扫描工具、人工漏洞排查分析等漏洞检查手段，及时发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。（F3）	攻击者可能利用操作系统存在的安全漏洞对系统进行攻击，应对系统进行漏洞扫描，及时发现系统中存在的已知漏洞，并在经过充分测试评估后更新系统补丁，.避免遭受由系统漏洞带的风险	访谈Oracle补丁升级机制，查看补丁安装情况： #cd $ORACLE HOME/0patch opatch lsinventory	返回OPatch version信息和OUI version信息	符合情况：有定期进行漏洞扫描，及时发现安全风险，并根据扫描结果及时对安全问题进行修补 部分符合情况：定期进行漏洞扫描，但未及时修补漏洞 不符合情况：未定期进行漏洞扫描
入侵防范	[重要]f)应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。	要维护系统安全，必须进行主动监视，一般是在网络边界、 核心等重要节点处部署IDS. IPS等系统，或在防火墙、UTM房用入侵检测功能，以检查息是否发生了入侵和攻击	此项不适合，该项要求一般在服务器层面上核查	此项不适合，该项要求一般在服务器层面上核查	此项不适合，该项要求一般在服务器层面上核查
入侵防范	[关键]g)所有安全计算环境设备应全部专用化，生产设备不得进行与业务不相关的操作。（F3）	所有安全计算环境设备全部专用化，生产设备不得进行与业务不相关的操作。	1)应核查设备是否全部专用化，	当前设备统一由安全部门部署搭建，仅相关管理员拥有设备账户进行运维管理，并且无法进行与业务不相关的操作	符合情况：所有安全计算环境设备全部专用化，生产设备不得进行与业务不相关的操作 不符合情况：未对安全计算环境设备的使用进行限制，可以进行与业务不相关的操作。
入侵防范	[关键]h)应能够有效屏蔽系统技术错误信息，不得将系统产生的错误信息直接或间接反馈到前台界面。（F3）	能够有效屏蔽系统技术错误信息，不得将系统产生的错误信息直接或间接反馈到前台界面。	此项不适合，该项要求一般在应用层面上核查	此项不适合，该项要求一般在应用层面上核查	此项不适合，该项要求一般在应用层面上核查
恶意代码防范	[关键]a)应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断并定期统一进行升级和更新防恶意代码库。（F3）	无论是Windows主机还是Linux主机，都面临木马、蠕虫等病毒的破坏。因此一般的主机为防范病毒，均会安装反病毒软件，或者采用可信验证机制对系统程序、应用程序等进行可信执行验证	此项不适合，该项要求一般在服务器上实现	此项不适合，该项要求一般在服务器上实现	此项不适合，该项要求一般在服务器上实现
恶意代码防范	[关键]b)应建立病毒监控中心，对网络内计算机感染病毒的情况进行监控。（F3）	建立病毒监控中心，对网络内计算机感染病毒的情况进行监控。	此项不适合，该项要求一般在服务器上实现	此项不适合，该项要求一般在服务器上实现	此项不适合，该项要求一般在服务器上实现

可信验证	[一般]a)可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	针对服务器设备，需要服务器在启动过程对预装软件(包括系统引导程序、系统程序、相关应用程序和重要配置参数)进行完整性验证或检测，确保对系统引导程序、系统程序、重要配置参数和关键应用程序的篡改行为能被发现，并报警便于后续的处置动作	1)核查服务器的启动，是否实现可信验证的检测过程，查看对那些系统引导程序、系统程序或重要配置参数进行可信验证 2)修改其中的重要系统程序之一和应用程序之一，核查是否能够检测到并进行报警 3)是否将验证结果形成审计记录送至安全管理中心	1) 服务器具有可信根芯片或硬件 2)启动过程基于可信根对系统引导程序、系统程序，重要配置参数和关键应用程序等进行可信验证度量 3)在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心 4)安全管理中心可以接收设备的验证结果记录	符合情况：服务器具有可信根芯片或硬件，可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心 部分符合情况：具有可信根芯片或硬件，但未将验证结果形成审计记录送至安全管理中心 不符合情况：无可信根芯片或硬件
数据完整性	[重要]a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、 重要业务数据、重要审计数据、重要配置数据.重要视频数据和重要个人信息在传输过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1)询问系统管理员，该数据库的鉴别数据、重要业务数据、重要审计数据，重要配置数据，重要视频数据和重要个人信息等在传输过程中是否采用了校验技术或密码技术保证完整性 2)使用工具对通信报文中的鉴别数据、重要业务数据、重要审计数据，重要配置数据、重要视频数据和重要个人信息等进行篡改，查看是否能够检测到未知据在传输过程中的完整性受到破坏并能够及时恢	1） 数据库提供对鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性保护措施 2） 数据库检测到鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性受到被坏后采取了技术措施进行处理，如重传或其他方式	符合情况：已采用校验技术或密码技术保障重要数据在传输过程中的完整性 部分符合情况：无 不符合情况：未采用校验技术或密码技术保障重要数据在传输过程中的完整性
数据完整性	[关键]b)应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。	对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息在存储过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施	1)询问数据库管理员，是否采用校验技术或密码技术保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性 2)尝试修改存储在数据库中的鉴别数据，重要业务效据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等，查看系统反应	1)数据库采用校验技术或密码技术保证了鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性 2)数据库可检测到存储在数据库中的鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等被修改的行为，并具备恢复措施	符合情况：已采用校验技术或密码技术保障重要数据在存储过程中的完整性 部分符合情况：无 不符合情况：未采用校验技术或密码技术保障重要数据在存储过程中的完整性
数据保密性	[关键]a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。	对鉴别数据、重要业务数据、和重要个人信息在传输过程中采取保密措施，如对这些数据加密等	1)询问数据库管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性 2) 通过嗅探等方式抓取传输过程中的数据，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理	1)数据库管理员采用密码技术对鉴别数据、重要业务数据和重要个人信息进行了保密性处理 2) 通过嗅探等方式抓取传输过程中的数据，未发现鉴别数据、重要业务数据和重要个人信息	符合情况：已采用密码技术保障重要数据在传输过程中的保密性 部分符合情况：无 不符合情况：未采用密码技术保障重要数据在传输过程中的保密性
数据保密性	[关键]b)应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于系统鉴别数据、重要业务数据和个人金融信息中的客户鉴别信息以及与账号结合使用可鉴别用户身份的鉴别辅助 信息等个人敏感信息，对于其他直接反应特定自然人某些情况的信息，宜使用密码技术保护 其存储过程中的保密性。 (F3)	对鉴别数据、重要业务数据和重要个人信息在存储过程中采取保密措施，如对这些数据进行加密等	1)询问数据库管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性 2) 核查数据库中的相关字段，查看鉴别数据、重要业务数据和重要个人信息等是否加密存储	1)系统采用了密码技术对存储在数据库中的鉴别数据、重要业务数据和重要 2)数据库中存储的鉴别数据、重要业务数据和重要个人信息等均加密存储	符合情况：已采用密码技术保障重要数据在存储过程中的保密性 部分符合情况：无 不符合情况：未采用密码技术保障重要数据在存储过程中的保密性

数据备份恢复	[关键]a)应提供重要数据的本地数据备份与恢复功能，采取实时备份与异步备份或增量备份与完全备份的方式，增量数据备份每天一次，完全数据备份可根据系统的业务连续性保障相关指（如RPO，RTO）以及系统数据的重要程度、行业监管要求，制定备份策略。备份介质场外存放，数据保存期限依照国家相关规定。（F3）	提供重要数据的本地数据备份与恢复功能，采取实时备份与异步备份或增量备份与完全备份的方式，增量数据备份每天一次，完全数据备份可根据系统的业务连续性保障相关指（如RPO，RTO）以及系统数据的重要程度、行业监管要求，制定备份策略。备份介质场外存放，数据保存期限依照国家相关规定。	1)应核查设备的备份恢复策略	)核查备份结果与备份策略一致 2)核查近期恢复测试记录能够进行正常的数据恢复	符合情况：已提供重要数据处理系统的热冗余，如热备、集群、负载均衡等高可用方式 部分符合情况：无 不符合情况：未提供重要数据处理系统的热冗余
数据备份恢复	[重要]b)应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地。	提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地。	1)应核查设备的数据异地备份策略	1)已部署异地备份机房，并符合备份策略通过网络定期进行异地备份 2)查看实现的配置结果与备份策略一致	符合情况：已提供异地数据备份功能，实时将数据备份至异地备份机房 部分符合情况：已提供异地数据备份功能，但未实时将数据备份至异地机房 不符合情况：未提供异地数据备份功能
数据备份恢复	[关键]c)应提供重要数据处理系统的热冗余，保证系统的高可用性。	提供重要数据处理系统的热冗余，保证系统的高可用性。	1)应核查设备的部署方式，是否采用热冗余方式进行部署	1)对重要数据，如用户数据，鉴别数据等定期进行备份，通过磁带备份到本地 2)对于重要设备，采取热备、集群、负载均衡等高可用方式	符合情况：已提供重要数据处理系统的热冗余，如热备、集群、负载均衡等高可用方式 部分符合情况：无 不符合情况：未提供重要数据处理系统的热冗余
数据备份恢复	[关键]d)对于同城应用级灾难备份中心，应与生产中心直线距离至少达到30km，可以接管所有核心业务的运行；对于异地应用级灾难备份中心，应与生产中心直线距离至少达到100km。（F3）	于同城应用级灾难备份中心，应与生产中心直线距离至少达到30km，可以接管所有核心业务的运行；对于异地应用级灾难备份中心，应与生产中心直线距离至少达到100km。	1)应核查系统是否部署灾难备份中心，生产中心与灾备中心的直线距离是否满足要求。	系统提供异地实时备份功能，并且同城灾备机房与生产中心的直线距离达到30KM以上，异地灾备中心与生产中心直线距离达到100KM以上	符合情况：系统提供异地实时备份功能，并且异地灾备机房与生产中心的直线距离达到100KM以上 部分符合情况：无 不符合情况：同城灾备中心与生产中心直线记录未达到30KM以上，或者异地灾难备份中心，与生产中心直线距离未达到100km以上
数据备份恢复	[关键]e)为满足灾难恢复策略的要求，应对技术方案中关键技术应用的可行性进行验证测试，并记录和保存验证测试结果。（F3）	为满足灾难恢复策略的要求，应对技术方案中关键技术应用的可行性进行验证测试，并记录和保存验证测试结果。	1)应核查是否对关键技术应用的可行性进行验证测试。 2)核查是否具备验证测试记录	1)对备份数据定期进行验证测试 2)对进行的验证测试留有相应的测试记录	符合情况：定期每季度对备份数据进行一次验证测试，并每次验证测试留有测试记录 部分符合情况：定期每季度对备份数据进行一次验证测试，但是没有测试记录 不符合情况：未定期对备份数据进行验证测试
数据备份恢复	[关键]f)数据备份应至少保存两个副本，且至少一份副本异地存放，完全数据备份至少保证以一个星期为周期的数据冗余。（F3）	数据备份应至少保存两个副本，且至少一份副本异地存放，完全数据备份至少保证以一个星期为周期的数据冗余。	1)应核查数据备份是否至少保存两个副本，且至少一份副本异地存放， 2)核查是否具备数据备份记录	1)对备份的数据至少保存两个版本，其中一份异地存放 2)对备份数据提供备份记录	符合情况：当前数据备份保存有两个副本，存在异地和本地备份等多种方式，分别保存在主机房和灾备机房，并且留存有数据备份记录 部分符合情况：当前数据备份保存有两个副本，存在异地和本地备份等多种方式，分别保存在主机房和灾备机房，但是未保存数据备份记录 不符合情况：备份数据未采用多

数据备份恢复	[关键]g)异地灾难备份中心应配备恢复所需的运行环境，并处于就绪状态或运行状态，“就绪状态”指备份中心的所需资（相关软硬件以及数据等资源）已完全满足但设备CPU还没有运行，“运行状态”指备份中心除所需资源完全满足要求外，CPU也在运行状态。（F3）	异地灾难备份中心应配备恢复所需的运行环境，并处于就绪状态或运行状态，“就绪状态”指备份中心的所需资（相关软硬件以及数据等资源）已完全满足但设备CPU还没有运行，“运行状态”指备份中心除所需资源完全满足要求外，CPU也在运行状态。	1)应核查异地灾难备份中心是否配备恢复所需的运行环境，是否处于就绪状态或运行状态，	异地灾难备份中心已配备恢复所需的运行环境，处于就绪状态或运行状态	符合情况：异地灾难备份中心已配备恢复所需的运行环境，处于就绪状态或运行状态 部分符合情况：无 不符合情况：异地灾难备份中心未配备恢复所需的运行环境
剩余信息保护	[关键]a)应保证操作系统、数据库系统和应用系统用户鉴别信息所在的存储空间被释放或重新分配前得到完全清除，无论这些信息是存放在硬盘上还是内存中。（F3）	保证操作系统、数据库系统和应用系统用户鉴别信息所在的存储空间被释放或重新分配前得到完全清除，无论这些信息是存放在硬盘上还是内存中。	1)应核查操作系统、数据库系统和应用系统用户鉴别信息所在的存储空间被释放或重新分配前是否得到完全清除，	数据库采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。	符合情况：采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除系统中的剩余信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等。 不符合情况：未对剩余信息进行及时清理。
剩余信息保护	[关键]b)应保证操作系统、数据库系统和应用系统用户存有敏感数据的存储空间被释放或重新分配前得到完全清除，无论这些信息是存放在硬盘上还是内存中。（F3）	保证操作系统、数据库系统和应用系统用户存有敏感数据的存储空间被释放或重新分配前得到完全清除，无论这些信息是存放在硬盘上还是内存中。	1)应核查操作系统、数据库系统和应用系统用户存有敏感数据的存储空间被释放或重新分配前是否得到完全清除	数据库采取了措施保证对存储介质(如硬盘或内存）中的敏感数据进行及时清除	符合情况：采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除系统中的剩余信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等。 不符合情况：未对剩余信息进行及时清理。
个人信息保护	[关键]a)金融机构在收集、使用个人金融信息时，应遵循合法、正当、必要的原则，应以隐私政策等方式公开收集、使用规则，向个人金融信息主体明示收集、使用信息的目的、方式和范围，并获得个人信息主体的同意。（F3）	金融机构在收集、使用个人金融信息时，遵循合法、正当、必要的原则，应以隐私政策等方式公开收集、使用规则，向个人金融信息主体明示收集、使用信息的目的、方式和范围，并获得个人信息主体的同意。	1)应核查在收集、使用个人金融信息时，是否遵循合法、正当、必要的原则，是否以隐私政策等方式公开收集、使用规则，向个人金融信息主体明示收集、使用信息的目的、方式和范围，并获得个人信息主体的同意，	1）记录数据库所存储的个人信息。如数据库存储了用户身份证号、电话等个人信息 2)记录数据库哪个功能模块使用哪些用户个人信息，以及所使用个人信息的必要性	符合情况：数据库所存储的用户个人信息均为业务所必需的，不存在非必要用户个人信息 部分符合情况：无 不符合情况：数据库违规保存非业务必需的用户个人信息
个人信息保护	[关键]b)应仅采集和保存业务必需的用户个人金融信息。（F3）	仅采集和保存业务必需的用户个人金融信息。	1)应核查是否仅采集和保存业务必需的用户个人金融信息。	1)系统采取了措施控制了数据库账户对个人信息的访问，如权限控制等 2)未授权无法访问和使用用户的个人信息	符合情况：系统已采取措施限制了数据库账户对个人信息的访问，非授权用户无法访问和使用用户的个人信息，且已制定相关个人信息保护制度 部分符合情况：无 不符合情况：未对用户个人信息的访问和使用进行严格的管理，未采取措施来禁止非授权访问和
个人信息保护	[关键]c)应根据“业务需要”和“最小权限”原则，进行个人金融信息相关权限管理，严格控制和分配相关操作权限，应禁止未授权访问和非法使用用户个人金融信息。（F3）	根据“业务需要”和“最小权限”原则，进行个人金融信息相关权限管理，严格控制和分配相关操作权限，应禁止未授权访问和非法使用用户个人金融信息。	1)应核查是否根据“业务需要”和“最小权限”原则，进行个人金融信息相关权限管理，	1)根据数据库访问规则限制了数据库用户仅能对自身权限范围内的表进行操作和访问，禁止非授权访问和非法使用个人金融信息	符合情况：根据数据库访问规则限制了数据库用户仅能对自身权限范围内的表进行操作和访问，禁止非授权访问和非法使用个人金融信息 部分符合情况：无 不符合情况：未对个人信息管理

个人信息保护	[关键]d)金融机构应依据 JR/T 0171—2020 对个人金融信息收集、传输、存储、使用、删除、销毁等处理的整个过程进行管理与控制，并对个人金融信息生命周期过程进行安全检查与评估。（F3）	金融机构应依据 JR/T 0171—2020 对个人金融信息收集、传输、存储、使用、删除、销毁等处理的整个过程进行管理与控制，并对个人金融信息生命周期过程进行安全检查与评估。	1)应核查是否依据 JR/T 0171—2020 对个人金融信息收集、传输、存储、使用、删除、销毁等处理的整个过程进行管理与控制，	依据 JR/T 0171—2020 对个人金融信息收集、传输、存储、使用、删除、销毁等处理的整个过程进行管理与控制	符合情况：依据 JR/T 0171—2020 对个人金融信息收集、传输、存储、使用、删除、销毁等处理的整个过程进行管理与控制 部分符合情况：无 不符合情况：未对个人金融信息收集、传输、存储、使用、删除、销毁等处理的整个过程进行管理与控制
个人信息保护	[关键]e)金融机构应依据国家与行业主管部门要求，对通过计算机屏幕、客户端软件、银行卡受理设备、ATM 设备、自助终端设备、纸（如受理终端打印出的支付交易凭条等交易凭证）等界面展示的个人金融信息，应采取字段屏蔽（或截词）等处理措施，降低个人金融信息在展示环节的泄露风险。（F3）	金融机构依据国家与行业主管部门要求，对通过计算机屏幕、客户端软件、银行卡受理设备、ATM 设备、自助终端设备、纸（如受理终端打印出的支付交易凭条等交易凭证）等界面展示的个人金融信息，应采取字段屏蔽（或截词）等处理措施，降低个人金融信息在展示环节的泄露风险。	1)应核查是否依据国家与行业主管部门要求，对通过计算机屏幕、客户端软件、银行卡受理设备、ATM 设备、自助终端设备、纸（如受理终端打印出的支付交易凭条等交易凭证）等界面展示的个人金融信息，采取字段屏蔽（或截词）等处理措施，	应依据国家与行业主管部门要求，对通过计算机屏幕、客户端软件、银行卡受理设备、ATM 设备、自助终端设备、纸（如受理终端打印出的支付交易凭条等交易凭证）等界面展示的个人金融信息，采取字段屏蔽（或截词）等处理措施，	符合情况：已对计算机屏幕、客户端软件、银行卡受理设备、ATM 设备、自助终端设备、纸（如受理终端打印出的支付交易凭条等交易凭证）等界面展示的个人金融信息，采取字段屏蔽（或截词）等处理措施 部分符合情况：无 不符合情况：未对计算机屏幕、客户端软件、银行卡受理设备、ATM 设备、自助终端设备、纸（如受理终端打印出的支付交易凭条等交易凭证）等界面展示的个人金融信息，采取字段屏蔽（或截词）等处理措施
个人信息保护	[关键]f)应向个人金融信息主体告知共享、转让个人金融信息的目的、数据接收方的身份和数据安全保护能力，并事先征得个人金融信息主体明示同意，共享、转让经去标识化处理的个人金融信息，且确保数据接收方无法重新识别个人金融信息主体的除外。（F3）	向个人金融信息主体告知共享、转让个人金融信息的目的、数据接收方的身份和数据安全保护能力，并事先征得个人金融信息主体明示同意，共享、转让经去标识化处理的个人金融信息，且确保数据接收方无法重新识别个人金融信息主体的除外。	1)应核查是否向个人金融信息主体告知共享、转让个人金融信息的目的、数据接收方的身份和数据安全保护能力	在发生共享、转让个人金融信息时应向个人金融信息主体告知转让个人金融信息的目的、数据接收方的身份和数据安全保护能力	符合情况：在发生共享、转让个人金融信息时，应向个人金融信息主体告知转让个人金融信息的目的、数据接收方的身份和数据安全保护能力 部分符合情况：无 不符合情况：在发生共享、转让个人金融信息时，未告知个人金融信息主体 不适用情况：数据库中收集的个人金融信息，只在单位内部管理员使用，不存在将个人金融信息
个人信息保护	[关键]g)开发环境、测试环境不应使用真实的个人金融信息，应使用虚构的或经过去标识化处理的个人金融信息，账号、卡号、协议号、支付指令等测试确需除外。（F3）	开发环境、测试环境不应使用真实的个人金融信息，应使用虚构的或经过去标识化处理的个人金融信息，账号、卡号、协议号、支付指令等测试确需除外。	1)应核查开发环境、测试环境是否使用真实的个人金融信息，是否使用虚构的或经过去标识化处理的个人金融信息，账号、卡号、协议号、支付指令等测试确需除外。	在开发环境、测试环境未使用真实的个人金融信息，使用虚构的或经过去标识化处理的个人金融信息，账号、卡号、协议号、支付指令等测试确需除外。	符合情况：在开发环境、测试环境未使用真实的个人金融信息，使用虚构的或经过去标识化处理的个人金融信息，账号、卡号、协议号、支付指令等测试确需除外。 部分符合情况：无 不符合情况：在开发环境、测试环境中使用真实的个人金融信息，未做虚构或去标识化处理

安全计算环境-应用系统要求（S3A3G3）作业指导书					
安全控制点	检测项	要求解读	测评方法	预期结果或主要证据	符合情况
身份鉴别	[关键]a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，应实现身份鉴别信息防窃取和 防重用。静态口令应在8位以上，由字母、数字、符号等混合组成并每半年更换口令，不允 许新设定的口令与前次旧口令相同。应用系统用户口令应在满足口令复杂度要求的基础上定 期更换。（F3）	对用户进行身份鉴别是防止非法入侵最基本的一种保护措施，本条款要求应用系统必须对登录系统的用户进行身份的合法性进行核实，并为每一个登录用户提供身份标识，且身份标具有唯-性，以便系统对用户操作行为进行审计。同时，为了增加非授权用户使用暴力猜测等手段破解用户鉴别信息的难度，应保证用户的鉴别信息具有一定的复杂性，从而使身份鉴别信息不易被冒用和破解,如用户登录口令的长度至少为8位、需要强制由字母、数字和符号混合组成，且提供口令更换周期等限制	1)询问系统管理员，用户在登录时是否采用了身份鉴别措施 2)在未登录状态下直接访问任一操作页面或操作功能 3)核查用户身份标识的设置策略 4)核查鉴别信息复杂度和更换周期的设置策略。(可通过查看修改口令等功能模块验证口令复杂度生效情况) 5)扫描应用系统，检查应用系统是否存在弱口令和空口令用户 6)新设定口令与前一次口令是否相同	1)用户在登录时，系统提供了身份鉴别措施 2)在未登录的状态下，用户不可访问任何页面或操作功能，身份鉴别措施不能被绕 3)记录用户在系统中的唯一性息份标识，如用户在数据库用户表中的唯一ID等 4)用户口令具有长度、组成复杂度限制和更换周期限制。(如口令长度8位以上，需要包含数字、牢母和符号，并强制3本月更换一次等) 5)应用系统不存在弱口令和空口令用户 6)新设定口令与前一次口令不相同	符合情况：采用了一种及以上的身份鉴别方式，身份标识具备唯一性，用户口令8位及以上，口令组成由大小写字母、数字和字符组成，口令每90天进行一次更换。新设定口令与前一次口令不同 部分符合情况：预期结果1,2,3,4满足一部分为部分符合。新设定口令与前一次口令相同 不符合情况：未采取身份鉴别方式，用户口令8位以下，且口令组成未采用大小写字母、数字和特殊字符，未定期进行口令更换
身份鉴别	[关键]b)应具有登录失败处理功能，应配置并启用结束会话、限制登录间隔、限制非法登录次数和当登 录连接超时自动退出等相关措施。（F3）	非法用户能够通过反复输入密码，达到猜测用户密码的目的，因此应该限制用户登录过程中连续输入错误密码的次数。 当用户多次输入错误密码后，操作系统应自动锁定该用户或一段时间内禁止该用户登录，从而增加猜测密码难度的目的。 Windows操作系统具备登录失败处理功能，可以通过适当的配置“账户锁定策略”来对用户的登录进行限制	1)询问系统管理员，该系统是否具有登录失败处理功能以及登录失败处理策略 2)以正确的用户名，错误的口令连续多次登录系统，查看系统的反应自动断开的等待时间 3询问统管理员用户登录过程中，系统进行身份鉴别时，设置了合理的连接超时自动断开等待时间 4）询问系统管理员，用户登录后，长时间无操作，系统端束会话时间	1)系统提供了登录失败处理功能 2)以正确的用户名、错误的口令连续多次登录系统，超过预定错误次数时，系统锁定该用户，由管理员解锁或过-段时间后自动解锁 3)用户登录过程中，系统进行身份鉴别时,设置了合理的连接超时自动断开的等待时间。 4)用户登最后，长时间无操作，系统设置了符合业务需求的结束会话时间	符合情况：启用了登录失败处理功能，且非法登录达到一定次数后进行限制，配置了连接自动退出功能。 部分符合情况：预期结果1,2,3满足一部分为部分符合。 不符合情况：未配置登录失败处理功能，未配置非法登录限制措施，未配置登录连接自动超时退出功能。
身份鉴别	[关键]c)当进行远程管理时，应对管理终端进行身份标识和鉴别，采用密码技术防止鉴别信息在网络 传输过程中被窃听。（F3）	为方便管理员进行管理操作，众多服务器采用网络登录的方式进行远程管理操作，Windows一般使用“远程桌面 (Remote Desktop)”进行远程管理，《基本要求》中规定了这些传输的数据需要进行加密处理，目的是为了保障账户和口令的安全， Windows Server 2003 SP1中针对远程桌面提供了SSL加密功能，它可以基于SSL来实现以下两个功能:对RDP客户端提供终端服务器的服务器身份验证、加密和RDP客户端的通信。要使用远程桌面的SSL.加密功能，远程桌面必须使用RDP的版本是5.2或以上，即所远行的操作累统必须是Windows Server 2003 SPI或其后版本。	1)如果是本地管理成KVM等硬件管理方式，此要求默认满足， 2)如果采用远程管理，则需采用带加密管理的远程管理方式。在命令行输入”pgedit.msc“弹出“本地组策略编辑器”窗口，查着“本地计算机策略一》计算机配置一>管理模板一>Windows组件一选程桌面服务>远程桌面会话主机-安全”中的相关项目	1)本地或VM，默认符合 2)远程运维，采取加密的传输协议	符合情况：采用SSH或HTTPS的加密方式进行远程管理。 部分符合情况：无部分符合情况。 不符合情况：采用telnet、http的方式进行远程管理。

身份鉴别	[关键]d)应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	本条款要求应用系统采取两种或两种以上组合的鉴别技术来实现身份鉴别。在这里，两种或两种以上组合签别技术是指同时使用不同种关=类的鉴别技术对应用系统的用户进行身粉鉴别，且其中二种鉴别技术至少应使用密码技术来实现，这样在很大程度上增加了非授权用户对身份鉴别信意进行攻击的难度，更有效的防止非法入侵。对应用系统测评时，双因素登录重点针对开系统内的管理用户	1)询问系统管理员，系统是否采用动态口念，数字证书和生物技术等两种或两种以上组合的鉴别技术对管理用户身份进行登别 2)询问系统管理员，其中一种鉴别技术是否使用密码技术来实现 3)使用系统内管理用户登录系统，验证其登录方式是否与询问结果一致	除口令之外，采用了另外一种鉴别机制，此机制采用了密码技术，如调用了密码机或采取SM1-SM4等算法	符合情况：同时采用两种或两种以上的身份鉴别方式，且其中一种鉴别方式采用了密码技术。 部分符合情况：采用了两种及两种以上的身份鉴别方式，但未包含密码技术。 不符合情况：未同时采用两种或两种以上的身份鉴别方式。
访问控制	[重要]a)应对登录的用户分配账户和权限。	应用系统的访问控制功能是为了保证应用系统被合法地使用，用户只能根据管理员分配的权限来访问应用系统相应的功能,不得越权访问。本项条款要求必须须对登录系统的用户进行账号和权限的分配	1)询问系统管理员，系统是否为登录的用户分配了账户和权限 2)以不同角色的用户登录系统，验证用户权限分配情况 3)尝试使用登录用户访问未授权的功能，查看访问控制策略生效情况	1)系统为登录的每一个用户分配了账户和权限 2)系统为不同类别角色的用户分配了不同的功能权限 3)通过菜单猜测等验证方式，登录用户不可访问未授权的功能权限	符合情况：对登录的用户分配了不同的账户，且分配了不同的权限。 部分符合情况：无部分符合情况。 不符合情况：未对登录的用户分配不同的账户，且未分配相
访问控制	[关键]b)应重命名或删除默认账户，修改默认账户或预设账户的默认口令。（F3）	应用系统正式上线后需要对默认账户进行重命名或删除，并对默认账户默认口令进行修改，默认用户一般指应用系统的公共账户，测试账户或权限不受限制的超级管理账户等	1)访谈系统管理员，系统如何处理多余的、过期的账户 2)核查数据库的用户表中用户状态标识，若系统内存在计=过期账户，则尝试使用过期账户登录系统 3)核查管理员用户与账户之间是否一一对应	1)2)3)使用默认口令无法登陆数据库账户，并且修改默认账户或预设账户的默认口令	符合情况：不存在默认的、无用的可登录账户，已删除或禁用默认账户 部分符合情况：存在默认账户或预设账户，但已修改默认账户默认口令 不符合情况：存在默认账户或预设账户，且默认账户口令也未修改
访问控制	[关键]c)应用系统应对首次登录的用户提示修改默认账户或预设账户的默认口令。（F3）	应用系统应对首次登录的用户提示修改默认账户或预设账户的默认口令。	1)应核查应用系统是否对首次登录的用户提示修改默认账户或预设账户的默认口令。	首次登录应用系统的账户必须需改默认口令。	符合情况：应用系统对首次登陆的用户提示修改账户的默认口令 部分符合情况：无 不符合情况：应用系统对首次登陆的用户未提示修改账户的默认口令
访问控制	[重要]d)应及时删除或停用多余的、过期的账户，避免共享账户的存在。	应用系统的管理员要及时将应用系统中多余的、过期的账户删除或停用，用时要避免多人共用同一账户的情况出现	在命令行输入“lusmrgr.msc",弹出“本地用户和组”窗口，查看“本地用户和组一>用户”中的相关项目，查看右侧用户列表中的用户,询问各账户的用途，确认账户是否属于多余的、 过期的账户或共享账户名	不存在多余账户、测试过期账户。不存在多部门、多人共享账户情况	符合情况：未发现多余、过期账户存在，且管理员用户与账户之间一一对应，无共享账户存在。 部分符合情况：预期结果1,2为一部分符合为部分符合。 不符合情况：设备存在多余、过期账户，且存在共享账户。

访问控制	[一般]e)应授予管理用户所需的最小权限，实现管理用户的权限分离。	本项条款要求应用系统授予管理用户为完成承担任务所需的最小权限，如管理用户仅需具备相关的管理操作，而无需为其分配业务操作的权限，同时，管理用户应实现权限分离，如管理员具备系统管理、用户创建与移除、角色创建与删除等功能权限，安全员具备安全参数配置、用户权限分配等功能权限，审计员具备日志查看等功能权限	1)询问系统管理员，该系统的所有管理账户是否只拥有完成承担任务所需的最小权限，且管理用户根据三权分立原则进行授权 2)抽取某一用户，询问该用户的职责，登录应用系统，查看该用户实际权限分配情况是否与工作职责相符，是否是其承担任务所需的最小权限 3)登录不同级别的管理用户，查看管理用户相互之间是否具有相互制约的关系。(如管理员不能审计、审计员不能管理、安全员不能审计和	1)系统所有管理账户只拥有完成自己承担任务所需的最小权限，所有管理账户均不具备业务操作权限，且管理账户分为管理员、安全员和审计员 2)抽取的用户实际权限分配情况与工作职责相符,为其承担任务所需的最小权限 3)不同管理用户相互之间具有相互制约的关系。(如管理员不能审计，审计员不能管理、安全员不能审计和管理等)	符合情况：创建有系统管理员、审计管理员、安全管理员等账户通过级划分，并赋予去角色权限，各账户仅分配最小的权限。 部分符合情况：预期结果1,2为一部分符合为部分符合。 不符合情况：未创建系统管理员、审计管理员、安全管理员等账户角色，各账户均具备相同的管理员权限。
访问控制	[关键]f)应严格限制默认账户或预设账户的权限，如默认账户和预设账户的权限应为空权限或某单一 功能专用权限等。（F3）	严格限制默认账户或预设账户的权限，如默认账户和预设账户的权限应为空权限或某单一 功能专用权限等。	1)应核查限制默认账户或预设账户的权限分配和限制措施	默认账户或预设账户为空权限或单一专用权限，不与其他用户权限交叉	符合情况：已对默认账户或预设账户的使用进行限制，并划分专用权限 不符合情况：对默认账户或预设账户的使用未进行限制，并且账户权限未进行划分
访问控制	[一般]g)应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。	本条款要求应用系统的访问控制策略应由授权主体（如安全管理员）进行配置，非授权主体不得更改访问控制策略，且访控问制策略的覆盖范围应包括所有主体和客体以及它们之同的操作	1）以管理用户登录，访问权限管理功能，查看访问控制策略 2)以非管理用户登录，访问权限管理功能，查看越权访问情形	1）管理用户负责配置访问控制策略，管理用户为账户分配不同的角色，每个角色分配不同的功能权限，当账户与角色关联时，该账户就具备与角色相关联的功能操作 2)非管理用户不能访问权限管理相关的功能	符合：系统用户账户仅通过管理员账号进行创建和划分权限； 部分部分：系统用户账户仅通过管理员账号进行创建和划分权限，非管理用户能够越权访问； 不符合：访问控制策略可由用户自行设置规则
访问控制	[一般]h)访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级。	明确提出访问控制的粒度要求，主体为用户或进程，客体为功能权限对应的文件和数据库表以及表中的记录或字段	核查并测试访问控制策略的控制粒度是否达到主体为用户级或进程,客体为文件、数据库表、记录或字段级	访问控制策略的控制粒度主体为登录账户，客体为功能权限以及功能权限关联的数据库表	符合：系统提供了访问控制列表，且按照列表进行权限划分，账户无法进行越权操作，访问控制粒度达到数据库表级； 部分符合：系统提供了访问控制列表，但访问控制粒度未达到用户、文件基本。 不符合：经测试系统用户账户
访问控制	[一般]i)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	安全标记表示主体/客体安全级别和安全范畴的一组信息，通过比较标记来控制是否允许主体对客体的访问，标记不允许其他用户进行修改，包括资源的拥有者。本项条款要求应用系统应提供设置安全标记的功能，通过安全标记控制用户对标记信息资源的访问。重要主体指系统中的管理账户，重要客体指系统中鉴别数据、重要业务数据、个人信息以及敏感数据等	1)核查应用系统是否依据安全策略对重要主体和客体设置了安全标记 2）测试依据安全标记是否实现主体对客体的强制访问控制功能	1）应用系统依据安全策略对重要账户和重要信息设置了安全标记 2)系统依据安全标记控制了账户对有安全标记信息资源的访问	符合：系统提供了敏感标记功能，经测试账户仅能对设置了安全标记的资源进行访问； 部分符合：无部分符合 不符合：系统未对重要用户或重要系统资源设置安全标记；

安全审计	[重要]a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。	本条款要求应用系统必须对应用系统所有用户重要操作(如用户登录和重要业务操作等)进行审计，并且对系统异常等事件进行审计	1)核查是否提供并启用了安全审计功能 2)核查审计范围是否覆盖到每个用户 3)核查并测试是否对重要的用户行为和重要安全事件进行审计	1)系统提供并启用了安全审计功能 2)安全审计范围覆盖到系统中的每个用户 3)系统对重要的用户行为和重要安全事件提供了审计	符合情况：设备已开启日志功能，审计范围能覆盖到每个用户，并对每个重要安全事件进行审计。 部分符合情况：预期结果1,2,3为一部分符合为部分符合。 不符合情况：设备未开启日志功能，未能审计到每个用户行
安全审计	[一般]b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	本条款要求审计记录至少包括事件日期，时间，发起者信息(如用户名、IP地址等)、类型、描述和结果(是否成功等)等内容	核查审计记录的内容构成。(查看数据库具体字段或日志展示信息)	审计记录至少包括事件日期，时间，发起者信息(如用户名、IP地址等)、类型、描述和结果(是否成功等)等内容	符合情况：审计记录能覆盖到具体的日期和时间、用户、事件类型、事件是否成功及审计相关信息，系统时间正确。 部分符合情况：预期结果1,2为一部分符合为部分符合。 不符合情况：未开启审计功能，审计记录未包含日期和时间、用户、事件类型、事件是否成功及其他审计信息。
安全审计	[关键]c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等，审计记录保存 时间应不少于 6 个月。（F3）	本条款要求应用系统对审计系统进行保护，定期做好数据备份。另外，应用系统应防止非授权删除、修改或覆盖审计记录	1)核查审计记录的保护措施和备份策略 2)核查应用系统功能权限，系统是否具备对审计记录的删除、修改或覆盖等功能，如果具备对审计记录的删除、修改或覆盖等功能,则查看日志记录删除、修改或覆盖的时间范围是否进行了限制	安全审计管理员定期对审计记录进行备份，对审计记录的维护和导出由专人负责，并且日志记录保存不少于6个月	符合情况：已对审计记录进行保护，无法进行删除、修改或覆盖，且定期备份，定期将本地存储日志转发至日志服务器，且保存时间大于6个月 部分符合情况：无 不符合情况：未对审计记录进行保护、保存时间未达到6个月
安全审计	[一般]d)应对审计进程进行保护，防止未经授权的中断。	本条款要求应用系统应对审计进程或功能进行保护，如果处理审计的事务是一个单独的进程，那么应用系统应对审计进程进行保护，不允许非授权用户子对进程进行中断:如果审计是一个独立的功能，则应用系统应防止非授权用户关闭审计功能	测试应用系统，如果审计模块是独立的进程，则试图非授权中断审计进程，查看是否成功，如果审计模块是一个独立的功能，则试图非授权关闭审计功能，查看是否成功	非授权不能中断审计进程或关闭审计功能	符合情况：非审计管理员的其他账户不能中断审计进程。 部分符合情况：无部分符合情况。 不符合情况：非审计管理员的其他账户能中断审计进程。

安全审计	[关键]e)对于从互联网客户端登录的应用系统，应在用户登录时提供用户上一次非常用设备成功登录 的日期、时间、方法、位置等信息。（F3）	对于从互联网客户端登录的应用系统，在用户登录时提供用户上一次非常用设备成功登录 的日期、时间、方法、位置等信息。	1)应核查对于从互联网客户端登录的应用系统，是否在用户登录时提供用户上一次非常用设备成功登录的日期、时间、方法、位置等信息。	从互联网登录的应用系统，在用户登录时提供用户上一次非常用设备成功登录 的日期、时间、方法、位置等信息	符合情况：从互联网登录的应用系统，在用户登录时提供用户上一次非常用设备成功登录的日期、时间、方法、位置等信息 部分符合情况：无 不符合情况：从互联网登录的应用系统，在用户登录时未提供用户上一次非常用设备成功登录 的日期、时间、方法、位
安全审计	[关键]f)审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的一致性与正 确性。（F3）	审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的一致性与正 确性。	1)应核查系统是否部署时钟同步服务器。	部署时钟同步的ntp服务器，审计记录产生的时间与系统范围内唯一确定的时钟产生的时间一致	符合情况：已部署ntp服务器，并且审计记录产生的时间与系统范围内唯一确定的时钟产生的时间一致 部分情况：无 不符合情况：未部署时钟同步的ntp服务器，审计记录时间无法对应
入侵防范	[重要]a)应遵循最小安装的原则，仅安装需要的组件和应用程序。	遵循最小安装原则，仅安装需要的组件和应用程序，能够极大的降低遭受攻击的可能性。及时更新系统补丁，避免遭受由于系统漏洞带来的风险	此项不适合，该项要求一般在服务器层面上核查	此项不适合，该项要求一般在服务器层面上核查	此项不适合，该项要求一般在服务器层面上核查
入侵防范	[关键]b)应关闭不需要的系统服务、默认共享和高危端口。	关闭不需要的系统服务、默认共享和高危端口，可以有效降低系统遭受攻击的可能性	此项不适合，该项要求一般在服务器层面上核查	此项不适合，该项要求一般在服务器层面上核查	此项不适合，该项要求一般在服务器层面上核查
入侵防范	[重要]c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。	为了保证安全，避免未授权的访问，需要对远程管理防火墙的登录地址进行限制，可以是某一特定的IP地址，也可以来自某一子网、地址范围或地址组	此项不适合，该项要求一般在服务器层面上核查	此项不适合，该项要求一般在服务器层面上核查	此项不适合，该项要求一般在服务器层面上核查
入侵防范	[关键]d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。	本条款要求应用系统应对数据的有效性进行验证，主要验证那些通过人机接口(如程序的界面)输入或通过通信接口输人的数据格式或长度是否符合系统设定要求，防止个别用户输入畸形数据而导致系统出錯(如SQL注入攻击等),从而影响系统的正常使用甚至危害系统的安全	1)询问系统管理员,该系统是否具备软件容错的能力，具体的措施是什么 2)在浏览器或客户端输入不同（如数据格式或长度等符合、不符合软件设定的要求，并可模仿特定的攻击模式）的数据，查看系统的反应	系统具备软件容错能力，提供对输入数据的长度、格式等进行检查和验证的功能，通过限制特定关键字的输入等防护措施防止SQL注入等攻击	符合情况：系统在人机接口中规定了输入内容的格式，长度等，经测试不符合要求的数据无法被提交； 部分符合：无部分符合情况。 不符合情况：系统未提供人机校验功能，可在系统中输入任意危险字符，或上传任意格式文件；

入侵防范	[关键]e)应能通过使用漏洞扫描工具、人工漏洞排查分析等漏洞检查手段，及时发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。（F3）	应用管理员定期对操作系统进行漏洞扫描，-旦发现漏洞应及时进行测试评估后并及时修补漏洞	1)通过漏洞扫描、渗透测试等方式核查应用软件、数据库管理系统和中间件存在高风险漏洞 2）访谈系统管理员是否在经过充分测试评估后及时修补漏洞	应用软件不存在高风险漏洞，若存在，则经过充分测试评估后及时修补漏洞	符合情况：定期对设备进行漏洞扫描，且针对发现的漏洞经过测试评估后及时进行修补。 部分符合情况：无部分符合情况。 不符合情况：未定期对设备进行漏洞扫描，且未进对发现的漏洞进行测评评估后及时进行修补。
入侵防范	[重要]f)应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。	要维护系统安全，必须进行主动监视，一般是在网络边界、 核心等重要节点处部署IDS. IPS等系统，或在防火墙、UTM房用入侵检测功能，以检查息是否发生了入侵和攻击	此项不适合，该项要求一般在服务器层面上核查	此项不适合，该项要求一般在服务器层面上核查	此项不适合，该项要求一般在服务器层面上核查
入侵防范	[关键]g)所有安全计算环境设备应全部专用化，生产设备不得进行与业务不相关的操作。（F3）	所有安全计算环境设备全部专用化，生产设备不得进行与业务不相关的操作。	1)应核查设备是否全部专用化，	当前设备统一由安全部门部署搭建，仅相关管理员拥有设备账户进行运维管理，并且无法进行与业务不相关的操作	符合情况：所有安全计算环境设备全部专用化，生产设备不得进行与业务不相关的操作 不符合情况：未对安全计算环境设备的使用进行限制，可以进行与业务不相关的操作。
入侵防范	[关键]h)应能够有效屏蔽系统技术错误信息，不得将系统产生的错误信息直接或间接反馈到前台界面。（F3）	能够有效屏蔽系统技术错误信息，不得将系统产生的错误信息直接或间接反馈到前台界面。	1)应核查是否能够有效屏蔽系统技术错误信息，不得将系统产生的错误信息直接或间接反馈到前台界面。	应用系统有效屏蔽系统技术错误信息，不得将系统产生的错误信息直接或间接反馈到前台界面	符合情况：应用系统有效屏蔽系统技术错误信息，未将系统产生的错误信息直接或间接反馈到前台界面 部分符合情况：无 不符合情况：应用系统未采用相关屏蔽技术，在系统产生的错误信息时，直接在前台界面显示
恶意代码防范	[关键]a)应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断并定期统一进行升级和更新防恶意代码库。（F3）	无论是Windows主机还是Linux主机，都面临木马、蠕虫等病毒的破坏。因此一般的主机为防范病毒，均会安装反病毒软件，或者采用可信验证机制对系统程序、应用程序等进行可信执行验证	此项不适合，该项要求一般在服务器上实现	此项不适合，该项要求一般在服务器上实现	此项不适合，该项要求一般在服务器上实现
恶意代码防范	[关键]b)应建立病毒监控中心，对网络内计算机感染病毒的情况进行监控。（F3）	建立病毒监控中心，对网络内计算机感染病毒的情况进行监控。	此项不适合，该项要求一般在服务器上实现	此项不适合，该项要求一般在服务器上实现	此项不适合，该项要求一般在服务器上实现

可信验证	[一般]a)可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	设备应作为通信设备或边界设备对待	查看设备是否具有可信根芯片	1）服务器具有可信根芯片或硬件 2)启动过程基于可信根对系统引导程序、系统程序，重要配置参数和关键应用程序等进行可信验证度量 3)在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心 4)安全管理中心可以接收设备的验证结果记录	符合情况：服务器具有可信根芯片或硬件，可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心 部分符合情况：具有可信根芯片或硬件，但未将验证结果形成审计记录送至安全管理中心 不符合情况：无可信根芯片或硬件
数据完整性	[重要]a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、重要业务数据、重要审计数据、重要配置数据.重要视频数据和重要个人信息在传输过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1)询问系统管理员，该系统的鉴别数据、重要业务数据、重要审计数据，重要配置数据，重要视频数据和重要个人信息等在传输过程中是否采用了校验技术或密码技术保证完整性 2)使用工具对通信报文中的鉴别数据、重要业务数据、重要审计数据，重要配置数据、重要视频数据和重要个人信息等进行篡改，查看是否能够检测到未知据在传输过程中的完整性受到破坏并能够及时恢	1）系统提供对鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性保护措施 2）系统检测到鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性受到被坏后采取了技术措施进行处理，如重传或其他方式	符合：系统通过https协议对传输过程中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统采取措施对传输中的数据进行完整性校验；仅包括业务数据。 不符合：系统未采取措施对传输中的数据进行完整性校验；
数据完整性	[关键]b)应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。	本条款要求对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息在存储过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施	1)询问系统管理员，是否采用校验技术或密码技术保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性 2)尝试修改存储在数据库中的鉴别数据，重要业务效据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等，查看系统反应	1)系统采用校验技术或密码技术保证了鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性 2)系统可检测到存储在数据库中的鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等被修改的行为，并具备	符合：系统通过MD5技术对存储中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过MD5技术对存储中的数据进行完整性校验；仅对鉴别数据，未包括业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行完整性校验；
数据保密性	[关键]a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。	本条款要求对鉴别数据、重要业务数据、和重要个人信息在传输过程中采取保密措施，如对这些数据加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性 2）通过嗅探等方式抓取传输过程中的数据，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理	1)系统管理员采用密码技术对鉴别数据、重要业务数据和重要个人信息进行了保密性处理 2）通过嗅探等方式抓取传输过程中的数据，未发现鉴别数据、重要业务数据和重要个人信息	符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对传

数据保密性	[关键]b)应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于系统鉴别数据、重要业务数据和个人金融信息中的客户鉴别信息以及与账号结合使用可鉴别用户身份的鉴别辅助 信息等个人敏感信息，对于其他直接反应特定自然人某些情况的信息，宜使用密码技术保护 其存储过程中的保密性。（F3）	本条款要求对鉴别数据、重要业务数据和重要个人信息在存储过程中采取保密措施，如对这些数据进行加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性 2) 核查数据库中的相关字段，查看鉴别数据、重要业务数据和重要个人信息等是否加密存储	1)系统采用了密码技术对存储在数据库中的鉴别数据、重要业务数据和重要 2)数据库中存储的鉴别数据、重要业务数据和重要个人信息等均加密存储	符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行加密；
数据备份恢复	[关键]a)应提供重要数据的本地数据备份与恢复功能，采取实时备份与异步备份或增量备份与完全备 份的方式，增量数据备份每天一次，完全数据备份可根据系统的业务连续性保障相关指（如 RPO，RTO）以及系统数据的重要程度、行业监管要求，制定备份策略。备份介质场外存放， 数据保存期限依照国家相关规定。（F3）	对数据进行备份，是防止数据遭到破坏后无法使用的最好方法。通过对数据采取不同的备份方式和形式等，保证系统重要数据在发生破坏后能够恢复。 本条款要求对应用系统的重要数据提供本地数据备份与恢复功能	1)询问数据库管理员，数据库的备份和恢复策略是什么 2)核查备份策略设置是否合理，配置是否则正确 3)核查备份结果是否与备份策略一致 4)核查近期恢复测试记录，查看是否能够进行正常的数据恢复	1)提供数据的每天全量备份《(或每天增量备份，定期全量备份) 2)近期数据库的恢复测试记录显示，能够使用备份文件进行数据恢复	符合：系统通过快照形式对应用程序进行备份，备份策略为每周2，4，6进行备份，备份保存7天，数据每天凌晨1：00全量备份； 部分符合：提供数据备份能力、未提供数据恢复功能。 不符合：系统未对应用程序及数据进行备份；
数据备份恢复	[重要]b)应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地。	应提供灾备中心， 对重要的数据提供异地数据级备份，保证当本地系统发生灾难性后果(如火灾)不可恢复时,利用异地保存的数据对系统数据能进行恢复	询问数据库管理员，是否提供异地实时备份功能，并通过网络将重要配置数据，重要业务数据实时备份至备份场地	提供异地实时备份功能，并通过网络将重要配置数据、重要业务数据实时备份至备份场地	符合：系统每周对应用程序及数据进行异地备份， 部分符合：无部分符合 不符合：未提供异地实施备份功能；
数据备份恢复	[关键]c)应提供重要数据处理系统的热冗余，保证系统的高可用性。	提供重要数据处理系统的热冗余，保证系统的高可用性。	1)应核查系统的部署方式，是否采用热冗余方式进行部署	1)对重要数据，如用户数据，鉴别数据等定期进行备份，通过磁带备份到本地 2)对于重要设备，采取热备、集群、负载均衡等高可用方式	符合情况：已提供重要数据处理系统的热冗余，如热备、集群、负载均衡等高可用方式 部分符合情况：无 不符合情况：未提供重要数据处理系统的热冗余
数据备份恢复	[关键]d)对于同城应用级灾难备份中心，应与生产中心直线距离至少达到30km，可以接管所有核心业 务的运行；对于异地应用级灾难备份中心，应与生产中心直线距离至少达到100km 。（F3）	于同城应用级灾难备份中心，应与生产中心直线距离至少达到30km，可以接管所有核心业 务的运行；对于异地应用级灾难备份中心，应与生产中心直线距离至少达到100km。	1)应核查系统是否部署灾难备份中心，生产中心与灾备中心的直线距离是否满足要求。	系统提供异地实时备份功能，并且同城灾备机房与生产中心的直线距离达到30KM以上，异地灾备中心与生产中心直线距离达到100KM以上	符合情况：系统提供异地实时备份功能，并且异地灾备机房与生产中心的直线距离达到100KM以上 部分符合情况：无 不符合情况：同城灾备中心与生产中心直线记录未达到30KM以上，或者异地灾难备份中心，与生产中心直线距离未达到100km以上
数据备份恢复	[关键]e)为满足灾难恢复策略的要求，应对技术方案中关键技术应用的可行性进行验证测试，并记录 和保存验证测试结果。（F3）	为满足灾难恢复策略的要求，应对技术方案中关键技术应用的可行性进行验证测试，并记录 和保存验证测试结果。	1)应核查是否对关键技术应用的可行性进行验证测试。 2)核查是否具备验证测试记录	1)对备份数据定期进行验证测试 2)对进行的验证测试留有相应的测试记录	符合情况：定期每季度对备份数据进行一次验证测试，并每次验证测试留有测试记录 部分符合情况：定期每季度对备份数据进行一次验证测试，但是没有测试记录 不符合情况：未定期对备份数据进行验证测试

数据备份恢复	[关键]f)数据备份应至少保存两个副本，且至少一份副本异地存放，完全数据备份至少保证以一个星 期为周期的数据冗余。（F3）	数据备份应至少保存两个副本，且至少一份副本异地存放，完全数据备份至少保证以一个星 期为周期的数据冗余。	1)应核查数据备份是否至少保存两个副本，且至少一份副本异地存放， 2)核查是否具备数据备份记录	1)对备份的数据至少保存两个版本，其中一份异地存放 2)对备份数据提供备份记录	符合情况：当前数据备份保存有两个副本，存在异地和本地备份等多种方式，分别保存在主机房和灾备机房，并且留存有数据备份记录 部分符合情况：当前数据备份保存有两个副本，存在异地和本地备份等多种方式，分别保存在主机房和灾备机房，但是未保存数据备份记录 不符合情况：备份数据未采用多副本的方式存储
数据备份恢复	[关键]g)异地灾难备份中心应配备恢复所需的运行环境，并处于就绪状态或运行状态，“就绪状态”指备份中心的所需资（相关软硬件以及数据等资源）已完全满足但设备CPU还没有运行，“运行状态”指备份中心除所需资源完全满足要求外，CPU也在运行状态。（F3）	异地灾难备份中心应配备恢复所需的运行环境，并处于就绪状态或运行状态，“就绪状态”指备份中心的所需资（相关软硬件以及数据等资源）已完全满足但设备CPU还没有运行，“运行状态”指备份中心除所需资源完全满足要求外，CPU也在运行状态。	1)应核查异地灾难备份中心是否配备恢复所需的运行环境，是否处于就绪状态或运行状态，	异地灾难备份中心已配备恢复所需的运行环境，处于就绪状态或运行状态	符合情况：异地灾难备份中心已配备恢复所需的运行环境，处于就绪状态或运行状态 部分符合情况：无 不符合情况：异地灾难备份中心未配备恢复所需的运行环境
剩余信息保护	[关键]a)应保证操作系统、数据库系统和应用系统用户鉴别信息所在的存储空间被释放或重新分配前得到完全清除，无论这些信息是存放在硬盘上还是内存中。（F3）	保证操作系统、数据库系统和应用系统用户鉴别信息所在的存储空间被释放或重新分配前得到完全清除，无论这些信息是存放在硬盘上还是内存中。	1)应核查操作系统、数据库系统和应用系统用户鉴别信息所在的存储空间被释放或重新分配前是否得到完全清除，	应用系统采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证鉴别信息存储空间被释放后得到完全清除； 部分符合：无部分符合 不符合：未采取措施保证鉴别信息存储空间被释放后得到完全清除；
剩余信息保护	[关键]b)应保证操作系统、数据库系统和应用系统用户存有敏感数据的存储空间被释放或重新分配前得到完全清除，无论这些信息是存放在硬盘上还是内存中。（F3）	保证操作系统、数据库系统和应用系统用户存有敏感数据的存储空间被释放或重新分配前得到完全清除，无论这些信息是存放在硬盘上还是内存中。	1)应核查操作系统、数据库系统和应用系统用户存有敏感数据的存储空间被释放或重新分配前是否得到完全清除	应用系统采取了措施保证对存储介质(如硬盘或内存入中的敏感数据进行及时清除，如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证敏感信息存储空间被释放后得到完全清除； 部分符合：无部分符合 不符合：未采取措施保证敏感信息存储空间被释放后得到完全清除；
个人信息保护	[关键]a)金融机构在收集、使用个人金融信息时，应遵循合法、正当、必要的原则，应以隐私政策等 方式公开收集、使用规则，向个人金融信息主体明示收集、使用信息的目的、方式和范围， 并获得个人信息主体的同意。（F3）	金融机构在收集、使用个人金融信息时，遵循合法、正当、必要的原则，应以隐私政策等 方式公开收集、使用规则，向个人金融信息主体明示收集、使用信息的目的、方式和范围， 并获得个人信息主体的同意。	1)应核查在收集、使用个人金融信息时，是否遵循合法、正当、必要的原则，是否以隐私政策等 方式公开收集、使用规则，向个人金融信息主体明示收集、使用信息的目的、方式和范围， 并获得个人信息主体的同意。	1）记录数据库所存储的个人信息。如数据库存储了用户身份证号、电话等个人信息 2)记录数据库哪个功能模块使用哪些用户个人信息，以及所使用个人信息的必要性	符合情况：数据库所存储的用户个人信息均为业务所必需的，不存在非必要用户个人信息 部分符合情况：无 不符合情况：数据库违规保存非业务必需的用户个人信息

个人信息保护	[关键]b)应仅采集和保存业务必需的用户个人金融信息。（F3）	仅采集和保存业务必需的用户个人金融信息。	1)应核查是否仅采集和保存业务必需的用户个人金融信息。	1)系统采取了措施控制了数据库账户对个人信息的访问，如权限控制等 2)未授权无法访问和使用用户的个人信息	符合情况：系统已采取措施限制了数据库账户对个人信息的访问，非授权用户无法访问和使用用户的个人信息，且已制定相关个人信息保护制度 部分符合情况：无 不符合情况：未对用户个人信息的访问和使用进行严格的管理，未采取措施来禁止非授权访问和非法使用个人信息
个人信息保护	[关键]c)应根据“业务需要”和“最小权限”原则，进行个人金融信息相关权限管理，严格控制和分 配相关操作权限，应禁止未授权访问和非法使用用户个人金融信息。（F3）	根据“业务需要”和“最小权限”原则，进行个人金融信息相关权限管理，严格控制和分 配相关操作权限，应禁止未授权访问和非法使用用户个人金融信息。	1)应核查是否根据“业务需要”和“最小权限”原则，进行个人金融信息相关权限管理，	1)根据数据库访问规则限制了数据库用户仅能对自身权限范围内的表进行操作和访问，禁止非授权访问和非法使用个人金融信息	符合情况：根据数据库访问规则限制了数据库用户仅能对自身权限范围内的表进行操作和访问，禁止非授权访问和非法使用个人金融信息 部分符合情况：无 不符合情况：未对个人信息管理权限进行划分
个人信息保护	[关键]d)金融机构应依据 JR/T 0171—2020 对个人金融信息收集、传输、存储、使用、删除、销毁等 处理的整个过程进行管理与控制，并对个人金融信息生命周期过程进行安全检查与评估。（F3）	金融机构应依据 JR/T 0171—2020 对个人金融信息收集、传输、存储、使用、删除、销毁等 处理的整个过程进行管理与控制，并对个人金融信息生命周期过程进行安全检查与评估。	1)应核查是否依据 JR/T 0171—2020 对个人金融信息收集、传输、存储、使用、删除、销毁等 处理的整个过程进行管理与控制，	依据 JR/T 0171—2020 对个人金融信息收集、传输、存储、使用、删除、销毁等 处理的整个过程进行管理与控制	符合情况：依据 JR/T 0171—2020 对个人金融信息收集、传输、存储、使用、删除、销毁等 处理的整个过程进行管理与控制 部分符合情况：无 不符合情况：未对个人金融信息收集、传输、存储、使用、删除、销毁等 处理的整个过程进行管理与控制
个人信息保护	[关键]e)金融机构应依据国家与行业主管部门要求，对通过计算机屏幕、客户端软件、银行卡受理设 备、ATM 设备、自助终端设备、纸（如受理终端打印出的支付交易凭条等交易凭证）等界面 展示的个人金融信息，应采取字段屏蔽（或截词）等处理措施，降低个人金融信息在展示环 节的泄露风险。（F3）	金融机构依据国家与行业主管部门要求，对通过计算机屏幕、客户端软件、银行卡受理设 备、ATM 设备、自助终端设备、纸（如受理终端打印出的支付交易凭条等交易凭证）等界面 展示的个人金融信息，应采取字段屏蔽（或截词）等处理措施，降低个人金融信息在展示环 节的泄露风险。	1)应核查是否依据国家与行业主管部门要求，对通过计算机屏幕、客户端软件、银行卡受理设 备、ATM 设备、自助终端设备、纸（如受理终端打印出的支付交易凭条等交易凭证）等界面 展示的个人金融信息，采取字段屏蔽（或截词）等处理措施，	应依据国家与行业主管部门要求，对通过计算机屏幕、客户端软件、银行卡受理设 备、ATM 设备、自助终端设备、纸（如受理终端打印出的支付交易凭条等交易凭证）等界面 展示的个人金融信息，采取字段屏蔽（或截词）等处理措施，	符合情况：已对计算机屏幕、客户端软件、银行卡受理设 备、ATM 设备、自助终端设备、纸（如受理终端打印出的支付交易凭条等交易凭证）等界面展示的个人金融信息，采取字段屏蔽（或截词）等处理措施 部分符合情况：无 不符合情况：未对计算机屏幕、客户端软件、银行卡受理设备、ATM 设备、自助终端设备、纸（如受理终端打印出的支付交易凭条等交易凭证）等界面 展示的个人金融信息，采取字段屏蔽（或截词）等处理措施

个人信息保护	[关键]f)应向个人金融信息主体告知共享、转让个人金融信息的目的、数据接收方的身份和数据安全 保护能力，并事先征得个人金融信息主体明示同意，共享、转让经去标识化处理的个人金融 信息，且确保数据接收方无法重新识别个人金融信息主体的除外。（F3）	向个人金融信息主体告知共享、转让个人金融信息的目的、数据接收方的身份和数据安全 保护能力，并事先征得个人金融信息主体明示同意，共享、转让经去标识化处理的个人金融 信息，且确保数据接收方无法重新识别个人金融信息主体的除外。	1)应核查是否向个人金融信息主体告知共享、转让个人金融信息的目的、数据接收方的身份和数据安全保护能力，	在发生共享、转让个人金融信息时应向个人金融信息主体告知转让个人金融信息的目的、数据接收方的身份和数据安全保护能力	符合情况：在发生共享、转让个人金融信息时，应向个人金融信息主体告知转让个人金融信息的目的、数据接收方的身份和数据安全保护能力 部分符合情况：无 不符合情况：在发生共享、转让个人金融信息时，未告知个人金融信息主体 不适用情况：数据库中收集的个人金融信息，只在单位内部管理员使用，不存在将个人金融信息转让或共享的情况
个人信息保护	[关键]g)开发环境、测试环境不应使用真实的个人金融信息，应使用虚构的或经过去标识化处理的个 人金融信息，账号、卡号、协议号、支付指令等测试确需除外。（F3）	开发环境、测试环境不应使用真实的个人金融信息，应使用虚构的或经过去标识化处理的个 人金融信息，账号、卡号、协议号、支付指令等测试确需除外。	1)应核查开发环境、测试环境是否使用真实的个人金融信息，是否使用虚构的或经过去标识化处理的个人金融信息，账号、卡号、协议号、支付指令等测试确需除外。	在开发环境、测试环境未使用真实的个人金融信息，使用虚构的或经过去标识化处理的个人金融信息，账号、卡号、协议号、支付指令等测试确需除外。	符合情况：在开发环境、测试环境未使用真实的个人金融信息，使用虚构的或经过去标识化处理的个 人金融信息，账号、卡号、协议号、支付指令等测试确需除外。 部分符合情况：无 不符合情况：在开发环境、测试环境中使用真实的个人金融信息，未做虚构或去标识化处

安全管理中心（S3A3G3）作业指导书					
安全控制点	**检测项**	**要求解读**	**测评方法**	**预期结果或主要证据**	**符合情况**
系统管理	[重要]a)应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计。	要求对系统管理员进行身份认证并严格限制系统管理员账户的管理权限，仅允许系统管理员通过特定方式进行系统管理操作,并对所有操作进行详细的审计记录	1)应核查是否对系统管理员进行身份鉴别 2)应核查是否只允许系统管理员通过特定的命令或操作界面进行系统管理操作 3应核查是否对系统管理操作进行审计	1)对管理员的登录进行认证 2)使用了管理工具或特定命令 3)所有操作有日志记录	符合情况：对管理员的登录进行认证；使用了管理工具或特定命令；所有操作有日志记录。 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足
系统管理	[一般]b)应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。	系统管理操作应由管理员完成，其管理、操作内容应不同于审计管理员和安全管理员	应核查是否通过系统管理员对系统的资源和运行进行配置、控制和管理,包括用户身份、、系统资源配置、系统加载和启动，系统运行的异常处理、数据和设备的备份与恢复等	1)管理员有权限划分 2)权限不同于审计管理员和安全管理员	符合情况：管理员有权限划分；权限不同于审计管理员和安全管理员。 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足
系统管理	[关键]c)应每月对设备的配置文件进行备份，发生变动时应及时备份。（F3）	每月对设备的配置文件进行备份，发生变动时应及时备份。	1)应核查是否每月对设备配置文件进行备份。 2)应核查设备配置变动时是否及时进行备份。	1每月对设备配置文件进行备份。 2设备配置变动时及时进行备份。	符合情况：每月对设备配置文件进行备份。设备配置变动时及时进行备份。 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足
系统管理	[关键]d)应使用自动化技术手段对设备运行状况进行实时监测，运维人员应每天定期查看并记录系统 运行状况。（F3）	需要使用自动化技术手段对设备运行状况进行实时监测，运维人员需要每天定期查看并记录系统 运行状况。	1)应核查系统是否部署性能监控系统。 2)应核查管理员对性能监控记录的处理方式，是否具备处理记录。	1系统部署性能监控系统。 2管理员对性能监控记录进行分析处理，并有处理记录	符合情况：系统部署性能监控系统。管理员对性能监控记录进行分析处理，并有处理记录 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足
系统管理	[关键]e)应每季度检验网络设备软件版本信息，并通过有效测试验证后进行相应的升级，同时留存测 试验证相关记录。（F3）	需要每季度检验网络设备软件版本信息，并通过有效测试验证后进行相应的升级，同时留存测 试验证相关记录。	1)应核查是否每季度检验网络设备软件版本信息。 2)应核查是否经过有效测试验证后再进行升级。 3)应核查是否具备测试验证记录。	1每季度检验网络设备软件版本信息。 2经过有效测试验证后再进行升级。 3具备测试验证记录。	符合情况：每季度检验网络设备软件版本信息。经过有效测试验证后再进行升级。具备测试验证记录。 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。

审计管理	[重要]a)应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计。	要求对审计管理员进行身份认证并严格限制审计管理员账户的管理权限，仅允许管理员通过特定方式进行审计管理操作,并对所有操作进行详细的审计记录	1)应核查是否对审计管理员进行身份鉴别 2)应核查是否只允许审计管理员通过特定的命令或操作界面进行安全审计操作 3)应核查是否对安全事代操作进行审计	1)对管理员的登录进行认证 2）使用了管理工具或特定命令 3)所有操作有日志记录	符合情况：对管理员的登录进行认证；使用了管理工具或特定命令；所有操作有日志记录。 部分符合情况：满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足
审计管理	[一般]b)应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。	针对综合安全审计系统、数据库审计系统等提供集中审计功能的系统，要求对审计管理员进行授权，并通过审计管理员对审计记录应进行分析	应核查是否通过审计管理员对审计记录进行分析,并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等	1)管理员有权限划分 2)权限不同于系统管理员和安全管理员 3)只有审计管理员可以查看审计分析数据	符合情况：管理员有权限划分；权限不同于系统管理员和安全管理员；只有审计管理员可以查看审计分析数据； 部分符合情况：满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足
审计管理	[关键]c)应严格限制审计数据的访问控制权限，限制管理用户对审计数据的访问，实现管理用户和审 计用户的权限分离，避免非授权的删除、修改或覆盖。（F3）	需要严格限制审计数据的访问控制权限，限制管理用户对审计数据的访问，实现管理用户和审 计用户的权限分离，避免非授权的删除、修改或覆盖。	1)应核查是否对管理员账户的权限进行限制，是否只有审计管理员具备审计数据的访问操作权限。是否已实现管理用户和审计用户的权限分离。	对管理员账户的权限进行限制，只有审计管理员具备审计数据的访问操作权限。实现管理用户和审计用户的权限分离。	符合情况：对管理员账户的权限进行限制，只有审计管理员具备审计数据的访问操作权限。实现管理用户和审计用户的权限分离。 部分符合情况：/ 不符合情况：上述条件全不满足。
安全管理	[重要]a)应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计。	要求对安全管理员进行身份认证并严格限制系统管理员账户的管理权限，仅允许安全管理员通过特定方式进行系统管理操作,并对所有操作进行详细的审计记录	1)应核查是否对安全管理员进行身份鉴别 2)应核查是否只允许安全管理员通过特定的命令或操作界面进行系统管理操作 3应核查是否对安全管理操作进行审计	1对管理员的登录进行认证 2)使用了管理工具或特定命令 3)所有操作有日志记录	符合情况：对管理员的登录进行认证；使用了管理工具或特定命令；所有操作有日志记录。 部分符合情况：满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足
安全管理	[一般]b)应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。	针对提供集中安全管理功能的系统，要求对安全管理员进行授权，并通过安全管理员部署安全组件或安全设备的安全策略	应核查是否通过安全管理员对系统中的安全策略进行配置，包括安全参数、主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等	1)管理员有权限划分 2)权限不同于系统管理员和审计管理员: 3)只有安全管理员可以配置安全策略有关的参数	符合情况：管理员有权限划分；权限不同于系统管理员和审计管理员；只有安全管理员可以配置安全策略有关的参数。 部分符合情况：满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足

集中管控	[关键]a)应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控。	应在网络中独立配置一个网络区域，用于部署集中管控措施。集中管控措施包括:集中监控系统、集中审计系统和集中安管系统等，通过这些集中管控措施实现对整个网络的集中管理	1)应核查是否划分出单独的网络区域用于安全管理 2)应核查是否各个安全设备或安全组件的配置等管理均由管理区的设备进行	1)网络拓扑图中有管理区 2)安全设备或组件的管理设备均在管理区	符合情况：网络拓扑图中有管理区；安全设备或组件的管理设备均在管理区。 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。
集中管控	[关键]b)应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理。	为了保障网络中信息传输的安全性，应采用安全方式对设备或安全组件进行管理	应核查是否采用安全方式(如SSH、HTTPS IPSec VPN等)对安全设备或安全组件进行管理，或者是否使用独业的带外管理网络对安全设备或安全组件进行管理	采用安全方式对设备进行访问，并对配置信息进行记录，例如: ssh server enable ssh user cssnet service-type stelnet authentication-type password	符合情况：采用安全方式对设备进行访问，并对配置信息进行记录。 不符合情况：未采用安全方式对设备进行访问，并对配置信息进行记录。
集中管控	[重要]c)应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测。	为了保障业务系统的正常运行，应在网络中部署具备运行状态监测功能的系统或设备，对网络链路、网络设备、安全设备、服务器及应用系统的运行状态进行集中、实时监控	1)应核查是否部署了具备运行状态监测功能的系统或设备，能够对网络链路、安全设备1)网络设备和服务器等的运行状况进行集中监测 2)应测试验证运行状态监测系统是否根据网络链路、安全设备、网络设备和服务器等的工作状态、依据设定的阀值(或默认阀值)实时报警	具备设备监测功能的系统或平台	符合情况：具备设备监测功能的系统或平台 不符合情况：未具备设备监测功能的系统或平台
集中管控	[关键]d)应对分散在各个设备上的安全事件、审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求。（F3）	部署集中审计分析系统，实现对基础网络平台及其上运行的各类型设备进行信息日志收集、 存储，并定期进行审计分析，从而发现潜在的安全风险。日志存储时间应符合法律法规要求，目前网络安全法要求日志保存时间不少于6个月	1)应核查各个设备是否配置并启用了相关策略，将审计数据发送到独立于设备自身的外部集中安全审计系统中 2)应核查是否部署统一的集中安全审计系统,统一收集和存储各设备日志，并根据需要进行集中审计分析 3)应核查审生记录的留带时间是否为6个月	1） 设备日志进行了转发 2)平台具备审计分析功能 3)审计记录保有了至少6个月以上	符合情况：设备日志进行了转发；平台具备审计分析功能；审计记录保有了至少6个月以上。 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。
集中管控	[重要]e)应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理。	在安全管理区域部署集中管理措施，应实现对各类型设备(如:防火墙、IPS、IDS. WAF等)安全策略的统一管理,应实现对网络恶意代码防护设备、主机操作系统恶意代码防护软件、病毒规则库的统一升级，应实现对各类型设备(如:主机操作系统、数据库操作系统等)的补丁升级进行集中管理等	1)应核查是否能够对安全策略(如防火墙访问控制策略、入侵保护系统防护策略、WAF安全防护策略等)进行集中管理 2)应核查是否实现对操作系统防恶意代码系统及网络恶意代码设备的集中管理 3） 实现对防恶意代码病毒规则库的统一升级和管理	1） 具有统一策略管理平台或多个(比如防火墙、IPS、 IDS. WAF等安全设备)分别策略管理的工具 2)通过平台或工具可以实施策略管理	符合情况：具有统一策略管理平台或多个(比如防火墙、IPS、 IDS. WAF等安全设备)分别策略管理的工具；通过平台或工具可以实施策略管理。 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足

集中管控	[关键]f)应能对网络中发生的各类安全事件进行识别、报警和分析、响应和处置。（F3）	能够通过集中管控措施，对基础网络平台范围内各类安全事件（如设备故障、恶意攻击、服务性能下降等）进行实时的识别和分析，并通过声、光、短信、邮件等措施进行实时报警	1)应核查是否部署了相关系统平台够对各类安全事传进行分析并通过声、光等方式实时报警 2)应核查监测范围是否能够覆盖网络所有可能的安全事件	1)具有安全事件管理平台或工具 2)相关平台或工具收集足够的可能安全事件，并具备报警提示功能	符合情况：具有安全事件管理平台或工具；相关平台或工具收集足够的可能安全事件，并具备报警提示功能。 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。
集中管控	[关键]g)应具有对高频度发生的相同安全事件进行合并告警，避免出现告警风暴的能力。（F3）	需要具有对高频度发生的相同安全事件进行合并告警，避免出现告警风暴的能力。	2)应核查针对高频度发生的相同安全事件是否具有合并告警功能。	针对高频度发生的相同安全事件具有合并告警功能。	符合情况：针对高频度发生的相同安全事件具有合并告警功能。 部分符合情况：/ 不符合情况：上述条件全不满足。

安全管理制度（S3A3G3）作业指导书					
安全控制点	检测项	要求解读	测评方法	预期结果或主要证据	符合情况
安全策略	[关键]a)应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框 架等，并编制形成网络安全方针制度文件。（F3）	网络安全工作的总体方针和安全策略文件作为机构网络安全工作的总纲，一般明确了网络安全工作的总体目标、原则、需遵循的总体策略等内容。可以以单一的文件形式发布， 也可与其他相互关联的文件作为一套文件发布	1)核查是否具有总体方针和策略文件 2)核查该文件是否明确了机构安全工作的总体目标，范围、原则和各类安全策略。 -般来讲，该策略文件中可以明确网络安全管理活动的责任部门或人员、也可覆盖到等级保护对象生命周期中所有关键的安全管理活动。其中安全管理框架应包括组织机构及岗位职责，人员安全管理、环境和资产安全管理、系统安全建设管理系统安全运行管理、事件处置和应急响应等方面，明确各个方面的职责分工，需要关注的管理活动、管理活动的控制方法等	1)机构具有网络安全方针和策略文件 2)文件明确了机构网络安全工作的总体目标、范围、原则和安全策略	符合情况：已制定《XXXXX信息安全方针》，制度中明确了网络安全工作的总体目标、适用范围、基本原则和安全框架体系等内容。 部分符合情况：已制定《XXXXX信息安全方针》，但文件中如未明确机构网络安全工作范围。 不符合情况：XXX公司未制定网络安全工作总体方针和安全策略文件，不具备网络安全管理体系等顶层构建
管理制度	[重要]a)应对安全管理活动中的各类管理内容建立安全管理制度。	具体的安全管理制度在安全方针策略文件的基础上，根据实际情况建立。可以由若干的制度构成，或若干个分册构成。可能覆盖机房安全管理、办公环境安全管理、网络和系统安全管理供应商管理、变更管理、备份和恢复管理、软件开发管理等方面，可以在每个制度文档中明确该制度的使用范围、目的、需要规范的管理活动、具体的规范方式和要求	1）核查是否有安全管理制度 2)核查制度是否覆盖机构和人员、物理和环境、安全建设和安全运维等层面的管理内容	1)建立了安全管理制度 2)安全管理制度覆盖了物理和环境、机构和人员、安全系统建设和安全运维等层面的管理内容	符合情况：已制定《XXX公司网络安全管理规定》、《XXX公司系统安全管理规定》、《XXX公司数据安全管理规定》等制度，相关制度中包含物理和环境、机构和人员、服务器运维、系统运维、系统数据安全等管理内容，具备相关表单。 部分符合情况：已制定《XXX公司网络安全管理规定》，但未覆盖安全建设和安全运维等层面的管理内容。 不符合情况：XXX公司未制定安全管

管理制度	[重要]b)应对管理人员或操作人员执行的日常管理操作建立操作规程。	安全操作规程是指各项具体活动的步骤或方法，可以是一个操作手册，一个流程表表单或一个实施方法，但必须能够明确体现或执行网络安全策略或网络安全所要求的策略或原则。配置规范指的是重要等级保护对象中部署的关键网络安全设备、主机操作系统、数据库管理系统等的安全配置规范。这些操作设备和安全配置规范可以应用于那些需要安装或配置计算机的用户。许多组织机构都应有书面规程规定应该如何安装操作系统，如何建立新用户账户，如何分配计算机权限，如何进行事件报告等等	核查是否具有日常管理操作规程，如系统维护手册和操作规程等（包括网络设备、安全设备、操作系统等的配置规范）	1）具有日常管理操作的操作规程 2)操作规程覆盖了物理环境、网络和通信、设备和计算、应用和数据层面的重要操作规程（如系统维护手册和操作规程）	符合情况：已制定《XXX公司安全策略管理规定》、《XXX公司网络安全管理规定》、《XXX公司系统安全管理规定》、《XXX公司数据安全管理规定》等制度，相关制度中包含对系统维护、系统配置、用户操作等方面的规定，具备相关维护记录、操作等表单记录。 部分符合情况：已制定《XXX公司操作手册》，但未覆盖XXX层面等。 不符合情况：XXX公司未对管理人员或操作人员执行的日常管理操作建立
管理制度	[重要]c)应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。	全面的安全管理制息体系包括网络安全工作的总体方针策略、各种安全管理活动的管理制度、日常操作行为的操作规程以及各类记录表单共同构成“金字塔”式结构	1)核查是否具有总体方针策略文件、管理制度，操作规程和记录表单等 2)核查管理体系各要素之间是否具有连贯性 一般情况下，一套全面的安全管理制度体系最常见的为4层架构，即由网络安全工作的总体方针策略，各种安全管理活动的管理制度、日常操作行为的操作规程和安全配置规范和各类记录表单	1) 有方针策略 2）有各项管理制度 3) 有操作规程 4）123有层次关系和内在逻辑联系。	符合情况：制定《XXXX公司信息安全管理制度》，形成全面的信息安全管理制度体系，由管理制度、操作规程构成，具备各个操作规程以及记录表单格式。 部分符合情况：已制定《XXXX公司信息安全管理制度》，但其中未包含操作规程。 不符合情况：XXX公司未形成由安全策略、管理制度、操作规程、记录表单等构成的信息安全管理制度体系

制定和发布	[关键]a)金融机构总部应负责制定适用全机构范围的安全管理制度，各分支机构应制定适用辖内的安 全管理制度。（F3）	金融机构总部应负责制定适用全机构范围的安全管理制度，各分支机构应制定适用辖内的安全管理制度。	1)核查是否由金融机构总部负责制定适用全机构范围的安全管理制度。	1) 安全管理制度在金融机构总部的总体负责下统一制定。 2) 制定了适用辖内的安全管理制度。	符合情况：通过xxx总部进行金融相关管理制度的统一制定和管理，当前已制定相关XXX制度等适用于各分支机构。 部分符合情况：未通过xxx总部进行金融相关管理制度的统一制定和管理，但当前已制定相关XXX制度等适用于各分支机构。 不符合情况：未通过xxx总部进行金融相关管理制度的统一制定和管理，未制定相关XXX制度等适用于各分支机构
制定和发布	[一般]b)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。	安全管理制度的制定和发布，应在相关部门的负责和指导下，严格按照制度制定的有关程序和方法，规范起草、论证、审定和发布等主要环节	1)访谈安全主管或配合人员，询问由什么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 2)核查人员职责、岗位设置等相关管理制度文件,或者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	1)有指定部门或人员负责安全管理制度的制定 2)相关职责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	符合情况：已在《XXXX制度》中指定XXX部负责安全管理制度的制定。 部分符合情况：已指定XXX部负责安全管理制度的制定，但无相关职责文件。 不符合情况：XXX公司未指定或授权专门的部门或人员负责安全管理制度的制定工作。

制定和发布	[一般]c)安全管理制度应通过正式、有效的方式发布，并进行版本控制。	正式、有效的发布方式，原则是机构所认可的有效的发布方式,且在有效范围内由相关部门发布即可，如:正式发文发布、内部OA发布、邮件发布、即时通讯发布等方式，不必拘泥具体的形式。	1核查制度制定和发布要求管理文档是否说明安全管理制度的制定和程序，格式要求及版本编号等相关内容 2)核查安全管理制度的收发登记记录是否通过正式、有效的方式收发，如正式发文、领导签署和单位盖章等，是否注明发布范围	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	符合情况：已制定《XXX制度》，要求所有安全管理制度均通过纸质文件正式下发至各部门/通过企业OA系统进行正式发布，且进行了版本控制，具有版本标识等。 部分符合：已制定《XXX制度》，但文档内容未覆盖安全管理制度制定和发布程序。 不符合情况：XXX公司安全管理制度均未通过正式、有效的方式发布。
评审和修订	[重要]a)应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。	安全管理制度的定期评审和修订主要考虑:制度体系整体性是否合理；体系各要素(如安全策略、管理制度或操作规程等)是否合理	1)访谈信息/网络安全主管是否定期对安全管理制度体系的合理性和适用性进行审定 2）核查是否具有安全管理制度的审定或论证记录，如果对制度做过修订，核查是否有修订版本的安全管理制度 安全管理制度体系涉及从上层方针到管理制度再到操作规程等整个单位等保护对象安全相关的所有文件，这里的定期一般可以为一年，具体可根据组织情况进行约定，但是，一旦发生可能引起安全管理制度不适用的事件时应该主动对安全管理制度进行检查和审定，发现不足及时修订	1)具有安全管理制度的核查或评审记录 2)如果有修订版本，具有修订版本的安全管理制度，修订内容与评审记录中保持一致	符合情况：已制定《XXX公司规章制度管理办法》、《XXX公司信息安全内部审核管理办法》，制度中要求由XXX部门每年对制度进行评审修订，且具备制度修订记录《XXXX》。 部分符合情况：制定《XXX公司规章制度管理办法》、《XXX公司信息安全内部审核管理办法》，制度中要求由XXX部门每年对制度进行评审修订，未查看到评审记录。 不符合情况：XXX公司未对安全管理制度的合理性和适

安全管理机构（S3A3G3）作业指导书					
安全控制点	检测项	要求解读	测评方法	预期结果或主要证据	符合情况
岗位设置	[关键]a)网络安全管理工作应实行统一领导、分级管理，总部统一领导分支机构的网络安全管理，各机构负责本单位和辖内的网络安全管理。（F3）	网络安全管理工作需要实行统一领导、分级管理，总部统一领导分支机构的网络安全管理，各机构负责本单位和辖内的网络安全管理。	1)访谈网络安全管理工作是否由总部统一领导，各机构负责本单位和辖内的网络安全管理。	1)机构成立了网络安全工作委员会或领导小组,且有明确的文件明确其组成机构及工作职责 2)具有由单位主管领导委任或授权的相关文件	符合情况：《XXX公司信息安全方针》中已明确成立了网络安全工作领导小组，明确了人员构成情况和相关职责，同时已明确其最高领导由XXX部门领导担任，组长为XXX，组员为XXX。 部分符合情况：《XXX公司信息安全方针》中已明确成立了网络安全工作领导小组，明确了人员构成情况，同时已明确其最高领导由XXX部门领导担任，组长为XXX，组员为XXX，但相关职责不明确。 不符合情况：XXX公司未成立指导和管理网络安全工作的委员会或领导小组。
岗位设置	[关键]b)应设立由本机构领导、业务与技术相关部门主要负责人组成的网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权，负责协调本机构及辖内网络安全管理工作，决策本机构及辖内网络安全重大事宜。（F3）	为保证安全管理工作的有效实施，应设立指导和管理网络安全工作的委员会或领导小组，负责单位网络安全管理的全局工作，是网络安全组织的最高管理层	1)访谈信息7网络安全官是否成立了指导和管理网络安全工作的委员会或领导小组 2)核查部门职责文档是否明确了网络安全工作委员会或领导小组构成情况和相关职责 3)核查相关委任授权文件是否明确其最高领导由单位主管领导委任或授权 一般情况下，一个机构成立了指导和管理网络安全工作的委员会或领导小组，均需有正式的发文 通常，在单位的内部结构上建立一整套从单位最高管理层(网络安全领导小组并且由单位最高领导委任或授权)到执行管理层(网络安全管理工作职能部门及安全主管)以及系统日常运营层(系统管理员、网络管理员、安全管理员等) 的三层及金字塔式的管理结构来约束和保证各项安全管理措施的执行。网络安全领导小组主要的职责包括对安全管理制度体系合理性和适用性的审定、对机构内关键网络安全工作进行授权和审批等,但其最主要的是负责单位网络安全管理的全局工作:网络安全管理职能部门的主要职责是对机构内重要网络	1) 成立了由本机构领导、业务与技术相关部门主要负责人组成的 指导和管理网络安全工作的委员会或领导小组。 2) 有网络安全工作委员会或领导小组构成情况和相关职责的文档。 3) 委员会或领导小组的最高领导是谁。	符合情况：已成立了由本机构领导、业务与技术相关部门主要负责人组成的指导和管理网络安全工作的委员会或领导小组，且具备领导小组职责划分文档，文档中明确了小组构成和相关职责，由XXX担任小组领导，为单位XXX职务。 部分符合情况：已成立了由本机构领导、业务与技术相关部门主要负责人组成的指导和管理网络安全工作的委员会或领导小组，未制定领导小组职责划分文档，文档中明确了小组构成和相关职责，由XXX担任小组领导，为单位XXX职务。 不符合情况：未成立了由本机构领导、业务与技术相关部门主要负责人组成的指导和管理网络安全工作的委员会或领导小组，且无领导小组职责划分文档，文档中明确了小组构成和相关职责

岗位设置	[关键]c)应设立网络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。	网络安全管理工作的职能部门是机构的执行管理层，一般负责对网络安全管理工作的授权和审批，内部相关业务部门和安全管理部门之间的沟通协调以及与机构外部单位的合作，定期对系统的安全措施落实情况进行检查，系统安全运行维护管理工作	1)访谈信息/网络安全主管，是否设立了网络安全管理职能部门和各方面负责人(如机房负责人、系统运维负责人，系统建设负责人等) 2)核查部门职责文档是否明确网络安全管理工作的职能部门和各负责人职责 “安全主管“一般是一个单位安全管理工作的主要责任人，全面负责等级保护对象安全规划、建设、运行维护等安全管理工作，一般由单位的高层或某一部门的主管担任。“安全管理各方面的负责人”一般包括物理安全负责人(其是保护等级保护对象物理进行环境和办公环境安全的责任人），系统建设方面负责人(其是保证等级保护对象安全规划、建设、工程实施过程的责任人)和系统运行维护方面的责任人(其是保证等级保护对象日常运行安全	1)机构设立了网络安全管理职能部门，并指定了各部门负责人 2)具有明确的职责文件明确部门和负责人的工作职质	符合情况：已指定由XXX部门担任网络安全管理工作的职能部门，且具备人员职责划分文档，文档中明确了部门及各个工作岗位的职责。 部分符合情况：已指定由XXX部门担任网络安全管理工作的职能部门，但未设立安全管理各个方面的负责人岗位，未定义各负责人的职责。 不符合情况：
岗位设置	[重要]d)应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。	系统管理员、网络管理员、安全管理员等为机构的日常运营层， 主要负责具体落实各项网络安全等级保护工作具体要求，负责日常的具体安全维护工作	1)访谈信息/网络安全主管是否设立了系统管理员、网络管理员和安全管生员等岗位 2)核查岗位职责文档是否明确了各岗位职责	1）机构设立了系统管理员、网络管理员、安全管理员岗位， 2）具有明确的各岗位职责说明文档	符合情况：XXX公司已进行安全管理岗位的划分，包括网络管理员、系统管理员、安全管理员等管理岗位，且具备人员职责划分文档，文档中明确了部门及各个工作岗位的职责。 部分符合情况：管理员岗位设立不完善，如当前实际情况缺失审计管理员等。 不符合情况：XXX公司未进行安全管理岗位的划分，未设置审计管理员、安全管理员等相关管理岗位。
岗位设置	[关键]e)应设立专门的网络安全审计岗位，负责网络安全审计制度和流程的实施，制订和执行网络安 全审计计划，对网络安全整个生命周期和重大事件等进行审计。（F3）	需要设立专门的网络安全审计岗位，负责网络安全审计制度和流程的实施，制订和执行网络安 全审计计划，对网络安全整个生命周期和重大事件等进行审计。	1)访谈是否设立专门的网络安全审计岗位。 2)核查岗位职责文档是否明确了各岗位职责	1) 设立了专门的网络安全审计岗位。 2) 具有明确了网络安全岗位的职责的说明文档。	符合情况：XXX公司已设置网络安全审计岗位，且具备人员职责划分文档，文档中明确了部门及各个工作岗位的职责。 部分符合情况：管理员岗位设立不完善，如当前实际情况缺失审计管理员等。 不符合情况：XXX公司未进行网络安全审计管理员岗位。

岗位设置	[关键]f)应坚持三分离原则，实现前后台分离、开发与操作分离、技术与业务分离，信息科技人员任 职要专岗专责，不得由业务人员兼任，也不得兼任业务职务。（F3）	坚持三分离原则，实现前后台分离、开发与操作分离、技术与业务分离，信息科技人员任 职要专岗专责，不得由业务人员兼任，也不得兼任业务职务。	1)访谈是否实现前后台分离、开发与操作分离、技术与业务分离，信息科技人员任职要专岗专责，不得由业务人员兼任，也不得兼任业务职务。 2)核查岗位职责文档是否明确了各岗位职责	1) 前后台分离、开发与操作分离、技术与业务分离。 2)具有岗位职责文档，明确了信息科技人员任职要专岗专责，不得由业务人员兼任，也不得兼任业务职务。	符合情况：XXX公司已对各项业务进行分离，具有岗位职责文档说明了专岗专责以及不得兼任岗位。 部分符合情况：XXX公司未对各项业务进行分离，但具有岗位职责文档说明了专岗专责以及不得兼任岗位。。 不符合情况：XXX公司未对各项业务进行分离，无相关岗位职责文档对了专岗专责以及不得兼任岗位等情况进行说明。
岗位设置	[关键]g)除网络安全管理部门外，其他部门均应指定至少一名网络安全员，协助网络安全管理部门开 展本部门的网络安全管理工作。（F3）	除网络安全管理部门外，其他部门均需要指定至少一名网络安全员，协助网络安全管理部门开 展本部门的网络安全管理工作。	1)访谈是否除网络安全管理部门外，其他部门均指定至少一名网络安全员 2)核查岗位职责文档是否明确了各岗位职责	1) 网络安全管理部门外的其他部门指定至少一名部门网络安全员。 2) 岗位职责文档明确了部门网络安全员需协助网络安全管理部门开展本部门的网络 安全管理工作。	符合情况：各部门至少指定了一位网络安全员，并在公司XXX中说明了相关网络安全员的职责。 部分符合情况：各部门未指定网络安全员，制定了公司XXX制度说明了相关网络安全员的职责。 不符合情况：各部门未指定网络安全员，未制定XXX制度说
人员配备	[重要]a)应配备一定数量的系统管理员、审计管理员和安全管理员等。	由于部分岗位人员拥有关键的操作权限，为避免人员失误或渎职现象的发生，应配备一定数量的安全管理人员，如系统管理员、审计管理员和安全管理员等	1)访谈信息/网络安全主管各个安全管理岗位人员配备情况 2) 核查管理人员名单，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. 3)与技术核查结合，各个岗位是否根据管理人员名单予以授权，如主机核查时系统管理员是否和管理人员名单一致	1)人员配备文档中明确了各岗位人员的配备人员及数量 2)管理人员名单中明确机房管理员、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 3)各个岗位根据管理人员名单任职	符合情况：XXX公司实际已配备相应的网络管理员、系统管理员、安全管理员，当前配备有网络管理员1名，安全管理员1名等。 部分符合情况：XXX公司实际已配备相应的网络管理员、系统管理员、安全管理员，当前配备有网络管理员1名，安全管理员1名等，但授权管理人员名单与实际管理人员不一致。 不符合情况：XXX公司仅配备一位系统管理员，无审计管理员及安全管理员，人员配备不完善。
人员配备	[关键]b)应配备专职安全管理员，实行A、B岗制度，不可兼任。（F3）	安全管理员不能兼任其他与等级保护对象相关的管理岗位，如系统管理员、网络管理员等	1）访谈安全主管，询问安全管理员的配备情况，是否是专职 2)核查管理人员名单，确认安全管理员是否是专职人员	1）人员配备文档表明安全管理员没有兼任系统管理员、 网络管理员等，并实行ab岗。 2）没有兼职干别的活。	符合情况：XXX公司已配备专职安全管理员，不存在兼任情况，当前安全管理员由XX领导担任。 部分符合情况：暂无 不符合情况：XXX公司安全管理员非专职，存在兼任情况。

授权和审批	[一般]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。	通过对部门和岗位职责的描述，应能明确指出部门或岗位可以进行审批的事项内容	1)访谈安全主管，询问对哪些等级保护对象活动进行审批，审批部门是什么部门，审批人是什么岗位 2)核查部门职责文档是否明确各部门的审批事项和审批岗位 3)核查岗位职责文档是否明确各岗位的审批事项 4)核查审批记录，是否与相关职责文件描述一致。	1)部门和各岗位的职责文件中包含了相关事项的审批描述 2)审批记录和相关职责文件描述一致	职责文档》，相关制度中已明确了各个部门岗位的具体职责划分以及授权审批事项、审批部门和批准人等，具备审批记录。 部分符合情况：已制定《XXX部门职责文档》，相关制度中已明确了各个部门岗位的具体职责划分以及授权审批事项、审批部门和批准人等，但无法提供相应的审批记录等表单。 不符合情况：XXX公司未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内容。
授权和审批	[关键]b)应针对系统投入运行、重要资（如敏感数据等资源）的访问、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。（F3）	相关的管理制度文档中一般对系统变更(如变更管理制度).物理访问(如机房管理制度)、系统接入(如网络管理制度)等重要活动明确审批流程，包括逐级审批流程。另外，要求保存审批过程记录文档，并要求保证执行中的审批程序、审批部门及批准人与审批制度文档中规定的一致性	1)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、重要管理制度的规定和发布，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， 其中哪些事项需要逐级审批 2)核查系统变更、重要操作、物理访问和系统接入等事项的相关管理制度是否明确相关操作的逐级审批程序 3)核查经逐级审批的记录，查看是否具有各级批准人的签字和审批部门的盖章，是否与相关制度一致 系统变更，一般分为重大变更和普通变更，前者如系统运行业务改变或系统核心设备更换等，后者如点如系统或设备配置更改等；重要操作，如设备加电或断电等；物理访问主要指对机房或重要办公区域的访问；:系统接入一般指外部系统或网络接入等级保护对象 逐级审批活动的重要程度可以是从执行管理层(安全主管、负责人)到运营层(各管理员)的二级审批，也可以是从最高层(网络	1相关管理制度中明确了系统变更、物理访问和系统接入等重要操作的审批流程 2)具有相关事项的审批记录 3逐级审批的记录，具有各级批准人的签字和审批部门的盖章，与相关制度一致	信息系统变更管理办法》、《XXX公司第三方安全管理规定》、《XXX公司信息系统项目管理规定》等制度，相关制度中对系统变更、重要操作、物理访问和系统接入等事项执行过程进行了审批流程规定，并特别强调了“系统上线”等重要活动的逐级审批要求，具体工作中通过OA线上审批。 部分符合情况：已制定《XXX公司信息系统变更管理办法》、《XXX公司第三方安全管理规定》、《XXX公司信息系统项目管理规定》等制度，相关制度中对系统变更、重要操作、物理访问和系统接入等事项执行过程进行了审批流程规定，并特别强调了“系统上线”等重要活动的逐级审批要求，但无法提供审批过程记录表单。
授权和审批	[一般]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。	审批事项可能会根据审批部门变更、审批人变更以及相关审批流程发生变更，因此需要及时根据实际情况变化进行审查并更新相关内容。另外需定期对相关审批事项进行审查，以更新需要更新的相关信息	1访谈信息/网络安全主管对各类审批事项进行更新 2)核查是否具有对相关审批事项的定期审查记果和授权更新记录 需要形成审批事项列表，在该列表中明确审批事项、涉及的审批部门、批准人等，并要求定期对该列表进行更新维护，如部门职责或岗位职责改变则某-审批活动涉及的审批部门和批准人则会改变，活动的重要程度改变则该活动的审批流程也会改	具有定期审查审批事项的记录和授权更新记录	符合情况：XXX公司每年对各类审批项目、审批部门和审批人进行更新，记录表单类文档中具有更新需授权和审批的项目、审批部门和审批人等信息，记录日期与审查周期一致。 部分符合情况： 不符合情况：XXX公司未定期审查审批事项。

授权和审批	[关键]d)用户应被授予完成所承担任务所需的最小权限，重要岗位的员工之间应形成相互制约的关系，权限变更应执行相关审批流程，并有完整的变更记录。（F3）	用户需要被授予完成所承担任务所需的最小权限，重要岗位的员工之间需要形成相互制约的关系，权限变更需要执行相关审批流程，并有完整的变更记录。	1)访谈用户是否被授予完成所承担任务所需的最小权限，重要岗位的员工之间是否形成相互制约的关系， 2) 权限变更是否执行相关审批流程，是否具备完整的变更记录。	1) 根据最小权限原则对用户授权，重要岗位的员工之间形成相互制约的关系。 2) 具有权限变更的相关审批流程和完整的变更记录。	符合情况：XXX公司根据最小权限原则对用户授权，重要岗位的员工之间形成相互制约的关系，并具有权限变更的相关审批流程和完整的变更记录。 部分符合情况： 不符合情况：XXX公司未根据最小权限原则对用户授权，重要岗位的员工之间未形成相互制约的关系，不具有权限变更的相关审批流程和完整的变更记录。
授权和审批	[关键]e)应建立系统用户及权限清单，定期对员工权限进行检查核对，发现越权用户要查明原因并及时调整，同时清理过期用户权限，做好记录归档。（F3）	建立系统用户及权限清单，定期对员工权限进行检查核对，发现越权用户要查明原因并及时调整，同时清理过期用户权限，做好记录归档。	1)核查是否建立系统用户及权限清单。 2)核查是否定期对员工权限进行检查核对。 3)核查是否具备检查记录。	1)建立系统用户及权限清单。 2)定期对员工权限进行检查核对。 3)具备检查记录。	符合情况：XXX公司建立了用户及权限列表，并通过XXX方式对员工账户权限进行定期核查，并保留相关检查记录。 部分符合情况：XX公司建立了用户及权限列表，但未对员工账户权限进行定期核查，并保留相关检查记录。 不符合情况：XX公司未建立用户及权限列表，未对员工账户权限进行定期核查，并保留相关检查记录。
沟通和合作	[重要]a)应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题。	一个单位的等级保护对象运行可能涉及到多个业务部门，因此，为保障整个等级保护对象安全工作的顺利完成，需要各业务部门的共同参与和密切配合。此处沟通方式的要求，要求采取例会或不定期召开会议的形式进行网络安全问题处理	1)访谈信息/网络安全主管，是否建立了各类管理人员之间、组织内部机构之间以及网络安全职能部门内部的合作与沟通机制 2)核查相关会议记录，是否涵盖安全相关内容。其中，针对组织内部机构之间以及网络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，是否具有安全管理委员会或领导小组安全管理工作执行清况的文件或工作记录(如会议记录/纪要，网络安全工作决策文档等)	1)内部机构之间网络安全职能部门内部建立了相相关沟通交流机制 2)具有定期召开会议的记录	符合情况：XXX公司已建立各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通机制，每年组织一次工作会议进行沟通合作，共同协调处理信息安全相关问题，具备相关会议记录。 部分符合情况：不定期召开协商会议或协商会议周期过长，无相关会议记录。 不符合情况：XXX公司未定期与各类管理人员、组织内部机构和网络安全管理部门之间进行合作沟通，不具备沟通合作

沟通和合作	[一般]b)应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通。	与外界各类单位、部门的沟通与合作机制可能有多种方式,如与网络管理部门定期汇报、检查工作,与供应商定期会议商讨系统中的安全问题，与业界专家进行安全评审咨询等方式	1)访谈信息/网络安全主管,是否建立了与网络安全管理部门、各类供应商、业界专家及安全组织的合作与沟通机制 2)核查相关沟通合作记录，是否具有与网络安全管理部门、各类供应商、业界专家沟通交流的记录	1）与网络安全管理部门、各类供应商、业界专家及安全组织的合作与沟通机制 2）具有日常沟通交流的记录和文件	符合情况：XXX公司已建立与网络安全职能部门、各类供应商、业界专家及安全组织等的沟通、合作机制，通过会议、电话、邮件等方式进行交流沟通。 部分符合情况：无法提供日常沟通交流的记录和文件，导致留档缺失。 不符合情况：XXX公司未定期与网络安全职能部门、各类供应商、业界专家及安全组织等进行合作沟通，不具备沟通合
沟通和合作	[一般]c)应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。	与外联单位的联系应建立联系列表并根据实际情况维护更新列表信息、明确合作内容以及联系人等相失的信息	核查外联单位联系列表，是否记录外联单位名称、合作内容、联系人和联系方式等信息	具有外联单位联系列表，且包括外联单位名称、合作内容、联系人和联系方式等信息	联单位联系列表，包含外联单位名称、合作内容、联系人和联系方式等信息。 部分符合情况：XXX公司已建立外联单位联系列表，但列表数据不全面。 不符合情况：XXX公司未建立外联单位联系列表。
审核和检查	[一般]a)应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。	常规的安全检查不同于日常的安全巡检，常规的安全检查一般是每周或每月开展，汇总一段时间内的系统状态	1)访谈信息/网络安全主管是否定期进行了常规安全核查 2)核查常规安全核查记录是否包括了系统日常运行系统漏洞和数据备份等情况	1)定期(如每周或每月)进行安全检查,检查内容涵盖系统日常运行状态、数据备份、漏洞检查等内容 2)具有相关的检查记录	符合情况：XXX公司每月/季度进行一次常规安全检查，具有常规安全检查记录表单，记录明确了检查日期，检查内容包括系统日常运行、系统漏洞和数据备份等情况，且出具有巡检报告。 部分符合情况：XXX公司每月/季度进行一次常规安全检查，具有常规安全检查记录表单，但检查内容不够详细，未包含系统漏洞和数据备份情况等内容。 不符合情况：XXX公司未定期
审核和检查	[关键]b)应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。	全面的安全检查可自行组织或通过第三方机构进行，无论哪种方式，检查内容均应涵盖技术和管理各方面安全措施的落实情况，如果是单位内部进行的全面安全检查相当于对等级保护对象安全的自评估。定期可以是半年一次也可以是一年一次	1)访谈信息/网络安全主管，是否定期进行了全面安全核查，核查内容都有哪些 2)核查全面安全核查记录类文档，是否包括了现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等	1)定期开展全面安全检查，检查内容覆盖技术有效性和管理措施落地执行情况等 2）具有全面安全检查记录	一次全面的安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等，且具备检查记录。 部分符合情况：暂无 不符合情况：XXX公司未定期进行全面安全检查。

审核和检查	[关键]c)应建立对门户网站内容发布的审核、管理和监控机制。（F3）	需要建立对门户网站内容发布的审核、管理和监控机制。	1)访谈是否建立门户网站内容发布的审核、管理和监控机制。 2)核查是否有相关文档规定。	1)建立了门户网站内容发布的审核、管理和监控机制 。 2)具有门户网站内容发布的审核记录。	符合情况：XXX公司通过XXX方式对门户网站的发布内容进行审核、管理、监控，并制定了相关审核记录表单。 部分符合情况：XXX公司通过XXX方式对门户网站的发布内容进行审核、管理、监控，但未制定相关审核记录表单。 不符合情况：XXX公司未对门户网站的发布内容进行审核、管理、监控，无相关审核记录表单。。
审核和检查	[关键]d)应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，要求限期整改的 需要对相关整改情况进行后续跟踪，并将每次安全检查报告和整改落实情况整理汇总后，对 安全检查结果进行通报并报上一级机构科技部门备案。（F3）	无论是日常检查还是定期全面的安全检查都需要制定安全检查格,记录全面检查结果，并形成安全检查报告，同时也要求将安全检查结果通知给相关人员，尤其是运营层的各岗位管理员	1)访谈安全管理员，询问是否制定安全核查表格实施安全检查,是否对检查结果进行通报 2)核查安全检查表格，安全检查记录，安全检查报告等文档，是否具有安全检查表格、安全检查记录、安全检查报告，安全检查结果通报记录 3)核查安全检查报告，查看报告日期与检查周期是否一致，报告中是否具有检查内容、检查时间、检查人员，检查数据汇总表、检查结果等的描述	1）具有安全检查表格，安全检查记录，安全检查报告等文档 2）安全检查报告日期与检查周期一致，报告中具有检查内容、检查时间、检查人员，检查数据汇总表、检查结果等的描述	检查表格、安全检查记录、安全检查报告、安全检查结果通报记录等；安全检查表记录包含常规检查、全面检查的相关数据，每年形成安全检查报告，通过邮件、会议等方式对安全检查结果进行通报。 部分符合情况：XXX公司具备安全检查表格、安全检查记录、安全检查结果通报记录等；安全检查表记录包含常规检查、全面检查的相关数据，通过邮件、会议等方式对安全检查结果进行通报，但未编写最终安全检查报告。 不符合情况：XXX公司未制定安全检查表格实施安全检查。
审核和检查	[关键]e)应制定违反和拒不执行安全管理措施规定的处罚细则。（F3）	制定违反和拒不执行安全管理措施规定的处罚细则。	1)访谈是否制定违反和拒不执行安全管理措施规定的处罚细则。	具有违反和拒不执行安全管理措施规定的处罚细则。	XXX管理制度，对违反和拒不执行安全管理措施规定的处罚细则进行了说明。 部分符合情况：暂无 不符合情况：XX公司未制定对违反和拒不执行安全管理措施规定的处罚细则进行说明的制度

安全管理人员（S3A3G3）作业指导书					
安全控制点	**检测项**	**要求解读**	**测评方法**	**预期结果或主要证据**	**符合情况**
人员录用	[一般]a)应指定或授权专门的部门或人员负责人员录用。	对员工的安全要求应该从聘用阶段就开始实施，无论是长期聘用的员工还是合同员工、临时员工，都应在员工的聘用合同中明确说明员工在网络安全方面应遵守的规定和应承担的安全责任，并在员工的聘用期内实施监督机制。为保证人员录用过程的规范，应明确专门的部门和人员负责	访谈信息/网络安全主管是否由专门的部门或人员负责人员的录用工作	1)具有相关的职能部门专门负责人员录用工作 2)具有明确规定负责人员录用工作的部门或人员的制度	符合情况：已指定公司人事部负责人员录用工作。 部分符合情况：具有相关的职能部门专门负责录用工作，但未制定相关的制度。 不符合情况：未指定公司人事部负责人员录用工作。
人员录用	[重要]b)应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核。	聘用员工时，应充分饰选、审查，特别是那些可能接触敏感信息的员工，需要进行包括身份、背景，专业资格和资质方面的审查和技术技能的考核	1核查人员安全管理文档是否说明录用人员应具备的条件(如学历要求，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) 2)核查是否具有人员录用时对录用人身份、背景、专业资格和审查的相关文档或记录，是否记录审查内容和审查结果等 3)核查人员录用时的缺技能考核文档或记录，是否记录考核内容和考核结果等	1)人员录用管理文档说明了不同岗位录用人员的条件。 2)具有人员录用的审查记录 3)具有人员录用的技能考核记录	符合情况：XXX公司在人员录用时对被录用人身份、安全背景、专业资格或资质等进行了审查，对其技术能力进行了考核，且具备相关审查记录及考核记录。 部分符合情况： XXX公司在人员录用时对被录用人身份、安全背景、专业资格及资质等进行了审查，且具备相关审查记录，但未对人员技能进行考核，不具备考核记录。 不符合情况：XXX公司在人员录用时未对被录用人身份、安全背景、专业资格及资质等进行了审查，且不具备相关审查记录，未对人员技能进行考核，不具备考核记录
人员录用	[关键]c)应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。	保密协议面向所有被录用人员，岗位安全协议则主要面向关键岗位，并根据岗位不同约束各自在岗位上的安全责任	1)核查保密协议，所有录用人员是否签署保密协议，明确保密范围、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)核查岗位安全协议文档，关键岗位是否签署岗位安全协议，明确岗位女全责任、协议的有效期限和责任人签字等内容 关键岗位的人员主要是指涉及到本单位核心业务或者核心技术的岗位人员，包括从事系统安全管理的安全管理员、系统管理员、网络管理员等。岗位安全协议不同于保密协议，其与岗位职责有关，主要在协议中明确如果未履行岗位职责或因失职而引发安全事件应该承担的安全责任	1)具有相关人员签字的人员保密协议，明确保密范围、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）具有关键岗位人员签字的岗位责任协议，明确岗位安全责任、协议的有效期限和责任人签字等内容	符合情况：XXX公司与正式员工签署有保密协议，与关键岗位人员签署有岗位责任协议；保密协议中包含保密范围、保密责任、违约责任、协议的有效期限和责任人签字等内容；岗位责任协议中包含岗位安全责任定义、协议的有效期限和责任人签字等内容。 部分符合情况：XXX公司与正式员工签署有保密协议，保密协议中包含保密范围、保密责任、违约责任、协议的有效期限和责任人签字等内容；但未与关键岗位人员签署岗位责任协议书。 不符合情况：XXX公司与正式员工未签署保密协议，未与关键岗位人员签署岗位责任协议书。
人员录用	[关键]d)应对网络安全管理人员实行备案管理，网络安全管理人员的配备和变更情况，应及时报上一 级科技部门备案，金融机构总部网络安全管理人员在总部科技部门备案。（F3）	需要对网络安全管理人员实行备案管理，网络安全管理人员的配备和变更情况，应及时报上一 级科技部门备案，金融机构总部网络安全管理人员在总部科技部门备案。	1核查是否对网络安全管理人员实行备案管理。 2核查是否对网络安全管理人员的配备和变更情况，及时报上一 级科技部门备案。 3核查是否具备案记录。	1) 具有网络安全管理人员的备案制度。 2)网络安全管理人员的配备变更情况报上一级科技部门备案，具有网络安全管理人员备案记录。	符合情况：制定了XXX制度对网络安全人员的备案流程事项进行说明，相关人员变更与上级部门报备，并保留相关备案记录。 部分符合情况：制定了XXX制度对网络安全人员的备案流程事项进行说明，但未将相关人员变更与上级部门报备，无相关备案记录。 不符合情况：未制定XXX制度对网络安全人员的备案流程事项进行说明，但未将相关人员变更与上级部门报备，无相关备案记录。
人员录用	[关键]e)凡是因违反国家法律法规和金融机构有关规定受到过处罚或处分的人员，不应从事网络安全 管理工作。（F3）	因违反国家法律法规和金融机构有关规定受到过处罚或处分的人员，不应从事网络安全 管理工作。	1核查是否制定相关规定，要求因违反国家法律法规和金融机构有关规定受到过处罚或处分的人员，不应从事网络安全 管理工作。	网络安全管理人员无因违反国家法律法规和金融机构有关规定而受到处罚或处分的记录	符合情况：网络安全管理人员无犯罪记录以及相关金融机构有关处罚和处分记录。 不符合情况：网络安全管理人员有犯罪记录或相关金融机构有关处罚和处分记录。

人员离岗	[重要]a)应及时终止离岗人员的所有访问权限，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。	解雇、退休、辞职、合同到期或其他原因离开单位或离岗的人员在离开前都必须到相应管理部门办理严格的调离手续，包括交回其拥有的相关证件、徽章、密钥、访问控制标识、单位配给的设备等	1)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。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 2)核查人员离岗记录文档，是否具有离岗人员终止其访问权限，交还身份证件、软硬件设备等的登记记录	具有离岗人员交还各类资产的登记记录	符合情况：人员离岗后已交还工作证件、软硬件设备，且及时终止了离岗员工的所有访问权限，具备人员离岗记录。 部分符合情况：人员离岗后已交还工作证件、软硬件设备，但未及时终止离岗员工的所有访问权限，不具备人员离岗记录。 不符合情况：人员离岗后未交还工作证件、软硬件设备，未及时终止了离岗员工的所有访问权限，不具备人员离岗记录
人员离岗	[重要]b)应办理严格的调离手续，并承诺调离后的保密义务后方可离开。	调离后的保密承诺可单独签署，或者在保密协议中有相关条款明	1）核查人员离岗的管理文档是否规定了人员调离手续和离岗要求 2)核查是否具有按照离岗程序办理调离手续的记录 3)核查保密承诺文档是否有调离人员的签字	1）具有相关规范人员调离手续要求的管理文档 2)具有相关人员调离手续的记录 3)具有调离人员签字的保密承诺文档	符合情况：《XXX公司人力资源安全管理规定》中制定了人员调离手续和离岗要求等，《人员离岗记录》中按照人员管理文档中的离岗程序办理了人员调离手续，具有调离人员签字后的保密承诺文档。 部分符合情况：《XXX公司人力资源安全管理规定》中制定了人员调离手续和离岗要求等，但不具备《人员离岗记录》，或《人员离岗记录》规范与记录不清晰。 不符合情况：不具备《人力资源安全管理规定》，不具备《人员离岗记录》
人员考核	[关键]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。（F3）	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）核查是否定期对各个岗位的人员进行安全技能及安全认知的考核。 2）核查考核文档，是否明确考核周期、考核方式 考核内容等相关内容	1）人员考核的管理文档明确要求定期对各个岗位的人员进行安全技能及安全认知的考核。 2) 具有安全技能及安全认知考核记录。	符合情况：制定人员考核相关要求文档XXX，要求对各个岗位人员进行定期安全机能和认知考核，并保留相关考核记录。 不符合情况：未制定人员考核相关要求文档XXX，无相关考核记录。
人员考核	[关键]b)应对关键岗位的人员进行全面、严格的安全审查和技能考核。（F3）	对关键岗位的人员进行全面、严格的安全审查和技能考核。	1）核查是否对关键岗位的人员进行全面、严格的安全审查和技能考核。 2）核查考核文档，是否明确考核周期、考核方式 考核内容等相关内容	1）对关键岗位的人员进行全面、严格的安全审查和技能核查。 2）具有审查和考核记录	符合情况：对关键岗位人员进行定期安全审查和技能考核，并保留相关审查和考核记录。 不符合情况：未对关键岗位人员进行定期安全审查和技能考核，无相关审查和考核记录
人员考核	[关键]c)应对考核结果进行记录并保存。（F3）	对考核结果进行记录并保存。	1）核查是否对考核结果进行记录并保存以及保存方式	考核记录中考核人员包括各个岗位的人员，考核内容包括安全知识、 安全技能、安全认知等，记录日期与考核周期一致	符合情况：对所有考核结果保留相关记录。 不符合情况：未对所有考核结果保留相关记录。
安全意识教育和培训	[重要]a)应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。	安全意识教育和培训是对人员的安全意识、 安全技能等方面进行提高的手段之一，保证人员具有与其岗位职责相适应的安全技术能力和管理能力，以减少人为操作失误给系统带来的安全风险	1)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 2)核查网络安全教育和技能培训文档，是否明确培训周期、培训方式 培训内容和考核方式等相关内容 3)核查安全责任和惩戒措施管理文档是否包含具体的安全责任和惩戒措施	1)有相关文档明确要求对人员进行安全意识教育和岗位技能培训 2）具有网络安全教育和技能培训文档，明确培训周期、培训方式 培训内容和考核方式等相关内容 3.具有相关文档明确安全责任和惩戒措施	符合：已制定《信息安全教育和培训制度》，制度中规定每半年对各部门人员进行安全意识教育和岗位技能培训，明确了相关考核标准，且具备培训考核记录。 部分符合：已制定《信息安全教育和培训制度》，制度中规定每半年对各部门人员进行安全意识教育和岗位技能培训，明确了相关考核标准，但不具备相关培训记录。 不符合：未制定《信息安全教育和培训制度》。

安全意识教育和培训	[一般]b)应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训。	针对不同岗位需要不同的培训的计划，培训计划一般在年初制定本季度规划或者年末制定下年的计划，由各个部门制定自己部门的计划后汇总至培训主管部门	1)访谈安全主管，询问是否针对不同的岗位制定不同的计划，并按照计划对各个岗位人员进行安全教育和培训 2) 核查安全教育和培训文档，查看是否明确规定应进行安全教育和培训 3)核查是否具有不同岗位的培训计划，查看培训内容是否包含网络安全基础知识、岗位操作规程等 4)核查安全教育和培训记录是否有培训人员、培训内容、培训结果等的描述	1)具有安全教育和培训管理文档，明确规定应进行安全教育和培训 2)具有针对不同岗位人员的培训计划 3)具有相关培训记录	符合情况：已制定《信息安全教育和培训制度》，具有不同岗位的培训计划，培训计划中包含了培训目的、培训方式、培训对象、培训内容、培训时间和地点等内容；且具备培训记录，记录中包含培训人员、培训内容、培训结果、人员签到等内容。 部分符合情况：已制定《信息安全教育和培训制度》，但只针对部分岗位的培训计划，培训计划中包含了培训目的、培训方式、培训对象、培训内容、培训时间和地点等内容；且具备培训记录，记录中包含培训人员、培训内容、培训结果、人员签到等内容。 不符合情况：XXX公司未针对不同岗位制定不同岗位培训计划
安全意识教育和培训	[关键]c)每年应至少对网络安全管理人员进行一次网络安全培训。（F3）	每年需要至少对网络安全管理人员进行一次网络安全培训	1)访谈安全主管，询问是否每年至少对网络安全管理人员进行一次网络安全培训。 2)核查培训文档，是否明确培训周期、培训方式 培训内容和考核方式等相关内容	具有定期的各岗位人员技能考核记录，记录的考核人员包括各个岗位的人员，考核内容包含安全知识、安全技能等，记录日期与考核周期一致	符合情况：XXX公司每季度针对不同岗位的人员进行技能考核，具有技能考核记录。 部分符合情况：XXX公司每季度针对不同岗位的人员进行技能考核，但不具有技能考核记录。 不符合情况：XXX公司未定期对不同岗位的人员进行技能考核
外部人员访问管理	[重要]a)应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案。	外部人员访问受控区域需要经相关人员批准并进行有效控制	1)核查外部人员访问管理文档，是否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 2)核查外部人员访问重要区域的书面申请文档是否具有批准人允许访问的批准签字等 3)核查外部人员访问重要区域的登记记录是否记录了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	1)相关管理文档明确了外部人员物理访问受控区域的要求 2)具有相关申请并批准进入的记录 3)具有外部人员访问受控区域的相关登记记录	符合：已制定《XXX公司第三方安全管理规定》，制度中对外来人员访问受控区域进行了申请流程规定，需签订协议并填写申请登记表，审批通过后须由专人陪同，且留存有相关记录表单。 部分符合：已制定《XXX公司第三方安全管理规定》，制度中对外来人员访问受控区域进行了申请流程规定，需签订协议并填写申请登记表，审批通过后须由专人陪同，但未留存有相关记录表单。 不符合：XXX公司未对外部人员访问受控区域做出规定，出专由专人全程进行陪同
外部人员访问管理	[重要]b)应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案。	外部人员存在接入受控网络的情况，需严格控制并采取相关的管理措施	1)核查外部人员该问管理文档是否明确外部人员接入受控网络前的申请审批流程 2)核查外部人员访问系统的书面申请文档是否明确外部人员的访问权限，是否具有允许访问批准签字等 3)核查外部人员访问系统的登记记录是否记录外部人员访问的权限、时间、账户等	1)相关管理文档明确了外部人员逻辑访问受控网络系统的审批要求 2)具有相关申请并批准接入网络的记录 3)具有外部人员逻辑访问受控区域的相关登记记录	符合：已制定《XXX公司第三方安全管理规定》，制度中规定了外部人员接入受控网络前的申请审批流程，外部人员访问系统的登记记录中记录了外部人员访问的权限、时限、账户等信息。 部分符合：已制定《XXX公司第三方安全管理规定》，制度中规定了外部人员接入受控网络前的申请审批流程，但不具备相关的接入记录。 不符合：外部人员接入受控网络无需提交书面申请
外部人员访问管理	[关键]c)应对允许被外部人员访问的网络资源建立存取控制机制、认证机制，列明所有用户名单及其 权限，其活动应受到监控。（F3）	对允许被外部人员访问的网络资源建立存取控制机制、认证机制，列明所有用户名单及其 权限，其活动应受到监控。	1)核查是否建立外部人员访问的网络资源的存取控制机制。 2)核查是否制定相关文档规定。	1) 对允许被外部人员访问的网络资源，建立存取控制机制、认证机制。 2) 外部人员权限表单包括所有外部人员及其权限。 3)外部人员访问活动受到监控	符合：已制定《XXX》，制度中规定了外部人员 的网络资源存取控制机制、认证机制等，并制定外部人员权限表单，通过XXX管理员对外部人员的访问活动进行监控。 部分符合：已制定《XXX》，制度中规定了外部人员 的网络资源存取控制机制、认证机制等，并制定外部人员权限表单，未通过XXX管理员对外部人员的访问活动进行监控。 不符合：未制定《XXX》，对外部人员的网络资源存取控制机制、认证机制等进行规定，无外部人员权限表单，未通过XXX管理员对外部人员的访问活动进行监控。

外部人员访问管理	[重要]d)外部人员离场后应及时清除其所有的访问权限。	外部人员特别是获得访问权限的外部人员，离场需进行严格的控制，并清除其所有的访问权限	1）应核查外部人员访问管理文档是否明确外部人员离开后及时清除其所有访问权限 2)核查外部人员访问系统的登记记录是否记录了访问权限清除时间	1具有相关管理文档明确外部人员离场后清除其权限的要求 2)具有相关清除访问权展的记录	符合情况：《XXX公司第三方安全管理规定》中已规定外部人员离场后须及时清除其所有的访问权限，具备外部人员访问系统登记记录，记录中包含访问权限的清除时间等内容。 部分符合情况：《XXX公司第三方安全管理规定》中已规定外部人员离场后须及时清除其所有的访问权限，不具备外部人员访问系统登记记录。 不符合情况：外部人员在离开受控区域及断开受控网络后，未及时清除其访问权限，不具备相关记录。
外部人员访问管理	[关键]e)获得系统访问授权的外部人员应签署保密协议，不得进行非授权增加、删除、修改、查询数 据等操作，不得复制和泄露金融机构的任何信息。（F3）	对获得系统访问授权的外部人员，需进行更加严格的保密控制措施	核查外部人员的访问保密协议或记录表单类文档，是否明确人员的保密义务(如不得进行非授接权操作，不得复制信息等)	具有相关外部人员签字的保密协议，明确其保密义务	符合情况：已制定《XXX公司第三方安全管理规定》，制度中规定获得系统访问权限的外部人员需签署保密协议，协议中明确了外部人员的保密义务，包含不得进行非授权操作，不得复制信息等内容。 部分符合情况：已制定《XXX公司第三方安全管理规定》，制度中规定获得系统访问权限的外部人员需签署保密协议，但保密协议内容不够规范。 不符合情况：未与具备相关权限的外部人员签署保密协议

安全建设管理（S3A3G3）作业指导书					
安全控制点	检测项	要求解读	测评方法	预期结果或主要证据	符合情况
定级和备案	[重要]a)应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由。	《等级保护对象安全等级保护定级报告》是全国各类等级保护对象定级报告的通用模板，具体文档内容参见www.djbh.net.	1)核查定级文档是否明确测评系统的安全保护等级 2)核查是否给出了定级的方法和理由	具有明确描述定级方法理由和最终定级结果的定级报告书	符合情况：系统具有定级报告，报告中明确了系统的安全保护等级，且描述了安全保护等级确定的方法和理由。 部分符合情况：无。 不符合情况：无定级报告。
定级和备案	[重要]b)应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定。	定级结果的准确性需要安全技术专家论证评审。若初步定级结果为第二级、第三级，可组织本行业和网络安全行业专家进行评审，若为四级，则需网络安全等级保护专家评审委员会专家进行评审	1)核查是否对测评系统组织相关部门或相关专家对定级结果进行了认证和审定 2)核查是否有定级结果的评审和论证记录文件	具有相关专家对定统结果论证意见	符合情况：组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定，具有专家评审意见。 部分符合情况：无。 不符合情况：未组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定
定级和备案	[重要]c)应保证定级结果经过相关部门的批准。	定级结果需由上级部门或本单位相关部门的批准	1)核查是否获得了相关主管部门的批准 2)核查是否有定级结果的审批文件	具有主管部门审批意见或本单位相关部门的审批意见	符合情况：有上级主管部门，通过上级主管部门审批；无上级主管部门的，有公司内部业务部门、信息安全部门等的批准。 部分符合情况：无。 不符合情况：定级结果未经过相关部门的批准。
定级和备案	[关键]d)应将备案材料报主管部门和相应公安机关备案。	有主管部门的，备案材料需向主管部门和公安机关备案，没有主管部门的，备案材料需向相应公安机关备案	1）核查是否向主管部门备案 2）核查是否有备案证明证书	具有主管部门和公安机关的备案证明	符合情况：备案材料已报主管部门和相应公安机关备案，具有公安局出具的备案证明。 部分符合情况：无。 不符合情况：未将备案材料报主管部门和相应公安机关备案。
安全方案设计	[重要]a)应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施。	系统确定安全保护等级后,安全规划设计需根据其安全保护等级确定基本安全保护措施	1)核查是否根据系统等级选择相应的安全保护措施 2)核查是否根据风险分析的结果补充安全措施 3)核查设计类文档是否根据系统等级或风险分析结果采取相应的安全保护措施 这里的安全规划设计类文档要求根据等级保护对象的安全保护，判断等级保护对象现有的安全保护水平与国家等级保护管理规范和技术标准之间的差距，提出等级保护对象	安全设计文档有明确描述系统安全保护等级，并在相关章节中描述安全措施设计是依据系统等级和其特殊安全需求进行选择	符合情况：具有《系统安全设计方案》，方案中明确根据安全保护等级确定安全保护措施。 部分符合情况：无 不符合情况：未设计安全方案。

安全方案设计	[关键]b)应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件。	被测系统是整个单位等级保护对象的一部分，其安全方案应作为单位整体安全规划的一部分，且其安全性在设计上与其位系统可能存在共享，譬如在网络结构设计、安全措施部署上都具有共享关系，因此单位的整体安全规划也很有必要，安全规划是等级保护对象安全等级保护实施的环节之一，也是确保安全等级保护有效实施的重要环节，其目标是根据等级保护对象的划分情况，等级保护对象的定级情况、等级保护对象承载业务情况，通过分析明确等级保护对象安全需求设计合理、满足等级保护要求的安全方案	1)核查是否有保护对象的相关设计文档 2）核查保护对象的总体规划和设计文档，且文档内容是否连贯配套，内容是否含密码技术相关内容 一般情况下，配套文件中包括总体安全策略、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内容。在定期开展等级测评和安全评结后，如果发现等级保护对象安全现状已经不满足等级保护的基本安全要求或者发现等级保护对象有新的安全需求，则应该调整和修订安全保证体系的相关配套文件 安全规划管理示例： a)安全规划设计是指对系统总体安全建设规划，近期和远期安全建设工作计划、安全方案等进行设计、编制 b)安全方案设计是指根据系统的定级情况、承载业务情况，通过分析明确等级保护对象的安全需求，设	具有单位总体的安全规划文档和被删系统安全设计文档，且包含相关密码设计内容(如果采用了密码产品和算法)	符合情况：《系统安全设计方案》中包含与其他级别保护对象的关系进行整体安全体划和安全方案设计，其中包含密码技术相关内容，并形成配套文件。 部分符合情况：《系统安全设计方案》未中包含密码技术相关内容，或无与其他系统如何进行交互的内容。 不符合情况：《系统安全设计方案》及其他配套文件与其他系统如何进行交互的内容，也未包含密码相关内容。
安全方案设计	[重要]c)应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。	设计合理的安全方案是保障等级保护对象安全建设和运行的基础，安全设计方案应当对系统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、详细设计方案等内容作出具体的规划和设计，并经过论证、审定和批准	1)核查是否组织相关人员对系统规划和建设文档进行论证和评审 2)核查评审的文档和批准意见	具有总体安全规划和安全设计方案的专家论证、批准意见	符合情况：该系统的安全规划、安全设计方案及其配套文件均已进行评审。具有评审意见，批准后正式实施。 部分符合情况：无。 不符合情况：未组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定
产品采购和使用	[关键]a)应确保网络安全产品采购和使用符合国家的有关规定。	我国对网络安全产品的管理在不同发展阶段可能存在不同的管理政策,因此在该条款的理解上，应根据当下国家的管理要求去落实，目前而言，在此方面国家的主要管理要求是连从产品获得《计算机等级保护对象安全专用产品销售许可证》才能在市场上流通的政策。产品购买方在采购过程中应从已获得销售许可证的产品系列中选取	1)访谈建设负责人产品采购的流程或流通的标准2)抽样核查网络安全产品的销售许可标志	网络安全产品均具有销售许可证	符合情况：该系统相关网络安全产品有安全产品采购流程及符合国家有关规定。 部分符合情况：无 不符合情况：未有采购流程，未遵守合国家有关规定。
产品采购和使用	[关键]b)应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。	如若被测系统中采用了商用密码产品，则该产品的采购和使用需符合国家的用密码管理部门的要求，(如《信息安全等级保护商用密码管理办法》等)	1)访谈建设负责人是否采用了商用密码产品或服务 2)核查使用的密码产品的许可证明或批文 密码产品是指采用密码技术对信息进行加密保护或安全认证的产品，如加密电子证书等	密码产品符合国家相关部门的要求	符合情况：该系统使用的密码产品或服务，符合国家密码主管部门的要求。 部分符合情况：无 不符合情况：使用的密码产品不符合国家密码主管部门要求。

产品采购和使用	[关键]c)各机构购置扫描、检测类网络安全产品应报本机构科技主管部门批准、备案。（F3）	各机构购置扫描、检测类网络安全产品需要报本机构科技主管部门批准、备案。	1)访谈是否各机构购置扫描、检测类网络安全产品需要报本机构科技主管部门批准、备案。 2)核查相关制度文档。 3)核查是否具备审批、备案记录。	机构购置扫描、检测类网络安全产品需要报本机构科技主管部门批准、备案。	符合情况：机构购置扫描、检测类网络安全产品需要报本机构科技主管部门批准、备案。 部分符合情况：无 不符合情况：机构购置扫描、检测类网络安全产品无需报本机构科技主管部门批准、备案。
产品采购和使用	[一般]d)应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。	在采购产品时，不仅要考虑产品的使用环境、安全功能、成本(包括采购和维护成本)等因素，还要考虑产品本身的质量和安全性，因此需要预先对产品进行选型测试	1)访谈建设负责人产品采购流程 2)核查产品采购管理制度或要求 3)核查采购管理内容是否覆盖产品的选择方式以及定期审定和更新产品列表 通常情况下，产品采购的管理需要制定相关制度要求，产品采购管理示例： 产品采购管理是指对等级保护对象软硬件产品采购过程的管理，包括安全产品、网络产品、服务器以及应用和系统软件等 由XX处提出产品采购需求，由XX处按照政府采购流程进行产品采购，对于大宗产品的采购必须经过XX审批 采购的防火墙， IDS.防病毒软件等安全产品必须具有公安部下发的《计算机安全产品销售许可证》，采	具有产品选型测试报告、候选产品清单和定期更新名单	符合情况：产品采购由专门部门对产品进行选型测试，留存有产品选型测试文档、候选产品采购清单等。 部分符合情况：无。 不符合情况：产品采购前未进行选型测试。
产品采购和使用	[关键]e)扫描、检测类网络安全产品应仅限于本机构网络安全管理人员或经主管领导授权的技术人员 使用。（F3）	扫描、检测类网络安全产品仅限于本机构网络安全管理人员或经主管领导授权的技术人员 使用。	1)访谈是否扫描、检测类网络安全产品仅限于本机构网络安全管理人员或经主管领导授权的技术人员 使用。 2)核查相关制度文档。 3)核查是否具备使用登记记录。	扫描、检测类网络安全产品仅限于本机构网络安全管理人员或经主管领导授权的技术人员 使用。	符合情况：扫描、检测类网络安全产品仅限于本机构网络安全管理人员或经主管领导授权的技术人员 使用。 部分符合情况：无。 不符合情况：扫描、检测类网络安全产品不限于本机构网络安全管理人员或经主管领导授权的技术人员 使用
产品采购和使用	[关键]f)应定期查看各类网络安全产品相关日志和报表信息并汇总分析，若发现重大问题，立即采取 应急措施并按规定程序报告。（F3）	定期查看各类网络安全产品相关日志和报表信息并汇总分析，若发现重大问题，立即采取急措施并按规定程序报告。	1)核查是否定期查看各类网络安全产品相关日志和报表信息并汇总分析。 2)核查是否具备分析记录。 3)访谈发生重大问题时的紧急措施和报告程序。	定期查看各类网络安全产品相关日志和报表信息并汇总分析，若发现重大问题，立即采取急措施并按规定程序报告。	符合情况：定期查看各类网络安全产品相关日志和报表信息并汇总分析，若发现重大问题，立即采取急措施并按规定程序报告。 部分符合情况：无。 不符合情况：未定期查看各类网络安全产品相关日志和报表信息并汇总分析。
产品采购和使用	[关键]g)应定期对各类网络安全产品产生的日志和报表进行备份存档。（F3）	定期对各类网络安全产品产生的日志和报表进行备份存档。	1)访谈是否定期对各类网络安全产品产生的日志和报表进行备份存档。 2)核查相关制度文档。 3)核查是否具备相关备份记录。	定期对各类网络安全产品产生的日志和报表进行备份存档。	符合情况：定期对各类网络安全产品产生的日志和报表进行备份存档。 部分符合情况：无。 不符合情况：未定期对各类网络安全产品产生的日志和报表进行备份存档

产品采购和使用	[关键]h)应及时升级维护网络安全产品，凡超过使用期限的或不能继续使用的网络安全产品，要按照 固定资产报废审批程序处理。（F3）	及时升级维护网络安全产品，凡超过使用期限的或不能继续使用的网络安全产品，要按照 固定资产报废审批程序处理。	1)访谈是否定期升级维护网络安全产品，对于超过使用期限的或不能继续使用的网络安全产品，是否按照固定资产报废审批程序处理。 2)核查相关制度文档。 3)核查是否具备相关维护、报废审批记录。	及时升级维护网络安全产品。超过使用期限的或不能继续使用的网络安全产品，要按照 固定资产报废审批程序处理。	符合情况：1及时升级维护网络安全产品。2超过使用期限的或不能继续使用的网络安全产品，要按照 固定资产报废审批程序处理。 部分符合情况：满足1/2中的一种 不符合情况：1/2均不满足
自行软件开发	[关键]a)应将开发环境、测试环境、实际运行环境相互分离，敏感数据经过脱敏后才可在开发或测试 中使用。（F3）	需要将开发环境、测试环境、实际运行环境相互分离，敏感数据经过脱敏后才可在开发或测试 中使用。	1)访谈是否将开发环境、测试环境、实际运行环境相互分离，敏感数据经过脱敏后才可在开发或测试 中使用 2)核查相关制度文档。	1将开发环境、测试环境、实际运行环境相互分离，2敏感数据经过脱敏后才可在开发或测试中使用。	符合情况：1将开发环境、测试环境、实际运行环境相互分离，2敏感数据经过脱敏后才可在开发或测试中使用。 部分符合情况：满足1/2中的一种 不符合情况：1/2均不满足
自行软件开发	[关键]b)应确保开发人员和测试人员分离，开发人员不能兼任系统管理员或业务操作人员，确保测试 数据和测试结果受到控制。（F3）	为避免开发过程中对系统造成影响，要保证开发环境与实际运行环境纷开，开发人员和测试人员分离，开发人员不能兼任系统管理员或业务操作人员，测试数据和测试结果受到控制	1)访谈建设负责人,开发的控制流程和控制措施有哪些 2)核查软件开发相关管理的规定和要求 3)管理内容是否覆盖开发环境和运行环境分开的规定以及测试数据是否受控 开发人员和测武人员分离，即开发人员不能做测试人员，测试数据和测试结果受到控制，是指它们应该与软件设计相关档文一起有专人管理，并且对他们的使月和访问进行	1开发人员和测试人员分离，2开发人员不兼任系统管理员或业务操作人员，3测试数据和测试结果受到控制。	符合情况：1开发人员和测试人员分离，2开发人员不兼任系统管理员或业务操作人员，3测试数据和测试结果受到控制。 部分符合情况：满足1/2/3中的一种或两种 不符合情况：1/2/3均不满足
自行软件开发	[重要]c)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。	为保证软件开发过程的安全性和规范性，应制定软件开发方面的管理制度，规定开发过程的控制方法和人员行为准则	1)访谈安全建设负责人，是否有软件开发方面的管理制度 2)核查管理制度内容是否覆盖软件开发的整个生命周期 3)开发过程中是否覆盖开发过程的控制方法和行为准则	1)开发环境与运行环境分离 2)有明确的管理要求控制测试数据和测试结果的使用	符合情况：部署有独立的开发和测试环境，与生成环境物理隔离，测试部门具有独立的测试库等，设置访问权限，对测试数据和结果进行控制。 部分符合情况：开发环境与实际运行环境物理分开，对测试数据和结果无法实现安全可控，或开发环境与实际运行环境未物理分开，但测试部门具有独立的测试库等，设置访问权限，对测试数据和结果进行控制。 不符合情况：开发环境与实际运行环境未物理分开，对测试数据和结果无法实现安全可控。
自行软件开发	[重要]d)应制定代码编写安全规范，要求开发人员参照规范编写代码。	一般一个应用软件需要多名开发人员共同开发，然而不同开发人员有不同的代码编写风格，这给代码的维护、整合等工作带来了很大的困难。因此，要求针对不同的开发语言制定相应的代码编写规范，并要求所有开发人员都按照相应d的规范编写代代码，这将给代码的阅读、理解、维护、修改、跟踪调试、整合等带来极大的方便	1）访谈系统建设负责人是否有代码编写安全规范 2）代码编写规范是否明确代码的编写规则	具有代码编写安全规范	符合情况：制定《代码编写安全规范》，对排版要求、注释规范、方法（函数）等进行定义。 部分符合情况：无。 不符合情况：无制定《代码编写安全规范》。

自行软件开发	[一般]e)应具备软件设计的相关文档和使用指南，并对文档使用进行控制。	系统开发过程中，开发人员需编制软件设计的相关文档和使用指南，而且，系统开发文档的保管、使用应严格管理，加以限制。	1)访谈系统建设负责人是否有人负责对软件设计的相关文档进行管控 2)被测评系统是否有开发文档和使用说明文档	具有软件开发过程中的相关文档(如软件概要设计文档、软件详细设计文档等)和使用指南	符合情况：具有系统软件设计的流程图、效果图、设计文档、系统使用指南等文档，具有文档使用范围，对文档使用进行控制。 部分符合情况：无。 不符合情况：未有系统设计的相关文档和使用指南。
自行软件开发	[关键]f)应保证在软件开发过程中对代码规范、代码质量、代码安全性进行审查，在软件安装前对可能存在的恶意代码进行检测。（F3）	应在软件开发过程中加强软件的安全性测试，以便及早发现软件的安全漏洞、在软件安装前进行代码安全审计，通过工具测试和人工确认的方式识别恶意代码，这是保证软件安全运行的最后一道屏障。可通过第三方检测机构内或机构内部自行测试	1）访谈安全建设负责人，是否在软件开发的生命周期中进行安全性测试 2)核查是否具有安全性测试报告和代码审计报告	具有阶段性软件安全测试报告和软件安装前代码审计报告	符合情况：系统在开发过程中，进行了恶意代码检测等安全测试，并出具相关报告。 部分符合情况：系统在开发过程中，进行了恶意代码检测等安全测试，未出具相关报告。 不符合情况：系统在开发过程中，未对恶意代码检测等安全测试
自行软件开发	[重要]g)应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制。	对程序资源库的访问，维护等应进行严格管理	1)访谈建设负责人是否对程序资源库进行管控 2)核查是否有管控记录文件 要求对程序源代码及源程序库的修改、更新和发布都得到授权和批准。这里的发布-方面包括向程序员发布程序源代码，另一方面包括修改或更新程序代码后应用软件重新上线	具有程序资源库修改、更新、发布的授权、批准记录	符合情况：已对程序资源库的修改、更新、发布的流程进行管理，并对资源库进行严格的版本控制。 部分符合情况：对程序资源库的修改、更新、发布的流程进行管理，未对资源库进行严格的版本控制。 不符合情况：未对程序资源库的修改、更新、发布进行授权和批
自行软件开发	[一般]h)应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。	软件开发需保证开发人员为专职人员，并对其开发过程能够有效的控制	1)访谈建设负责人开发人员是否为专职人员 2)核查软件开发管控制度是否对开发过程和人员的行为准则进行了规定和要求	开发人员为专职人员，有相关管理要求或手段对开发人员进行控制、监视或审查	符合情况：所有人员均为专职人员，签署劳动合同，并对开发人员的开发活动受到控制、监视和审查。 部分符合情况：开发人员为专职人员，但开发人员的开发活动未受到控制、监视和审查。 不符合情况：未保证开发人员为专职人员，开发人员的开发活动未受到控制、监视和审查
自行软件开发	[关键]i)在软件开发过程中，应同步完成相关文档手册的编写工作，保证相关资料的完整性和准确性。（F3）	软件开发过程中，需要同步完成相关文档手册的编写工作，保证相关资料的完整性和准确性。	1)访谈软件开发过程中，是否同步完成相关文档手册的编写工作。 2)核查相关制度文档。 3)核查是否具备文档手册记录。	同步完成相关文档手册的编写工作	符合情况：在软件开发过程中，同步完成相关文档手册的编写工作。 部分符合情况：/ 不符合情况：未在在软件开发过程中同步完成相关文档手册的编写工作
外包软件开发	[重要]a)应在软件交付前检测其中可能存在的恶意代码。	同自行软件开发一样,对于外包软件,在交付前同样需要进行恶意代码检测，以保证软件的安全性,可要求外包方进行检测或机构内部自行检测	1)访谈建设负责人是否做恶意代码检测 2)核查是否有恶意代码检测报告	具有恶意代码检测报告	符合情况：软件交付前进行恶意代码检测，并出具相关报告。 部分符合情况：软件交付前检测进行恶意代码检测，未出具相关报告。 不符合情况：软件交付前未进行恶意代码检测。

外包软件开发	[一般]b)应保证开发单位提供软件设计文档和使用指南。	软件开发完成之后，应要求外包开发单位提供软件设计相关文档和使用指南	1)访谈建设负责人是否有软件设计的相关文档和使用指南 2)核查是否提供了软件生命周期中的所有文档	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、使用指南等	符合情况：开发单位提供的交付清单包括软件审计文档和使用指南。 部分符合情况：无。 不符合情况：开发单位未提供软件设计文档和使用指南。
外包软件开发	[关键]c)应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。	后门和隐蔽信道的审查在可专业的测试进行，若开发单位无法提供该类报告，则需提供书面材料保证软件源代码中不存在后门和隐蔽信道	1)访谈建设负责人，外包开发单位是否提供源代码 2)核查是否提供源代码的安全检查报告 3)核查软件源代码及源代码的审查记录 审查软件中可能存在的后门时，一般通常在系统的设计者利用应用系统的开发时机，故意设置机关，用以监视计算机系统，但有时也因偶然考虑不周而存在(如漏洞)。可以通过人工或采用专业工具(如Fortify SCA、Checkmarx 等)事方式进行源代码审查，发现软件中可能存在的	1.提供软件源代码 2.具有软件测试报告，内容涵盖后门和隐蔽信道的测试	符合情况：开发单位已提供源代码，对系统源代码进行审计工作，对可能存在的后门和隐蔽信道进行检测。 部分符合情况：无。 不符合情况：开发单位未提供软件源代码。进行审查。
外包软件开发	[关键]d)应要求外包服务商保留操作痕迹、记录完整的日志，相关内容和保存期限应满足事件分析、 安全取证、独立审计和监督检查需要。（F3）	要求外包服务商保留操作痕迹、记录完整的日志，相关内容和保存期限应满足事件分析、 安全取证、独立审计和监督检查需要。	1)访谈是否要求外包服务商保留操作痕迹、记录完整的日志。 2)核查相关制度文档。 3)核查是否具备外包服务商的操作记录。	1外包服务商保留操作痕迹、记录完整的日志2相关内容和保存期限应满足事件分析、 安全取证、独立审计和监督检查需要。	符合情况：1外包服务商保留操作痕迹、记录完整的日志2相关内容和保存期限应满足事件分析、 安全取证、独立审计和监督检查需要。 部分符合情况：满足1/2中一种。 不符合情况：1/2均不满足
外包软件开发	[关键]e)应禁止外包服务商转包并严格控制分包，保证外包服务水平。（F3）	禁止外包服务商转包并严格控制分包，保证外包服务水平。	1)访谈是否禁止外包服务商转包并严格控制分包 2)核查相关制度文档。	禁止外包服务商转包并严格控制分包，	符合情况：禁止外包服务商转包并严格控制分包， 部分符合情况：/ 不符合情况：未禁止外包服务商转包并严格控制分包
外包软件开发	[关键]f)应要求外包服务商聘请外部机构定期对其进行安全审计并提交审计报告，督促其及时整改发现的问题。（F3）	要求外包服务商聘请外部机构定期对其进行安全审计并提交审计报告，督促其及时整改发现的问题。	1)访谈是否要求外包服务商聘请外部机构定期对其进行安全审计并提交审计报告，督促其及时整改发现的问题。 2)核查相关制度文档。 3)核查是否具备审计报告。	1要求外包服务商聘请外部机构定期对其进行安全审计 2具备审计报告。	符合情况：1要求外包服务商聘请外部机构定期对其进行安全审计 2具备审计报告。 部分符合情况：满足1/2中一种。 不符合情况：1/2均不满足
工程实施	[一般]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。	等级保护对象工程实施应当指定或授权专门的部门或人员负责工程实施过程的管理，以保证实施过程的正式有效性	1）访谈建设负责人，工程实施是否指定专门部门或人员进行工程实施过程的管控 2）核查部门或岗位职责文档	指定了专门部门或人员对工程实施过程进行进度和质量控制	符合情况：指定部门负责工程实施过程的管理。 部分符合情况：无。 不符合情况：未指定部门负责工程实施过程的管理。

工程实施	[一般]b)应制定安全工程实施方案控制工程实施过程。	工程实施过程的控制需要事先制定实施方案，对工程时间限制、进度控制和质量控制等内容进行规定	1)访谈建设负责人是否有工程实施方案 2)核查工程实施方面的管理制度以及控制方法 总体的工程实施方案应说明任务量、计划进度、实施阶段、各阶段结束的标志和开始的条件、完成时提交的内容等。一旦实施方案确定，就必须按照方案的阶段安排逐步开展工作,并进行量化和考核，否则将造成工程实施组织的混乱，无法保证工程的顺利完成。 详细的工程实施方案要求的正式执行行是相对于系统工程能力成熟度模型(SSE-CMM)中所定义的一级，非正式执行。该级仅要求对所有基本实践都被执行，而对执行的结果并无明确要求。因此，正式执行意味着对执行结果和执行工程必须严格控制，根据制定的工程实施方案落实各个执行中间结果，保证实施结果与预定目标相符	具有工程实施方案，内容包括工程时间限制、进度控制等方面的方面	符合情况：制定《系统实施方案》，方案中对项目各阶段进行要求。 部分符合情况：无。 不符合情况：未制定《系统实施方案》控制实施过程。
工程实施	[重要]c)应通过第三方工程监理控制项目的实施过程。	一般来讲，对于外包实施项目，需要第三方工程监理的参与，来控制项目的实施过程，对工程进展，时间计划、控制措施、工程质量等进行把关	1)访谈建设负责人测评系统是否为外包项目 2)核查是否聘请了第三方监理 3)核查监理报告以及主要控制措施	第三方工程监理，工程监理报告明确了工程进展、时间计划、控制措施、工程质量等	符合情况：聘请监理单位进行项目监理工作。 部分符合情况：无。 不符合情况：未聘请第三方工程监理控制项目的实施过程
工程实施	[关键]d)应制定灾难备份系统集成与测试计划并组织实施，通过技术和业务测试，确认灾难备份系统 的功能与性能达到设计指标要求。（F3）	制定灾难备份系统集成与测试计划并组织实施，通过技术和业务测试，确认灾难备份系统 的功能与性能达到设计指标要求。	1)访谈是否制定灾难备份系统集成与测试计划，是否通过技术和业务测试，确认灾难备份系统 的功能与性能达到设计指标要求。 2)核查相关制度文档。 3)核查是否具备测试记录	1制定灾难备份系统集成与测试计划 2通过技术和业务测试，确认灾难备份系统 的功能与性能达到设计指标要求。	符合情况：1制定灾难备份系统集成与测试计划 2通过技术和业务测试，确认灾难备份系统 的功能与性能达到设计指标要求。 部分符合情况：满足1/2中一种。 不符合情况：1/2均不满足
工程实施	[关键]e)系统的建设、升级、扩充等工程应经过科学的规划、充分的论证和严格的技术审查，有关材 料应妥善保存并接受主管部门的检查。（F3）	系统的建设、升级、扩充等工程需要经过科学的规划、充分的论证和严格的技术审查，有关材 料需要妥善保存并接受主管部门的检查。	1)访谈对于系统的建设、升级、扩充等工程是否经过科学的规划、充分的论证和严格的技术审查。有关材料是否妥善保存并接受主管部门的检查。 2)核查相关制度文档。 3)核查是否具备审查论证记录	1系统的建设、升级、扩充等工程需要经过科学的规划、充分的论证和严格的技术审查，2具备审查论证记录	符合情况：1系统的建设、升级、扩充等工程需要经过科学的规划、充分的论证和严格的技术审查，2具备审查论证记录 部分符合情况：满足1/2中一种。 不符合情况：1/2均不满足
测试验收	[关键]a)应根据设计方案或合同要求等制订测试验收方案，并依据测试验收方案实施测试验收，在测试验收过程中应详细记录测试验收结果，形成测试验收报告。（F3）	此处的测试验收，可以包括外包单位项目实施完成后的测试验收，也可包括机构之间的内部开发部门移交给运维部门过程的验收等	1）访谈建设负责人是否对测试验收进行管控 ）2核查是否有调试验收方案和测试验收报告	1制订测试验收方案，2形成测试验收报告。	符合情况：1根据设计方案或合同要求等制订测试验收方案，2依据测试验收方案实施测试验收，在测试验收过程中应详细记录测试验收结果，形成测试验收报告。 部分符合情况：满足1/2中一种。 不符合情况：1/2均不满足

测试验收	[关键]b)应由项目承担单（部门）或公正的第三方制订安全测试方案，进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容，并将测试报告报科技部门审查。（F3）	为保证系统建设工程按照既定方案和要求实施，并达到预期要求，在工程实施完成之后，系统交付使用之前，应当指定或授权专业机构依据安全方案进行安全性测试	1访谈建设负素人在系统证线前是否展开安全性测试 2)安全性测试是否括密码应用方面的内容 一般情况下，上线前的安全测试由第三方测试单位进行，第三方测试单位是指非系统拥有者和系统建设方，第三方测试有别于开发人员或用户进行的测试，其目的是为了保证测试工作的客观性。第三方一般属于权威的专业测试机构，针对物理环境、硬件设施、软件设施等方面可能存在的缺陷或问题进行测试	1由项目承担单（部门）或公正的第三方制订安全测试方案，2进行上线前的安全性测试，并出具安全测试报告，3安全测试报告应包含密码应用安全性测试相关内容，并将测试报告报科技部门审查。	符合情况：1由项目承担单（部门）或公正的第三方制订安全测试方案，2进行上线前的安全性测试，并出具安全测试报告，3安全测试报告应包含密码应用安全性测试相关内容，并将测试报告报科技部门审查。 部分符合情况：满足1/2/3中一种或两种。 不符合情况：1/2/3均不满足
测试验收	[关键]c)新建应用系统投入生产运行前，原则上应进行不少于1个月的模拟运行和不少于3个月的试运 行。（F3）	新建应用系统投入生产运行前，原则上需要进行不少于1个月的模拟运行和不少于3个月的试运 行。	1)访谈对于新建应用系统投入生产运行前，是否进行不少于1个月的模拟运行和不少于3个月的试运 行。 2)核查相关制度文档。 3)核查是否具备相关运行记录	1进行不少于1个月的模拟运行2进行不少于3个月的试运 行。	符合情况：1新建应用系统投入生产运行前，进行不少于1个月的模拟运行。2进行不少于3个月的试运行。 部分符合情况：满足1/2中一种。 不符合情况：1/2均不满足
测试验收	[关键]d)对于在生产系统上进行的测试工作，应先进行风险分析和告知，同时制定详细的系统测试方 案、数据备份与系统恢复措施、应急处置措施后，经系统用户和主管领导审批同意后，才能 开展测试工作，以确保生产系统的安全。（F3）	对于在生产系统上进行的测试工作，需要先进行风险分析和告知，同时制定详细的系统测试方 案、数据备份与系统恢复措施、应急处置措施后，经系统用户和主管领导审批同意后，才能 开展测试工作，以确保生产系统的安全。	1)访谈系统测试工作的流程 2)核查相关制度文档。 3)核查是否具备相关测试方案、审批记录以及测试记录。	1进行风险分析和告知。2制定详细的系统测试方 案、数据备份与系统恢复措施、应急处置措施。3具备相关测试方案、审批记录以及测试记录	符合情况：1进行风险分析和告知。2制定详细的系统测试方 案、数据备份与系统恢复措施、应急处置措施。3具备相关测试方案、审批记录以及测试记录 部分符合情况：满足1/2/3中一
系统交付	[一般]a)应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点。	系统在工程实施并验收完以后，需要根据协议有关要求，按照交付清单对设备备、软件、文档进行交付	1访谈建设负责人是否对系统交付建立管控流程以及交付清单 2)核查交付清单内容	具有交付清单，交付清单对交付的各类设备、软件、文档等有明确的说明	符合情况：制定交付清单，包括交接的设备、软件和说明文档等。 部分符合情况：无。 不符合情况：未制定交付清单。
系统交付	[一般]b)应对负责运行维护的技术人员进行相应的技能培训。	系统交付时，交付单位或部门需要对运维和操作人员进行必要的培训	1)访谈建设负责人是否对运行维护人员进行技能培训 2)核查培训记录相关记录文档	具有运维技术培训相关文档，内容包括培训内容、培训时间和参与人员等方面的信息	符合情况：系统上线前对负责系统运维的技术人员进行技能培训。 部分符合情况：无 不符合情况：未对负责系统运维的技术人员进行技能培训
系统交付	[一般]c)应提供建设过程文档和运行维护文档。	交付单位或部门需提供建设过程中的文档和指导用户进行运行维护的文档，以便指导运维人员和操作人员后期的运行维护	1)访谈建设负责人建设过程的管控措施 2）核查建设过程文档和运行维护文档	在系统交付的文档中包括指导用户进行维护的文档等，且符合管理规定相关要求	符合情况：系统交付文档中包含建设过程文档和运行维护文档。 部分符合情况：无。 不符合情况：未供建设过程文档和运行维护文档。
系统交付	[关键]d)外部建设单位应与金融机构签署相关知识产权保护协议和保密协议，不得将系统采用的关键 安全技术措施和核心安全功能设计对外公开。（F3）	外部建设单位需要与金融机构签署相关知识产权保护协议和保密协议，不得将系统采用的关键 安全技术措施和核心安全功能设计对外公开。	1)访谈外部建设单位是否与金融机构签署相关知识产权保护协议和保密协议，是否在协议中明确不得将系统采用的关键 安全技术措施和核心安全功能设计对外公开。 2)核查相关制度文档。 3)核查是否具备相关协议文档。	1具备相关知识产权保护协议和保密协议 2明确不得将系统采用的关键 安全技术措施和核心安全功能设计对外公开。	符合情况：1具备相关知识产权保护协议和保密协议 2明确不得将系统采用的关键 安全技术措施和核心安全功能设计对外公开。 部分符合情况：满足1/2中一种。 不符合情况：1/2均不满足

等级测评	[关键]a)应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改。	对等级保护对象进行等级测评是检验系统达到相应等级保护要求的途径，也是发现系统安全隐患的重要途经，通过选择有资质的测评机构对系统进行定期的测评，有助于系统发现问题并进行及时的整改，就目前来说，第三级等级保护对象应当每年至少进行一次测评	1)访谈等级测评负责人是否每年定期开展等级测评 2)核查等级测评报告和整改记录	1)定期开展测评工作，且非首次，以往进行过几次测评，并根据测评结果进行相应的安全整改 2)具有以往等级测评报告和安全整改方案	符合情况：本次系统测评为首次测评。系统每年开展等级测评，针对测评的不符合项问题进行整改。 部分符合情况：无。 不符合情况：未定期进行等级测评
等级测评	[重要]b)应在发生重大变更或级别发生变化时进行等级测评。	系统在发生重大的网络结构调整或大范围的设备更换，应用系统功能变化等变更时，应重新进行等级测评，并评估系统级别是否发生变化，若变化，则需按照最新的安全保护等级要求进行测评	1)访谈测评系统是否发生过重大变更或开级 2)核查重大升级变更或改造的文件	1）有过重大变更或级别发生过变化，若有，及时开展了等级测评 2)具有相应情况下的等级测评报告	符合情况：系统在发生重大变更或级别发生变化时，重新进行等级测评。系统尚未发生重大变更或级别发生变化，在管理制度中规定，发生变化时进行等级测评、 部分符合情况：无。 不符合情况：在发生重大变更或级别发生变化时未进行等级测评
等级测评	[关键]c)应选择公安部认可的全国等级保护测评机构推荐目录中的测评单位进行等级测评，并与测评 单位签订安全保密协议。 (F3)	目前国家对等级保护测许机构的管理遵从测评机构名录管理要求,即在国家网络安全等级保护工作协调小组办公室推荐测评机构名单内的测评机构均可透，具体参见www.dibh.net	1)访谈测评负责人是否选择了具有测评资质的测评机构 2)到www.djbh.net上核查该机构是否符合要求	1等级测评的测评单位具有国家相关等级测评资质的单位 2与测评 单位签订安全保密协议	符合情况：1等级测评的测评单位具有国家相关等级测评资质的单位 2与测评 单位签订安全保密协议 部分符合情况：满足1/2中一种。 不符合情况：1/2均不满足
服务供应商选择	[关键]a)应评估服务供应商的资质、经营行为、业绩、服务体系和服务品质等要素。 (F3)	需要评估服务供应商的资质、经营行为、业绩、服务体系和服务品质等要素	1)访谈是否评估服务供应商的资质、经营行为、业绩、服务体系和服务品质等要素。 2)核查相关制度文档。 3)核查是否具备相关评估记录。	1评估服务供应商的资质、经营行为、业绩、服务体系和服务品质等要素 2具备相关评估记录。	符合情况：1评估服务供应商的资质、经营行为、业绩、服务体系和服务品质等要素 2具备相关评估记录。 部分符合情况：满足1/2中一种。 不符合情况：1/2均不满足
服务供应商选择	[重要]b)应确保服务供应商的选择符合国家的有关规定。	对各类供应商的选择均应符合国家对其的管理要求(如相关资质管理要求、销售许可要求等)	1访谈建设负责人如何选择服务商 2)核查服务商资质文件	选择的安全服务商符合国家有关规定	符合情况：由XX公司提供安全服务，该公司具有资质。符合国家有关规定。 部分符合情况：无。 不符合情况：服务供应商的选择未符合国家的规定。
服务供应商选择	[重要]c)应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。	服务提供商所提供服务的质量，将直接影响到系统的安全，为了减少或者杜绝这些服务带来新的安全问题，在选择服务商的时候，除了选择具有相应服务资质的机构，还要以协议或合同方式明确其职责以及后期的服务承诺等	1)访谈建设负责人对服务供应商的管控措施 2)核查服务供应商的服务内容和协议	具有与安全服务商签订的服务合同或安全责任合同书，并明确了后期的技术支持和服务承诺等内容	符合情况：该系统与服务提供商签订服务协议，协议中明确双方的责任和义务。 部分符合情况：无 不符合情况：未与服务供应商签订相关协议。
服务供应商选择	[一般]d)应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。	对供应商的监视和评审主要基于与其所签订协议中的网络安全相关条款和条件,验证其所提供服务与协议的符合程度，通过定期评审其工作服务报告，确保有足够的服务能力按照可行的工作计划履行其服务职责	1访谈建设负责人是否对服务供应商进行定期监督、评审和审核 2)核查对服务供应商的管理规定或要求 3)核查服务供应商服务报告或服务审核报告	1）具有安全服务商定期提交的安全服务报告 2)定期审核评价安全服务供应商所提供的服务，具有服务审核报告 3)具有安全服务商评价审核管理制度，明确了针对服务商的评价指核内容等	符合情况：指定部门对安全服务公司进行监督，对安全服务商服务变更申请，进行审核；明确一旦安全服务商变更服务内容，须评价是否符合要求。 部分符合情况：无。 不符合情况：未定期监督、评审和审核服务供应商提供的服务,并对其变更服务内容加以控制。

安全运维管理（S3A3G3）作业指导书					
安全控制点	检测项	要求解读	测评方法	预期结果或主要证据	符合情况
环境管理	[关键]a)应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理，填写机房值班记录、巡视记录。（F3）	机房是存放等级保护对象基础设施的重要场所,要落实机房环境的管理责任人，因此要确保机房的运行环境良好、安全，应对机房环境进行严格管理和控制	1)访谈物理安全负责人是否指定部门和人员负责机房安全管理工作，如对机房的出入进行管理、对基础设施(如空调、供配电设备、灭火设备等)进行定期维护 2)核查来访人员登记记录 3)来访人员记录内容是否包括了来访人员、来访时间、离开时间，携带物品等 4)核查设施维护记录 S)设施维护记录内容是否包括了维护日期、维护人、维护设备、故障维护结果等	1）指定部门和人员负责机房安全管理工作，如对机房的出入进行管理，基础设施(如空调、供配电设备、灭火设备等)进行定期维护 2)具有来访人员登记记录 3)来访人员记录内容包括了来访人员、来访时间、离开时间、携带物品等 4)具有设施维护记录护结果等 5)设施维护记界内容包格了维护日期、维护人、维护设备、故障原因、维护结果等	符合情况（全部满足）： 1）有专人定期负责维护机房基本设施；有来访人员登记记录和设备维护记录且内容完善 部分符合情况： 1）指定了部门和人员负责机房安全管理工作，但是未提供其余预期结果证据 不符合情况： 1）未指定机房负责人或者责任部门，可判为不符合 2）如果提供其余预期结果证据，但是未指定机房负责人或者责任部门，或现场测评过程中机房进出申请管理随意，可判为不符合 不适用情况： 1）云租户系统，机房管理统一为平台方管理，该项可判为不适用，但是需要提供平台方报告附录，包含物理机房情况
环境管理	[重要]b)应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定。	为保证系统有个良好安会的运行环境，应针对机房建立管理规定或要求	1)核查机房安全管理制度 2)制度内容是否包括了机房物理访问、物品带进带出机房和机房环境安全等 3)核查机房物理访问、物品带进带出机房和机房环境安全等相关记录	1)具有机房安全管理制度 2)制度内容包括了机房物理访问、物品带进带出机房和机房环境安全 3)具有机房物理访问，物品带进带出机房和机房环境安全相关记录	符合情况（全部满足）： 1）具有机房安全管理制度，内容包括了机房物理访问、物品带进带出机房和机房环境安全，且记录与制度相符。 部分符合情况： 1）具有机房安全管理制度，制度内容缺失或制度内容与实际不符， 不符合情况： 1）未建立机房安全管理制度 不适用情况： 1）云租户系统，机房管理统一为平台方管理，该项可判为不适用，但是需要提供平台方报告附录，包含物理机房情况
环境管理	[关键]c)机房布线应做到跳线整齐，跳线与配线架统一编号，标记清晰。（F3）	机房布线需要做到跳线整齐，跳线与配线架统一编号，标记清晰。	1)核查机房是否做到跳线整齐，跳线与配线架统一编号，标记清晰。	1机房布线做到跳线整齐， 2跳线与配线架统一编号，标记清晰。	符合情况：1机房布线做到跳线整齐， 2跳线与配线架统一编号，标记清晰。 部分符合情况：满足1/2中一种。 不符合情况：1/2均不满足
环境管理	[关键]d)机房管理员应经过相关培训，掌握机房各类设备的操作要领。（F3）	机房管理员需要经过相关培训，掌握机房各类设备的操作要领。	1)访谈机房管理员需要经过相关培训，是否掌握机房各类设备的操作要领。 2)核查是否具备培训记录。	机房管理员经过相关培训，掌握机房各类设备的操作要领。	符合情况：机房管理员经过相关培训，掌握机房各类设备的操作要领。 部分符合情况：/ 不符合情况：机房管理员未经过相关培训，未掌握机房各类设备的操作要领。
环境管理	[关键]e)应定期对机房设施进行维修保养，加强对易损、易失效设备或部件的维护保养。（F3）	定期对机房设施进行维修保养，加强对易损、易失效设备或部件的维护保养。	1)访谈是否定期对机房设施进行维修保养，加强对易损、易失效设备或部件的维护保养。 2)核查相关制度文档。 3)核查是否具备维修保养记录。	1定期对机房设施进行维修保养 2具备维修保养记录。	符合情况：1定期对机房设施进行维修保养 2具备维修保养记录。 部分符合情况：满足1/2中一种。 不符合情况：1/2均不满足

环境管理	[关键]f)进出机房人员应经主管部门审批同意后，由机房管理员陪同进入。（F3）	进出机房人员需要经主管部门审批同意后，由机房管理员陪同进入。	1)访谈是否进出机房人员需要经主管部门审批同意后，由机房管理员陪同进入。 2)核查相关制度文档。 3)核查是否具备审批记录。	1进出机房人员需要经主管部门审批同意后，由机房管理员陪同进入。 2具备审批记录。	符合情况：1进出机房人员需要经主管部门审批同意后，由机房管理员陪同进入。 2具备审批记录。 部分符合情况：满足1/2中一种。 不符合情况：1/2均不满足
环境管理	[关键]g)应设置弱电井，并留有足够的可扩展空间。（F3）	设置弱电井，并留有足够的可扩展空间。	1)核查机房是否设置弱电井，并留有足够的可扩展空间。	设置弱电井，留有足够的可扩展空间。	符合情况：设置弱电井，留有足够的可扩展空间。 部分符合情况：/ 不符合情况：未设置弱电井，未留有足够的可扩展空间。
环境管理	[关键]h)机房所在区域应安装24小时视频监控录像装置，重要机房区域实行24小时警卫值班，机房实 行封闭式管理，设置一个主出入口和一个或多个备用出入口，出入口控制、入侵报警和电视 监控设备运行资料应妥善保管，保存期限不少于3个月，销毁录像等资料应经单位主管领导批 准后实施。（F3）	机房所在区域需要安装24小时视频监控录像装置，重要机房区域实行24小时警卫值班，机房实 行封闭式管理，设置一个主出入口和一个或多个备用出入口，出入口控制、入侵报警和电视 监控设备运行资料应妥善保管，保存期限不少于3个月，销毁录像等资料应经单位主管领导批 准后实施。	1)核查机房所在区域是否安装24小时视频监控录像装置，重要机房区域是否实行24小时警卫值班，是否设置一个主出入口和一个或多个备用出入口。监控记录是否保存不少于3个月。 2)核查相关制度文档。 3)核查是否具备录像记录、审批文档	1机房所在区域安装24小时视频监控录像装置，重要机房区域实行24小时警卫值班，机房实 行封闭式管理，设置一个主出入口和一个或多个备用出入口， 2出入口控制、入侵报警和电视 监控设备运行资料妥善保管，保存期限不少于3个月，销毁录像等资料经单位主管领导批 准后实施。	符合情况：1机房所在区域安装24小时视频监控录像装置，重要机房区域实行24小时警卫值班，机房实 行封闭式管理，设置一个主出入口和一个或多个备用出入口， 2出入口控制、入侵报警和电视 监控设备运行资料妥善保管，保存期限不少于3个月，销毁录像等资料经单位主管领导批 准后实施。 部分符合情况：满足1/2中一种。 不符合情况：1/2均不满足
环境管理	[一般]i)应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。	加强内部办公环境的管理是控制网络安全风险的措施之一，为保证内部办公环境的独立性、敏感性，应降低外部人员无意或有意访问内部区域的可能性，同时杜绝都员工因无意行为而泄露敏感文档而导致网络安全事件的发生	1)核查办公环境的安全管理制度 2)制度内容是否明确了来访人员的接待区域 3)核查员工的办公桌面上是否含有敏感信息的纸质文件和移动介质	1)具有办公环境的安全管理制度 2） 制度内容明确了来访人员的接待区域 3)员工的办公桌面上是否含有敏感信息的纸质文件和移动介质	符合情况（全部满足）： 1）具有办公环境安全管理制度，明确来访人员的接待区域，员工的办公桌面上或公共位置不含有敏感信息的纸质文件和移动介质 部分符合情况： 1）具有办公环境安全管理制度，但是制度内容缺失或制度去实际现场环境不符 不符合情况： 1）未建立办公环境安全管理制度 不适用情况： 1）无
资产管理	[一般]a)应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。	等级保护对象资产种类较多， 如保护对象的资产管理比较混乱，容易导致等级保护对象发生安全问题或不利于发生安全问题时有效应急	1)核查资产清单 2)资产清单内容是否包括了资产范围(含设备设施、软件、文档等）、资产责任部门、重要程度和所处位置等	1)具有资产清单 2)资产清单内容包括了资产范围(含设备设施、软件、文档等)任部门、重要程度和所处位置等	符合情况（全部满足）： 1）建有资产清单，注明资产责任人，责任部门，重要程度，所属位置等 部分符合情况： 1）建有资产清单，但是是清单内信息无法追溯资产当前状况。 不符合情况： 1）未建立资产清单 不适用情况： 1）无

资产管理	[一般]b)应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施。	信息资产的重要程度不同，在系统中所起的作用也不尽相同，应综合考虑资产的价值、在系统件的地位，作用等因素，按照重要程度高低对资产进行分类、分级管理，分类的原则应在相关文档中选行明确，且需明确重要资产和非重要资产在资产管理环节(如入库、维修、出库)的不同要求	1)核查资产管理制度 2)制度内容是否包括了资产的标识方法以及不同资产的管理措施要求 3)核查资产清单中的设备是否具有相应的标识 4)核查资产清单中的设备上的标识方法是否符合相关要求	1)具有资产管理制度 2)制度内容包括了资产的标识方法以及不同资产的管理措施要求 3)资产清单中的设备具有相应的标识 4)资产清单中的设备上的标识方法符合相关要求	符合情况（全部满足）： 1）建立有资产管理制度，内容包括了资产的标识方法以及不同资产的管理措施要求 2）资产清单内资产按制度进行标识和区分类别重要程度，且根据制度区分不同的管理方法。 部分符合情况： 1）具有资产管理制度，但是制度内容缺失或制度内容与实际不符， 不符合情况： 1）未建立资产管理制度 不适用情况：
资产管理	[重要]c)应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。	信息作为资产的一种，可根据其所属的类别不同，重要程度不同进行信息的整理分类(一般可分为:敏感、内部公开、对外公开等不同类别），不同类别的信息在使用、传输和存储等方面管理要求也应不同	1)核查安全管理制度中是否明确了对信息进行分类与标识的原则和方法 2)核查安全管理制度中是否明确了对不同类信息的使用、传输和存储等操作的要求	1）安全管理制度中具有对信息进行分类与标识的原则和方法 2)安全管理制度中具有对不同类信息的使用、传输和存储等操作的要求。	符合情况（全部满足）： 1）制度中具有对信息进行分类与标识的原则和方法 2）制度中具有对不同类信息的使用、传输和存储等操作的要求。 部分符合情况： 1）制度中具有对信息进行分类与标识的原则和方法，但是与实际不符 不符合情况： 1）制度中不含有相关信息进行分类与标识的原则和方法 不适用情况：
介质管理	[一般]a)应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点。	介质类型可包括纸介质、磁介质、光介质等，由于存储介质是用来存放系统相关数据的，因此，介质管理工作非常重要，如果管理不善，可能会造成数据的丢失或损坏，应为存储介质提供安全的存放环境并进行妥善的管控	1)访谈资产管理员/存储介质管理员当前使用的存储介质类型或数据存储方式 2)访谈资产管理员/存储介质管理员当前使用的存储介质是否指派专人管理 3)核查存储介质(主要指移动存储介质，如脱机的硬盘、光盘、移动硬盘、U盘等)管理记录，记录内容是否包括了使用、归还、归档等	1）存储介质存放在指定的环境中 2)指定了部门或人员负责存储介质的管理 3)定期对存储介质进行盘点	符合情况（全部满足）： 1）介质存放和保护得到控制，存在在指定位置并有专人管理，介质归档和查询需要有相关流程记录，会对归档目录进行定期盘点 部分符合情况： 1）介质有指定位置进行存放有专人管理，但是介质归档和查询其中1个步骤流程缺失，不定期归档介质进行盘点 不符合情况： 1）介质无指定位置进行存放有专人管理， 2）介质有指定位置进行存放有专人管理，但是介质归档和查询步骤流程缺失， 不适用情况：

介质管理	[关键]b)应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，应选择安全可靠的传递、交接方式，做好防信息泄漏控制措施，并对介质的归档和查询等进行登记记录。（F3）	需系统存在离线的存储备份介质应对其进行管控，如对介质进行两地传输时，应遵循一定的管理要求，应选择可靠的传送人员，并对打包交付过程签字确认等	1)访谈资产管理员/存储介质管理员是否在存储介质的物理传输情况，如脱机的硬盘、光盘、移动硬盘、U盘等的物理传输 2)如有存储介质的物理传输，核查安全管理制度是否明确了物理传输过程的管理要求 3)核查物理介质传输的管理记录，记录内容是否包括了执行人、存储介质信息、存储介质打包、存储介质交付、存储介质归档、存储介质查询等	1)安全管理制度中具有介质在物理传输时的管理流程和要求 2)物理介质传输的管理记录，记录内容包括了执行人、存储介质信息、存储介质信打包、存储介质交付、存储介质归档、存储介质查询等	符合情况（全部满足）： 1）建立了制度，对介质物理传输过程各环节进行控制 1）对介质物理传输过程各环节有进行记录，且与制度相符 部分符合情况： 1）建立了制度，制度内容缺失或环节记录内容与制度不相符。 不符合情况： 1）未建立制度，对介质物理传输过程各环节进行控制 不适用情况：
介质管理	[关键]c)所有数据备份介质应防磁、防潮、防尘、防高温、防挤压存放。（F3）	所有数据备份介质需要防磁、防潮、防尘、防高温、防挤压存放。	1)访谈数据备份介质的存档要求以及存放地点。 2)核查相关制度文档。 3)核查当前备份介质的存放环境。	数据备份介质存放在防磁、防潮、防尘、防高温、防挤压的环境中	符合情况：数据备份介质存放在防磁、防潮、防尘、防高温、防挤压的环境中 部分符合情况：/ 不符合情况：数据备份介质未存放在防磁、防潮、防尘、防高温、防挤压的环境中
介质管理	[关键]d)对于重要文档，如是纸质文档则应实行借阅登记制度，未经相关部门领导批准，任何人不得 将文档转借、复制或对外公开，如是电子文档则应进行电子化审批流转登记管理。（F3）	对于重要文档，如是纸质文档则需要实行借阅登记制度，未经相关部门领导批准，任何人不得 将文档转借、复制或对外公开，如是电子文档则需要进行电子化审批流转登记管理。	1)访谈重要文档借阅登记流程 2)核查相关制度文档。 3)核查是否具备借阅登记记录。	1对于重要文档，如是纸质文档则需要实行借阅登记制度，未经相关部门领导批准，任何人不得 将文档转借、复制或对外公开，如是电子文档则需要进行电子化审批流转登记管理。 2具备相关制度文档和借阅登记记录。	符合情况：1对于重要文档，如是纸质文档则需要实行借阅登记制度，未经相关部门领导批准，任何人不得 将文档转借、复制或对外公开，如是电子文档则需要进行电子化审批流转登记管理。 2具备相关制度文档和借阅登记记录。 部分符合情况：满足1/2中一种。 不符合情况：1/2均不满足
介质管理	[关键]e)对载有敏感信息存储介质的销毁，应报有关部门备案，由科技部门进行信息消除、消磁或物 理粉碎等销毁处理，并做好相应的销毁记录，信息消除处理仅限于存储介质仍将在金融机构 内部使用的情况，否则应进行信息的不可恢复性销毁。（F3）	对载有敏感信息存储介质的销毁，需要报有关部门备案，由科技部门进行信息消除、消磁或物 理粉碎等销毁处理，并做好相应的销毁记录，信息消除处理仅限于存储介质仍将在金融机构 内部使用的情况，否则应进行信息的不可恢复性销毁。	1)访谈对于载有敏感信息存储介质的销毁流程 2)核查相关制度文档。 3)核查是否具备销毁记录。	1对载有敏感信息存储介质的销毁，由科技部门进行信息消除、消磁或物 理粉碎等销毁处理，2具备相关制度文档，具备销毁记录。	符合情况：1对载有敏感信息存储介质的销毁，由科技部门进行信息消除、消磁或物 理粉碎等销毁处理，2具备相关制度文档，具备销毁记录。 部分符合情况：满足1/2中一种。 不符合情况：1/2均不满足
介质管理	[关键]f)应制定移动存储介质使用规范，并定期核查移动存储介质的使用情况。（F3）	制定移动存储介质使用规范，并定期核查移动存储介质的使用情况。	1)核查是否制定移动存储介质使用规范，是否定期核查移动存储介质的使用情况。 2)核查相关制度文档。 3)核查是否具备核查记录。	1制定移动存储介质使用规范 2定期核查移动存储介质的使用情况。3具备核查记录。	符合情况：1制定移动存储介质使用规范 2定期核查移动存储介质的使用情况。3具备核查记录。 部分符合情况：满足1/2/3中一种或两种。 不符合情况：1/2/3均不满足
介质管理	[关键]g)应建立重要数据多重备份机制，其中至少1份备份介质应存放于科技部门指定的同城或异地安 全区域。（F3）	建立重要数据多重备份机制，其中至少1份备份介质应存放于科技部门指定的同城或异地安 全区域。	1)访谈是否建立重要数据多重备份机制。 2)核查相关制度文档。 3)核查是否具备备份记录。	1建立重要数据多重备份机制 2至少1份备份介质应存放于科技部门指定的同城或异地安 全区域。	符合情况：1建立重要数据多重备份机制 2至少1份备份介质应存放于科技部门指定的同城或异地安 全区域。 部分符合情况：满足1/2中一种。 不符合情况：1/2均不满足

介质管理	[关键]h)应对技术文档实行有效期管理，对于超过有效期的技术文档降低保密级别，对已经失效的技 术文档定期清理，并严格执行技术文档管理制度中的销毁和监销规定。（F3）	对技术文档实行有效期管理，对于超过有效期的技术文档降低保密级别，对已经失效的技 术文档定期清理，并严格执行技术文档管理制度中的销毁和监销规定。	1)访谈是否制定技术文档有效期管理流程，对于超过有效期的技术文档和已经失效的技 术文档是否有降低保密级别和定期清理流程。 2)核查相关制度文档。 3)核查是否具备销毁和降密记录。	1对于超过有效期的技术文档降低保密级别，对已经失效的技 术文档定期清理，2具备相关制度文档，具备销毁和降密记录。	符合情况：1对于超过有效期的技术文档降低保密级别，对已经失效的技 术文档定期清理，2具备相关制度文档，具备销毁和降密记录。 部分符合情况：满足1/2中一种。 不符合情况：1/2均不满足
介质管理	[关键]i)应定期对主要备份业务数据进行恢复验证，根据介质使用期限及时转储数据。（F3）	定期对主要备份业务数据进行恢复验证，根据介质使用期限及时转储数据。	1)访谈是否定期对主要备份业务数据进行恢复验证 2)核查相关制度文档。 3)核查是否具备恢复验证记录。	1定期对主要备份业务数据进行恢复验证，2具备相关制度文档，具备恢复验证记录。	符合情况：1定期对主要备份业务数据进行恢复验证，2具备相关制度文档，具备恢复验证记录。 部分符合情况：满足1/2中一种。 不符合情况：1/2均不满足
设备维护管理	[一般]a)应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理。	对设备进行有效的维护管理，在一定程度上可降低系统发生安全问题的概率，应明确设备管理的责任部门或人员	1）访谈设备管理员是否指派部门或专人对各类设施、设备进行定期维护管理 2)核查部门职责或人员岗位职责文档是否明确了设施、设备的维护管理责任	1)指定部门或人员对各类设施进行定期维护 2)部门职责或人员岗位职责具有文档具有设备维护管理责任	符合情况（全部满足）： 1）有专人或部门对各类设施进行定期维护 部分符合情况： 1）无 不符合情况： 1）未见专人或部门对各类设施进行定期维护 不适用情况： 1）无
设备维护管理	[一般]b)应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。	系统的正常运行依赖于对设备的正确使用和维护。为了保证对设备的正确使用和维护，应建立相应的管理规定或要求，相关人员必须严格按照规定要求对设备进行使用和维护，并认真做好使用和维护记录	1)核查设备维护管理制度是否明确维护人员的责任、维修和服务的审批、维修过程的监督控制等方面内容 2)核查是否留有维修和服务的审批、维修过程等记录，审批、记录内容是否与制度相符	1）具有设备维护管理方面的制度，在制度中明确了维护人员的责任、维修和服务的审批、维修过程的监督控制等方面内容 2)具有维修和服务的审批、维修过程等记录，审批、记录内容是否与制度相符	符合情况（全部满足）： 1）具有设备维护管理方面的制度，在制度中明确了维护人员的责任、维修和服务的审批、维修过程的监督控制等方面内容 2）具有维修和服务的审批、维修过程等记录，审批、记录内容是否与制度相符 部分符合情况： 1）具有相关制度，但是实际记录与制度不相符 不符合情况： 1）未建立相关制度 不适用情况： 1）无
设备维护管理	[关键]c)设备确需送外单位维修时，应彻底清除所存的工作相关信息，并与设备维修厂商签订保密协 议，与密码设备配套使用的设备送修前应请生产设备的科研单位拆除与密码有关的硬件，并 彻底清除与密码有关的软件和信息，并派专人在场监督。（F3）	设备确需送外单位维修时，彻底清除所存的工作相关信息，并与设备维修厂商签订保密协 议，与密码设备配套使用的设备送修前应请生产设备的科研单位拆除与密码有关的硬件，并彻底清除与密码有关的软件和信息，并派专人在场监督。	1)访谈设备送外维修的流程以及送外维修过程中的各项要求 2)核查相关制度文档。 3)核查是否具备送外维修记录。	1设备需送外单位维修时，彻底清除所存的工作相关信息，并与设备维修厂商签订保密协 议，2与密码设备配套使用的设备送修前请生产设备的科研单位拆除与密码有关的硬件，并彻底清除与密码有关的软件和信息，并派专人在场监督。3具备相关制度文档，具备送外维修记录。	符合情况：1设备需送外单位维修时，彻底清除所存的工作相关信息，并与设备维修厂商签订保密协 议，2与密码设备配套使用的设备送修前请生产设备的科研单位拆除与密码有关的硬件，并彻底清除与密码有关的软件和信息，并派专人在场监督。3具备相关制度文档，具备送外维修记录。 部分符合情况：满足1/2/3中一种或两种。 不符合情况：1/2/3均不满足

设备维护管理	[关键]d)应制定规范化的故障处理流程，建立详细的故障日（包括故障发生的时间、范围、现象、 处理结果和处理人员等内容）。（F3）	制定规范化的故障处理流程，建立详细的故障日（包括故障发生的时间、范围、现象、 处理结果和处理人员等内容）	1)访谈是否制定规范化的故障处理流程，是否建立详细的故障日（包括故障发生的时间、范围、现象、处理结果和处理人员等内容） 2)核查相关制度文档。 3)核查是否具备故障处理记录。	1制定规范化的故障处理流程 2建立详细的故障日 3具备相关制度文档，具备故障处理记录。	符合情况：1制定规范化的故障处理流程 2建立详细的故障日 3具备相关制度文档，具备故障处理记录。 部分符合情况：满足1/2/3中一种或两种。 不符合情况：1/2/3均不满足
设备维护管理	[关键]e)新购置的设备应经过验收，验收合格后方能投入使用。（F3）	新购置的设备需要经过验收，验收合格后方能投入使用。	1)访谈新购置的设备是否经过验收，验收合格后方能投入使用。 2)核查相关制度文档。 3)核查是否具备相关验收记录。	1新购置的设备经过验收，验收合格后方能投入使用。 2具备相关制度文档，具备相关验收记录。	符合情况：1新购置的设备经过验收，验收合格后方能投入使用。2具备相关制度文档，具备相关验收记录。 部分符合情况：满足1/2中一种。 不符合情况：1/2均不满足
设备维护管理	[关键]f)应制定设备管理规范，根据设备使用年限，及时进行更换升级，落实设备使用者的安全保护 责任。（F3）	制定设备管理规范，根据设备使用年限，及时进行更换升级，落实设备使用者的安全保护 责任。	1)访谈是否制定设备管理规范，是否根据设备使用年限，及时进行更换升级，落实设备使用者的安全保护 责任。 2)核查相关制度文档。 3)核查是否具备相关升级记录。	1制定设备管理规范 2根据设备使用年限，及时进行更换升级， 3具备相关制度文档，具备故障处理记录。	符合情况：1制定设备管理规范 2根据设备使用年限，及时进行更换升级， 3具备相关制度文档，具备故障处理记录。 部分符合情况：满足1/2/3中一种或两种。 不符合情况：1/2/3均不满足
设备维护管理	[重要]g)信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密。	信息处理设备的流转容易引起信息泄露的风险，必须严加管控,因此信息处理设备带离机房或办公等常规使用的地点时必须经过审批或采取加密的管控措施	1）核查设备带离机房的审批流程 2)核查设备带离机房或办公的审批记录 3)核查含有存储介质的设备带离机房的记录，记录中是否有对重要数据的加密措施	1)具有设备带离机房的审批流程 2)具有设备带离机房或办公的审批记录 3)重要数据的存储介质带出工作环境时采取XX加密措施后方可带离办公环境	符合情况（全部满足）： 1）具有设备带离机房的审批流程 2）具有审批记录证据 3）重要数据的存储介质带出工作环境时采取XX加密措施后方可带离办公环境 部分符合情况： 1）具有相关审批流程，且有审批记录，但是重要数据的存储介质带出工作环境时未采取XX加密措施，可带离办公环境 不符合情况： 1）未有审批流程 2）具有审批流程，但是无审批记录。 不适用情况： 1）无
设备维护管理	[关键]h)需要废止的设备，应由科技部门使用专用工具进行数据信息消除处理或物理粉碎等不可恢复 性销毁处理，同时备案；信息消除处理仅限于废止设备仍将在金融机构内部使用的情况，否 则应进行信息的不可恢复性销毁。（F3）	需要废止的设备，由科技部门使用专用工具进行数据信息消除处理或物理粉碎等不可恢复 性销毁处理，同时备案；信息消除处理仅限于废止设备仍将在金融机构内部使用的情况，否 则应进行信息的不可恢复性销毁。	1)访谈设备废止流程，是否对数据进行不可恢复性销毁处理。 2)核查相关制度文档。 3)核查是否具备废止销毁记录。	1需要废止的设备，由科技部门使用专用工具进行数据信息消除处理或物理粉碎等不可恢复 性销毁处理， 2具备相关制度文档，具备废止销毁记录。	符合情况：1需要废止的设备，由科技部门使用专用工具进行数据信息消除处理或物理粉碎等不可恢复 性销毁处理， 2具备相关制度文档，具备废止销毁记录。 部分符合情况：满足1/2中一种。 不符合情况：1/2均不满足

漏洞和风险管理	[重要]a)应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。	安全漏洞和隐患是引起安全问题的主要根源，采取有效的措施来及时识别系统漏洞和隐患，并对识别出的漏洞和隐患根据评估的情况进行修补	1)核查用来发现安全漏洞和隐患的措施 2)核查相关安全措施执行后的报告或记录 3)核查修复漏洞或消除隐患的操作记录	1)定期进行漏洞扫描，对发现的漏洞及时进行修补或评估可能的影响 2)具有漏洞扫描报告，报告描述了存在的漏洞、严重级别，原因分析和改进意见等方面 3)漏洞报告的时间跟定期扫描的要求相符	符合情况（全部满足）： 1）单位内部进行定期漏洞扫描，具有扫描结果记录 2）报告的时间跟定期扫描的要求相符 3）多扫描结果进行评估，并有评估结果或漏洞修补记录 部分符合情况： 1）定期进行漏洞扫描，但是不对扫描结果进行评估，或不对漏洞进行修补 不符合情况： 1）不定期进行漏洞扫描 不适用情况：
漏洞和风险管理	[重要]b)应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。	定期开展安全测评有利于及时发现系统潜在的安全问题，安全测评不局限于风险评估、等级测评，只要是通过对系统的全面测试评估方法	1)核查以往开展安全测评所获得的测评报告，确认测评工作是否定期开展 2)核查安全整改工作相关的文档，如整改方案、整改报告、工作总结等	1)具有安全测评报告 2)安全测评定期开展 3）具有安全整改工作相关的文档，如整改方案、整改报告、工作总结等	符合情况（全部满足）： 1）定期进行安全测评，并有相关测评报告 2）具有相关整改计划，整改报告，或工作总结，会议总结 部分符合情况： 1）定期进行安全测评，但是未采取措施应对发现的安全问题 不符合情况： 1）未定期进行安全测评 不适用情况：
网络和系统安全管理	[重要]a)应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限。	没有明确的责任和权限要求，容易发生泄职事件，因此要对管理员进行明确的划分并进行岗位职责的定义	1)核查管理员职责文档，确认是否划分了不同的管理员角色 2)核查管理员职责文档，确认是否明确了各个角色的责任和权限	1)管理员职责划分了不同的管理员角色 2)管理员职责明确了各个角色的责任和权限	符合情况（全部满足）： 1）职责划分有网络管理员，且任命到人 2）明确了网络管理员职责 部分符合情况： 无 不符合情况： 1）未划分角色或未任命到人 不适用情况： 1）无
网络和系统安全管理	[一般]b)应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制。	账户管理应由专门的部门或人员来负责，并对账户的生命周期进行管控	1)访谈运维负责人指派哪个部门或人员进行账户管理，含网络层面、系统面、数据库层面、 业务应用层面 2)核查账户管理记录，记录内容是否包括了账户申请、建立、停用、删除、重置等相关的审批情况。	1)指定了某部门(某岗)负责账户的管理工作 2)有相关审批记录或流程，对申请账户、建立账户、删除账户进行有效控制	符合情况（全部满足）： 1）指定了某部门(某岗)负责账户的管理工作 2）有相关审批记录或流程，对申请账户、建立账户、删除账户进行有效控制 部分符合情况： 1）指定了某部门(某岗)负责账户的管理工作，但是未见相关记录 不符合情况： 1）未制定账户管理流程。 不适用情况： 1）无

网络和系统安全管理	[重要]c)应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定。	对系统和网络安全管理缺乏规范性指导或规范性指导规定不一致，容易造成人员读职或无作为，因此对网络和系统安全应建立相应的管理策略和规程类的管理要求	1)核查网络和系统安全管理制度 2)制度内容是否包括了安全策略、账户管理(用户责任，义务，风险、权限审批、权限分配、账户注销等)、配置文件的生成及备份、变更审批、授权访问、最小服务、升级与补丁。、计日志管理、登录设备和系统的口令更新周期等	1)具有网络和系统安全管理制度 2）制度内容至少包括了安全策略、账户管理(用户责任，义务，风险、权限审批、权限分配、账户注销等)、配置文件的生成及备份、变更审批、授权访问、最小服务、升级与补丁。、计日志管理、登录设备和系统的口令更新周期等	符合情况（全部满足）： 1）具有网络和系统安全管理制度 2）制度内容至少包括了安全策略、账户管理(用户责任，义务，风险、权限审批、权限分配、账户注销等)、配置文件的生成及备份、变更审批、授权访问、最小服务、升级与补丁、计日志管理、登录设备和系统的口令更新周期等 部分符合情况： 1）具有网络和系统安全管理制度，但制度内容缺失 不符合情况： 1）未具有网络和系统安全管理制度 不适用情况： 1）无
网络和系统安全管理	[一般]d)应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等。	配置规范和配置基线是保障等级保护对象安全运行的基本前提，应对设备的配置和操作建立操作规范和配置基线	1)核查重要设备的配置和保作手册，重要设备如操作系统、数据库、网络设备、安全设备、应用和组件等 2)手册内容是否包括了操作步聚、维护方法、参数配置等	1)具有重要设备的配置和操作手册，如操件系统，数据库、网络设备、安全设备、应用和组件等的配置和操作手册 2)手册内容至少包括了操作步聚，维护方法、参数配置等	符合情况（全部满足）： 1）具有重要设备的配置和操作手册，如操件系统，数据库、网络设备、安全设备、应用和组件等的配置和操作手册 2）手册内容至少包括了操作步聚，维护方法、参数配置等 部分符合情况： 1）具有部分设备手册 不符合情况： 1）未核查到任何设备手册 不适用情况： 1）无
网络和系统安全管理	[关键]e)应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容，重 要运维操作要求至少两人在场，保留记录，并由操作和复核人员进行确认，维护记录和确认 记录应至少妥善保存6个月。（F3）	运维操作日志缺失，不利于安全事件的回溯或追踪，因此要对日常的记录运维操作日志进行详细的记录。重 要运维操作要求至少两人在场，	1)核查运维操作日志 2)日志内容是否包括了网络和系统的日常巡检、运行维护记录、参数的设置、修改等内容 3)重 要运维操作是否要求至少两人在场，	1)具有运维操作日志 2)日志内容至少包括了网络和系统的日常巡检、运行维护记录、参数的设置、修改等内容	符合情况（全部满足）： 1）具有运维操作日志 2）日志内容至少包括了网络和系统的日常巡检、运行维护记录、参数的设置、修改等内容 3）日志要与设备记录相符 4）如果依托于日志审计平台，且日志受到保护无法删除修改，且设备管理责任到人，可以给以符合 部分符合情况： 1）日志内容部分缺失 不符合情况： 1）不具有运维操作日志 不适用情况：
网络和系统安全管理	[关键]f)应制定远程访问控制规范，严禁跨境远程连接，严格控制国内远程访问范围。确因工作需要进行远程访问的，应由访问发起机构科技部门核准，提请被访问机构科技部（岗）开启远程访问服务，并采取单列账户、最小权限分配、及时关闭远程访问服务等安全防护措施。（F3）	制定远程访问控制规范，严禁跨境远程连接，严格控制国内远程访问范围。确因工作需要进行远程访问的，应由访问发起机构科技部门核准，提请被访问机构科技部（岗）开启远程访问服务，并采取单列账户、最小权限分配、及时关闭远程访问服务等安全防护措施。	1)访谈是否制定远程访问控制规范，访谈相关远程访问控制的开通流程。 2)核查相关制度文档。 3)核查是否具备审批记录。	1制定远程访问控制规范，2因工作需要进行远程访问的，应由访问发起机构科技部门核准，提请被访问机构科技部（岗）开启远程访问服务，并采取单列账户、最小权限分配、及时关闭远程访问服务等安全防护措施。 3具备审批记录。	符合情况：1制定远程访问控制规范，2因工作需要进行远程访问的，应由访问发起机构科技部门核准，提请被访问机构科技部（岗）开启远程访问服务，并采取单列账户、最小权限分配、及时关闭远程访问服务等安全防护措施。 3具备审批记录。 部分符合情况：满足1/2/3中一种或两种。 不符合情况：1/2/3均不满足

网络和系统安全管理	[关键]g)各机构应以不影响正常网络传输为原则，合理控制多媒体网络应用规模和范围，未经科技主 管部门批准，不得在内部网络上提供跨辖区视频点播等严重占用网络资源的多媒体网络应用。 (F3)	各机构以不影响正常网络传输为原则，合理控制多媒体网络应用规模和范围，未经科技主 管部门批准，不得在内部网络上提供跨辖区视频点播等严重占用网络资源的多媒体网络应用。	1)访谈多媒体网络应用的控制方法以及审批流程 2)核查相关制度文档。 3)核查是否具备审批记录。	1合理控制多媒体网络应用规模和范围，不得在内部网络上提供跨辖区视频点播等严重占用网络资源的多媒体网络应用。 2具备相关制度文档，具备审批记录。	符合情况：1合理控制多媒体网络应用规模和范围，不得在内部网络上提供跨辖区视频点播等严重占用网络资源的多媒体网络应用。 2具备相关制度文档，具备审批记录。 部分符合情况：满足1/2中一种或两种。 不符合情况：1/2均不满足
网络和系统安全管理	[关键]h)网络安全管理人员经本部门主管领导批准后，有权对本机构或辖内网络进行安全检测、扫描， 检测、扫描结果属敏感信息，未经授权不得对外公开，未经科技主管部门授权，任何外部机 构与人员不得检测或扫描机构内部网络。 (F3)	网络安全管理人员经本部门主管领导批准后，有权对本机构或辖内网络进行安全检测、扫描， 检测、扫描结果属敏感信息，未经授权不得对外公开，未经科技主管部门授权，任何外部机 构与人员不得检测或扫描机构内部网络。	1)访谈网络安全管理人员经本部门主管领导批准后，是否有权对本机构或辖内网络进行安全检测、扫描。针对于扫描结果的处理流程。 2)核查相关制度文档。 3)核查是否具备安全检测、扫描记录	1网络安全管理人员经本部门主管领导批准后，有权对本机构或辖内网络进行安全检测、扫描， 检测、扫描结果属敏感信息， 2未经科技主管部门授权，任何外部机 构与人员不得检测或扫描机构内部网络。 3具备相关制度文档，具备安全检测、扫描记录	符合情况：1网络安全管理人员经本部门主管领导批准后，有权对本机构或辖内网络进行安全检测、扫描， 检测、扫描结果属敏感信息， 2未经科技主管部门授权，任何外部机 构与人员不得检测或扫描机构内部网络。 3具备相关制度文档，具备安全检测、扫描记录 部分符合情况：满足1/2/3中一种或两种。 不符合情况：1/2/3均不满足
网络和系统安全管理	[关键]i)金融行业网间互联安全应实行统一规范、分级管理、各负其责的安全管理模式，未经金融机 构科技主管部门核准，任何机构不得自行与外部机构实施网间互联。 (F3)	金融行业网间互联安全实行统一规范、分级管理、各负其责的安全管理模式，未经金融机 构科技主管部门核准，任何机构不得自行与外部机构实施网间互联。	1)访谈网间互联的安全管理模式和处理流程。 2)核查相关制度文档。 3)核查是否具备审批、开通记录	1金融行业网间互联安全实行统一规范、分级管理、各负其责的安全管理模式，2未经金融机 构科技主管部门核准，任何机构不得自行与外部机构实施网间互联。 3具备相关制度文档，具备审批、开通记录	符合情况：1金融行业网间互联安全实行统一规范、分级管理、各负其责的安全管理模式，2未经金融机 构科技主管部门核准，任何机构不得自行与外部机构实施网间互联。 3具备相关制度文档，具备审批、开通记录 部分符合情况：满足1/2/3中一种或两种。 不符合情况：1/2/3均不满足
网络和系统安全管理	[关键]j)所有网间互联应用系统和外联网络区应定期进行威胁评估和脆弱性评估并提供威胁和脆弱性 评估报告。 (F3)	所有网间互联应用系统和外联网络区定期进行威胁评估和脆弱性评估并提供威胁和脆弱性 评估报告。	1)访谈是否定期对所有网间互联应用系统和外联网络区进行威胁评估和脆弱性评估并提供威胁和脆弱性评估报告。 2)核查相关制度文档。 3)核查是否具备评估报告。	1所有网间互联应用系统和外联网络区定期进行威胁评估和脆弱性评估 2具备威胁和脆弱性 评估报告。 3具备相关制度文档。	符合情况：1所有网间互联应用系统和外联网络区定期进行威胁评估和脆弱性评估 2具备威胁和脆弱性 评估报告。 3具备相关制度文档。 部分符合情况：满足1/2/3中一种或两种。 不符合情况：1/2/3均不满足
网络和系统安全管理	[关键]k)系统管理员不应兼任业务操作人员，系统管理员不应对业务数据进行任何增加、删除、修改 等操作，系统管理员确需对数据库系统进行业务数据维护操作的，应征得业务部门审批，并 详细记录维护内容、人员、时间等信息。 (F3)	系统管理员不应兼任业务操作人员，系统管理员不应对业务数据进行任何增加、删除、修改 等操作，系统管理员确需对数据库系统进行业务数据维护操作的，应征得业务部门审批，并 详细记录维护内容、人员、时间等信息。	1)访谈系统管理员是否兼任业务操作人员，系统管理员权限是否合理分配 2)核查相关制度文档。 3)核查是否具备权限审批和分配记录。	1系统管理员不应兼任业务操作人员 2系统管理员无法对业务数据进行任何增加、删除、修改 等操作， 3系统管理员确需对数据库系统进行业务数据维护操作的，征得业务部门审批，并详细记录维护内容、人员、时间等信息。 4具备相关制度文档，具备权限审批和分配记录。	符合情况：1系统管理员不应兼任业务操作人员 2系统管理员无法对业务数据进行任何增加、删除、修改 等操作， 3系统管理员确需对数据库系统进行业务数据维护操作的，征得业务部门审批，并详细记录维护内容、人员、时间等信息。 4具备相关制度文档，具备权限审批和分配记录。 部分符合情况：满足1/2/3/4中一种或两种。 不符合情况：1/2/3/4均不满足

网络和系统安全管理	[关键]l)每半年应至少进行一次漏洞扫描，对发现的安全漏洞及时进行修补，扫描结果应及时上报。（F3）	每半年至少进行一次漏洞扫描，对发现的安全漏洞及时进行修补，扫描结果应及时上报。	1)访谈是否每半年至少进行一次漏洞扫描，对发现的安全漏洞及时进行修补，扫描结果应及时上报。 2)核查相关制度文档。 3)核查是否具备扫描记录和上报记录。	1每半年至少进行一次漏洞扫描 2对发现的安全漏洞及时进行修补，扫描结果应及时上报。 3具备相关制度文档，具备扫描记录和上报记录。	符合情况：1每半年至少进行一次漏洞扫描 2对发现的安全漏洞及时进行修补，扫描结果应及时上报。 3具备相关制度文档，具备扫描记录和上报记录。 部分符合情况：满足1/2/3中一种或两种。 不符合情况：1/2/3均不满足
网络和系统安全管理	[一般]m)应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为。	没有明确的职责要求，容易引起人员读职或无作为，应对日志、 监测、报警数据等指定专人负责和统计	1)访谈网络和系统相关人员是否指派部门或人员对日志、监测和报警数据等进行统计、分析 2）核查日志、监测和报警数据的统计、分析的报告	1)指派了部门或人员对对日志、监测和报警数据等进行统计、分析 2)具有日志、监测和报警数据的统计、分析的报告	符合情况（全部满足）： 1）指派了部门或人员对对日志、监测和报警数据等进行统计、分析 2）具有日志、监测和报警数据的统计、分析的报告 部分符合情况： 1）无 不符合情况： 1）未指派部门或人员对对日志、监测和报警数据等进行统计、分析 2）指派了部门或人员对对日志、监测和报警数据等进行统计、分析，但未实际进行 不适用情况：
网络和系统安全管理	[重要]n)应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库。	变更管理不当， 极易引起安全问题，对运维过程中的变更操作需严格控制，变更的审批过程中保留痕迹，事后能够更新变更内容	1)核查配置变更审批程序，如对改变连接、 安装系统组件或调整配置参数的审批流程 2)核查配置变更审计日志 3）核查配置变更记录 4)核查配置信息库更新记录	1)具有配置变更审批程序，如对改变连接、 安装系统组件或调整配置参数的审批流程 2)核查配置变更审计日志 3）核查配置变更记录 4)核查配置信息库更新记录	符合情况（全部满足）： 1）具有变更流程 2）具有变更操作日志 3）如果是配置变更需要配置信息科更新 部分符合情况： 1）如果上数条款没有配置信息库，可以直接给予部分符合 2）具有变更流程，但是未记录 不符合情况： 1）管理员可以随意进行变更，且不进行任意记录 不适用情况： 1）无
网络和系统安全管理	[重要]o)应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据。	IT运维工具包括商业的专用运维工具，也有自行开发运维工具，无论采取哪种工具，都需进行严格的管控	1)核查运维工具的使用审批程序 2)核查运维工具的使用审批记录 3)核查通过运维工具执行操作的审计日志	1)具有运维工具的使用审批程序 2)具有运维工具的使用审批记录 3)具有通过运维工具执行操作的审计日志	符合情况（全部满足）： 1）具有运维工具的使用审批程序 2）具有运维工具的使用审批记录 3）具有通过运维工具执行操作的审计日志 部分符合情况： 1）不对运维工具接入进行控制，但是具有审计日志 不符合情况： 1）不对运维工具接入进行控制，且未有审计日志 不适用情况：

网络和系统安全管理	[重要]p)应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道。	远程运维是系统安全的隐患之一，如远程控制不当容易通成安全事件，应对远程运维的开通进行严格的控制，如确实需要开通，需要对操作过程日志进行留存并保证不可更改，运维结束后即刻关闭	1)核查远程运维的方式，使用的端口或通道 2)核查开通远程运维的审批程序 3)核查开通远程运维的审批记录 4)核查通过远程运维执行操作的审计日志	1)具有远程运维的方式，使用的端口或通道 2)具有开通远程运维的审批程序 3)具有开通远程运维的审批记录 4)具有通过远程运维执行操作的审计日志	符合情况（全部满足）： 1)具有开通远程运维的审批程序 2)具有开通远程运维的审批记录 3)具有通过远程运维执行操作的审计日志 部分符合情况： 1）远程运维不需要审批，不需要记录，单含有审计日志 不符合情况： 1）远程运维不需要审批，不需要记录，且无审计日志 不适用情况： 1）系统不涉及远程运维场景。
网络和系统安全管理	[重要]应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。	对所有外部链接进行管控，并且定期对违规外联进行检查	1)核查开通对外连接的审批程序 2)核查开通对外连接的审批记录。 3)核查开展违反规定无线上网及其他违反网络安全策略行为的检查记录	1)具有开通对外连接的审批程序 2)具有开通对外连接的审批记录。 3)具有开展违反规定无线上网及其他违反网络安全策略行为的检查记录	符合情况（全部满足）： 1）具有开通对外连接的审批程序，并进行控制，且对办公环境进行上网行为管理，并进行记录。 部分符合情况： 1）办公环境上网行为，未进行管理。 不符合情况： 1）不对生产网上网行为进行管理。 不适用情况： 1）无
恶意代码防范管理	[重要]a)应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等。	恶意代码对等级保护对象的危害极大，并且传播途径有多种方式，提升所有用户的防恶意代码意识是规避恶意代码发生概率的基本途径。恶意代码的防范不仅仅需要安装防恶意代码工具来解决，为有效预防恶意代码的侵入，除了提高用户的防恶意代码意识外，还应建立完美的恶意代码管理制度并有效实施	1)核查提升员工防恶意代码意识的培训或宣传记录 2)核查恶意代码防范管理制度 3)核查外来计算机或存储设备接入系统前进行恶意代码检查记录	1)开展提升员工防恶意代码意识的培训或宣传记录 2)具有恶意代码防范管理制度 3)开展外来计算机或存储设备接入系统前进行恶意代码检查记录	符合情况（全部满足）： 1）建立相关恶意代码防范管理制度 2）开展外来计算机或存储设备接入系统前进行恶意代码检查记录 部分符合情况： 1）存在检测中有未按恶意代码防范管理制度进行防护 2）未开展外来计算机或存储设备接入系统前进行恶意代码检查记录 不符合情况： 1）未建立恶意代码防范管理制度 不适用情况：
恶意代码防范管理	[重要]b)应定期验证防范恶意代码攻击的技术措施的有效性。	防恶意代码工具的技术措施最常见的是安装恶意代码软件，该类措施有效性保障就是定期升级恶意代码库，并对检测的恶意代码进行分析，另外如采用可信计算机技术也可防恶意代码攻击，需定期验证可信技术的有效性	1）核查恶意代码防范措施 2）核查恶意代码防范措施执行记录 3)核查恶意代码防范措施特征库的更新记录	1）具有恶意代码防范措施 2）具有查恶意代码防范措施执行记录 3)具有恶意代码防范措施特征库的更新记录	符合情况（全部满足）： 1）具有恶意代码防范措施 2）具有恶意代码防范措施特征库的更新记录 部分符合情况： 1）无 不符合情况： 1）未具有恶意代码防范措施 2）未具有恶意代码防范措施特征库的更新记录 不适用情况：

恶意代码防范管理	[关键]c)客户端应统一安装病毒防治软件，设置用户口令和屏幕保护口令等安全防护措施，确保及时更新病毒特征码并安装必要的补丁程序。（F3）	客户端统一安装病毒防治软件，设置用户口令和屏幕保护口令等安全防护措施，确保及时更新病毒特征码并安装必要的补丁程序。	1)访谈客户端是否统一安装病毒防治软件，是否设置用户口令和屏幕保护口令等安全防护措施 2)核查相关制度文档。 3)核查是否具备安装记录、升级记录。	1客户端统一安装病毒防治软件， 2设置用户口令和屏幕保护口令等安全防护措施，3及时更新病毒特征码并安装必要的补丁程序。 4具备相关制度文档，具备安装记录、升级记录。	符合情况：1客户端统一安装病毒防治软件， 2设置用户口令和屏幕保护口令等安全防护措施，3及时更新病毒特征码并安装必要的补丁程序。 4具备相关制度文档，具备安装记录、升级记录。 部分符合情况：满足1/2/3/4中一种或两种。 不符合情况：1/2/3/4均不满足
配置管理	[重要]a)应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。	系统配置信息的准确性，是系统正常运行的有效保障，因此要对系统的基本信息予以及时有效的记录和保存	1)核查配置信息保存记录 2)记录内容是否包括了网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等	记录和保存基本的配置信息，配置信息主要包括:网络拓扑、软件组件、设备配置等内容	符合情况（全部满足）： 1）记录和保存基本的配置信息，配置信息主要包括:网络拓扑、软件组件、设备配置等内容 部分符合情况： 1）记录配置信息不全面 不符合情况： 1）未记录配置信息 不适用情况： 1）无
配置管理	[一般]b)应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。	配置信息及时间同步是配置管理流程的重要环节，该条要求与变更管理和系统管理中的相关条款比较类似，应关注几方面信息保持一致	1）核查配置变更管理程序 2)核查配置信息变更记录	1)具有记录和保存配置信息的管理措施，且基本配置信息改变后会及时更新配置信息库 2)对配置信息的变更流程具有相应的管控程序或手段	符合情况（全部满足）： 1）核查配置信息修改是否包含在变更管理制度内 部分符合情况： 1）未见相关制度，但是有相关配置信息变更的记录 不符合情况： 1）未见相关制度，未见相关配置信息变更的记录 不适用情况：
密码管理	[关键]a)应遵循密码相关国家标准和行业标准。	密码生产需要授权许可，密码产品需要符合国家和行业的相关标准	1)访谈安全管理员当前使用的密码产品类型 2)如果使用密码产品，核查密码产品的商用密码产品型号证书或国家相关部门出具的检测报告中所遵循的相关国家标准和行业标准	1)确认密码产品类别、型号 2)具有商用密码产品型号证书	符合情况（全部满足）： 1）当前密码产品与服务遵循相关的国家标准和行业标准 部分符合情况： 2）无 不符合情况： 3）当前密码产品与服务未遵循相关的国家标准和行业标准 不适用情况： 1）无
密码管理	[关键]b)应使用国家密码管理主管部门认证核准的密码技术和产品。	系统使用的密码产品要有国家密码主管部门核发的相关型号证书	核查密码产品是否具有销售许可证明或国家相关部门出具的检测报告	密码产品具有商用密码产品型号证书	符合情况（全部满足）： 1）当前密码产品与服务遵循相关的国家标准和行业标准 部分符合情况： 2）无 不符合情况： 3）当前密码产品与服务未遵循相关的国家标准和行业标准 不适用情况： 1）无

密码管理	[关键]c)应建立对所有密钥的产生、分发和接收、使用、存储、更新、销毁等方面进行管理的制度，密钥管理人员应是本机构在编的正式员工，并逐级进行备案，规范密钥管理。（F3）	建立对所有密钥的产生、分发和接收、使用、存储、更新、销毁等方面进行管理的制度，密钥管理人员应是本机构在编的正式员工，并逐级进行备案，规范密钥管理。	1)访谈是否建立对所有密钥的产生、分发和接收、使用、存储、更新、销毁等方面进行管理的制度，密钥管理人员是否是本机构在编的正式员工，是否逐级进行备案，规范密钥管理。 2)核查相关制度文档。 3)核查是否具备备案记录。	1建立对所有密钥的产生、分发和接收、使用、存储、更新、销毁等方面进行管理的制度 2密钥管理人员是本机构在编的正式员工，并逐级进行备案，规范密钥管理。 3具备相关制度文档，具备备案记录。	符合情况：1建立对所有密钥的产生、分发和接收、使用、存储、更新、销毁等方面进行管理的制度 2密钥管理人员是本机构在编的正式员工，并逐级进行备案，规范密钥管理。 3具备相关制度文档，具备备案记录。 部分符合情况：满足1/2/3中一种或两种。 不符合情况：1/2/3均不满足
密码管理	[关键]d) 系统管理员、数据库管理员、网络管理员、业务操作人员均应设置口令密码，并每半年更换，口令密码的强度应满足不同安全性要求。（F3）	系统管理员、数据库管理员、网络管理员、业务操作人员均设置口令密码，并每半年更换，口令密码的强度应满足不同安全性要求。	1)访谈系统管理员、数据库管理员、网络管理员、业务操作人员是否均设置口令密码，是否每半年更换，口令密码的强度是否满足不同安全性要求。 2)核查相关制度文档。 3)核查是否具备口令更换记录、安全性要求。	1系统管理员、数据库管理员、网络管理员、业务操作人员均设置口令密码，2口令每半年更换，口令密码的强度应满足不同安全性要求。3具备相关制度文档，具备口令更换记录、安全性要求。	符合情况：1系统管理员、数据库管理员、网络管理员、业务操作人员均设置口令密码，2口令每半年更换，口令密码的强度应满足不同安全性要求。3具备相关制度文档，具备口令更换记录、安全性要求。 部分符合情况：满足1/2/3中一种或两种。 不符合情况：1/2/3均不满足
密码管理	[关键]e)系统和设备的口令密码设置应在安全的环境下进行，必要时应将口令密码纸质密封交相关部门保管，未经科技部门主管领导许可，任何人不得擅自拆阅密封的口令密码，拆阅后的口令密码使用后应立即更改并再次密封存放。（F3）	系统和设备的口令密码设置在安全的环境下进行，必要时应将口令密码纸质密封交相关部门保管，未经科技部门主管领导许可，任何人不得擅自拆阅密封的口令密码，拆阅后的口令密码使用后应立即更改并再次密封存放。	1)访谈系统和设备的口令密码设置是否在安全的环境下进行，必要时是否将口令密码纸质密封交相关部门保管，拆阅后的口令密码使用后是否立即更改并再次密封存放。 2)核查相关制度文档。 3)核查是否具备口令保存文档、记录	1系统和设备的口令密码设置在安全的环境下进行，必要时将口令密码纸质密封交相关部门保管， 2拆阅后的口令密码使用后立即更改并再次密封存放。 3具备相关制度文档，具备口令保存文档、记录。	符合情况：1系统和设备的口令密码设置在安全的环境下进行，必要时将口令密码纸质密封交相关部门保管， 2拆阅后的口令密码使用后立即更改并再次密封存放。 3具备相关制度文档，具备口令保存文档、记录。 部分符合情况：满足1/2/3中一种或两种。 不符合情况：1/2/3均不满足
密码管理	[关键]f)密钥注入、密钥管理功能调试和密钥档案的保管应由专人负责，密钥资料须保存在保险柜内，保险柜钥匙由专人负责，使用密钥和销毁密钥要在监督下进行并应有使用、销毁记录。（F3）	密钥注入、密钥管理功能调试和密钥档案的保管由专人负责，密钥资料须保存在保险柜内，保险柜钥匙由专人负责，使用密钥和销毁密钥要在监督下进行并应有使用、销毁记录。	1)访谈密钥注入、密钥管理功能调试和密钥档案的保管是否由专人负责，密钥资料是否保存在保险柜内，使用密钥和销毁密钥是否在监督下进行并应有使用、销毁记录。 2)核查相关制度文档。 3)核查是否具备保存记录、使用销毁记录。	1密钥注入、密钥管理功能调试和密钥档案的保管由专人负责，密钥资料须保存在保险柜内， 保险柜钥匙由专人负责， 2使用密钥和销毁密钥要在监督下进行并有使用、销毁记录。 3具备相关制度文档，具备保存记录、使用销毁记录。	符合情况：1密钥注入、密钥管理功能调试和密钥档案的保管由专人负责，密钥资料须保存在保险柜内， 保险柜钥匙由专人负责， 2使用密钥和销毁密钥要在监督下进行并有使用、销毁记录。 3具备相关制度文档，具备保存记录、使用销毁记录。 部分符合情况：满足1/2/3中一种或两种。 不符合情况：1/2/3均不满足
密码管理	[关键]g)确因工作需要经授权可远程接入内部网络的用户，应妥善保管其身份认证介质及口令密码，不得转借他人使用。（F3）	确因工作需要经授权可远程接入内部网络的用户，需要妥善保管其身份认证介质及口令密码，不得转借他人使用。	1)访谈针对确因工作需要经授权可远程接入内部网络的用户，其账户口令的保管要求 2)核查相关制度文档。	1因工作需要经授权可远程接入内部网络的用户，妥善保管其身份认证介质及口令密码，不得转借他人使用。 2具备相关制度文档	符合情况：1因工作需要经授权可远程接入内部网络的用户，妥善保管其身份认证介质及口令密码，不得转借他人使用。 2具备相关制度文档 部分符合情况：满足1/2中一种。 不符合情况：1/2均不满足
密码管理	[关键]h)应支持各类环境中密码设备使用、管理权限分离。（F3）	支持各类环境中密码设备使用、管理权限分离。	1)访谈各类环境中密码设备使用、管理是否权限分离。 2)核查相关制度文档。	1支持各类环境中密码设备使用、管理权限分离。 2具备相关制度文档	符合情况：1支持各类环境中密码设备使用、管理权限分离。 2具备相关制度文档 部分符合情况：满足1/2中一种。 不符合情况：1/2均不满足

变更管理	[关键]a)变更管理应流程化、文档化和制度化，变更流程中应明确变更发起方、实施方的职责，应明 确变更方案的测试、审批流程及实施策略，对有可能影响客户利益的变更应事先通知客户并 得到客户的确认。（F3）	变更管理流程化、文档化和制度化，变更流程中明确变更发起方、实施方的职责，明 确变更方案的测试、审批流程及实施策略，对有可能影响客户利益的变更应事先通知客户并 得到客户的确认。	1)访谈变更管理是否流程、文档化和制度化，流程中是否明确变更发起方、实施方的职责。是否明确变更方案的测试、审批流程及实施策略，对有可能影响客户利益的变更是否事先通知客户并 得到客户的确认。 2)核查相关制度文档。 3)核查是否具备变更方案、测试记录、实施记录。	1变更管理流程化、文档化和制度化， 2变更流程中明确变更发起方、实施方的职责，明 确变更方案的测试 、审批流程及实施策略，对有可能影响客户利益的变更应事先通知客户并 得到客户的确认。 3具有相关制度文档，具备变更方案、测试记录、实施记录。	符合情况：1变更管理流程化、文档化和制度化， 2变更流程中明确变更发起方、实施方的职责，明 确变更方案的测试、审批流程及实施策略，对有可能影响客户利益的变更应事先通知客户并 得到客户的确认。 3具有相关制度文档，具备变更方案、测试记录、实施记录。 部分符合情况：满足1/2/3中一种或两种。 不符合情况：1/2/3均不满足
变更管理	[重要]b)应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。	变更管理受控是降低系统由变更带来安全问题的有效手段，因此要对变更策略进行明确的规定，并对变更流程进行全程管控	1)核查变更方案，方案内容是否包括了变更类型，变更原因，变更过程、变更前评估等内容 2)核查变更方案评审记录,记录内容是否包括了评审时间、参与人员、评审结果等 3)核查变更过程记录，记录内容是是否包括了变更执行人，执行时间、操作内容、变更内容等	1)具有相应的变更方案，方案内容是否包括了变更类型，变更原因，变更过程、变更前评估等内容 2)具有XXX变更方案评审记录和变更过程记录文档 3)对于新建或执行过变更操作的被测系统，此条可不适用	符合情况（全部满足）： 1）具有相应的变更方案，方案内容是否包括了变更类型，变更原因，变更过程、变更前评估等内容 部分符合情况： 1）变更方案，内容不全面 不符合情况： 1）未含有变更方案，管理员随意进行系统变更。 不适用情况：
变更管理	[一般]c)应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程。	执行变更操作要遵循变更管控的相关控制程序，约束变更过程，并有效记录	1)核查变更控制的申报、控制审批程序 2)核查变更实施过程的记录 3)记录的内容是否包括申报的变更类型、申报流程、审批部门、批准人等	1)不同变更类型具有相应的变更管控策略，如变更类型、变更原因、变更影响分析等 2)具有XXX变更实施过程的记录文档 3)对于新建或未执行过变更操作的被测系统，可没有相关记录	符合情况（全部满足）： 1）不同变更类型具有相应的变更管控策略，如变更类型、变更原因、变更影响分析等 部分符合情况： 1）无 不符合情况： 1）未建立不同变更类型具有相应的变更管控策略 不适用情况：
变更管理	[一般]d)应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。	变更失败恢复程序一般会在变更方案中予以明确，变更方案除了描述变更过程操作外，重要的是明确变更失败后的恢复操作	1）核查变更失败后的恢复程序、工作方法和相关人员职责。 2)核查恢复过程演练记录	1）对变更失败后的恢复程序、工作方法和职责进行了文件化的规定和要求，具有变更失败后的恢复程序 2)具有XX变更恢复演练记录和恢复流程 3)对于新建或未执行过变更操作的被测系统，可没有相关记录	符合情况（全部满足） 1）建立变更失败恢复程序 部分符合情况： 1）无 不符合情况： 1）未建立变更失败恢复程序 不适用情况： 1）无
变更管理	[关键]e)变更前应做好系统和数据的备份，风险较大的变更，应在变更后对系统的运行情况进行跟踪。（F3）	变更前做好系统和数据的备份，风险较大的变更，在变更后对系统的运行情况进行跟踪。	1)访谈变更前是否做好系统和数据的备份，风险较大的变更，是否在变更后对系统的运行情况进行跟踪。 2)核查相关制度文档。 3)核查是否具备变更记录和跟踪记录	1变更前做好系统和数据的备份，风险较大的变更，在变更后对系统的运行情况进行跟踪。 2具备相关制度文档，具备变更记录和跟踪记录，	符合情况：1变更前做好系统和数据的备份，风险较大的变更，在变更后对系统的运行情况进行跟踪。 2具备相关制度文档，具备变更记录和跟踪记录， 部分符合情况：满足1/2中一种或两种。 不符合情况：1/2均不满足

变更管理	[关键]f)如果需要对生产环境进行重大变更，应按变更管理流程，制订详细的系统变更方案、系统及数据备份恢复措施和应急处置方案，经测试环境稳妥测试通过，系统用户和主管领导审批同 意后，再进行变更操作，以确保生产系统的安全。（F3）	如果需要对生产环境进行重大变更，按变更管理流程，制订详细的系统变更方案、系统及数据备份恢复措施和应急处置方案，经测试环境稳妥测试通过，系统用户和主管领导审批同 意后，再进行变更操作，以确保生产系统的安全。	1)访谈针对生产环境进行重大变更，是否按变更管理流程，制订详细的系统变更方案、系统及数据备份恢复措施和应急处置方案， 2)核查相关制度文档。 3)核查是否具备变更方案、备份恢复措施、应急处置预案、测试记录。	1对生产环境进行重大变更，按变更管理流程，制订详细的系统变更方案、系统及数据备份恢复措施和应急处置方案，经测试环境稳妥测试通过，系统用户和主管领导审批同 意后，再进行变更操作，以确保生产系统的安全。 2具备相关制度文档，具备变更方案、备份恢复措施、应急处置预案、测试记录。	符合情况：1对生产环境进行重大变更，按变更管理流程，制订详细的系统变更方案、系统及数据备份恢复措施和应急处置方案，经测试环境稳妥测试通过，系统用户和主管领导审批同 意后，再进行变更操作，以确保生产系统的安全。 2具备相关制度文档，具备变更方案、备份恢复措施、应急处置预案、测试记录。 部分符合情况：满足1/2中一种或两种。 不符合情况：1/2均不满足
变更管理	[关键]g)当生产中心发生变更时，应同步分析灾备系统变更需求并进行相应的变更，评估灾备恢复的 有效性，应尽量减少紧急变更。（F3）	当生产中心发生变更时，应同步分析灾备系统变更需求并进行相应的变更，评估灾备恢复的 有效性，应尽量减少紧急变更。	1)访谈当生产中心发生变更时是否同步分析灾备系统变更需求并进行相应的变更，是否评估灾备恢复的有效性， 2)核查相关制度文档。 3)核查是否具备变更记录、评估记录。	1生产中心发生变更时，同步分析灾备系统变更需求并进行相应的变更， 2评估灾备恢复的 有效性， 3具备相关制度文档，具备变更记录、评估记录。	符合情况：1生产中心发生变更时，同步分析灾备系统变更需求并进行相应的变更， 2评估灾备恢复的 有效性， 3具备相关制度文档，具备变更记录、评估记录。 部分符合情况：满足1/2/3中一种或两种。 不符合情况：1/2/3均不满足
备份与恢复管理	[一般]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。	对于要备份的信息进行识别，并制定相应的备份策略	核查数据备份策略，策略内容至少明确了备份周期、备份的信息类别或数据类型	1)具有数据备份策略 2)数据备份策略内容至少包括了备份周期、备份的信息类别或数据类型	符合情况（全部满足）： 1）建立备份策略，对系统需要备份的内容进行识别 部分符合情况： 1）备份周期不合理，但是有进行备份 不符合情况： 1）未建立相关备份制度 不适用情况： 1）无
备份与恢复管理	[一般]b)应规定备份信息的备份方式、备份频度、存储介质、保存期等。	对需要备份的制定相应的备份策略，如备份方式、备份频度、存储介质等等	核查备份与恢复管理制度，制度内容至少明确了备份方式、备份频度、存储介质、保存期等	1)具有备份与恢复管理制度 2)制度内容至少包括了备份方式、备份频度、存储介质、保存期等	符合情况（全部满足）： 1）具有备份与恢复管理制度 2）制度内容至少包括了备份方式、备份频度、存储介质、保存期等 部分符合情况： 1）建立了备份与恢复管理制度，但是制度内容不全面 不符合情况： 1）未建立备份与恢复管理制度 不适用情况：
备份与恢复管理	[重要]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、备份程序和恢复程序等。	数据备份策略是根据数据性质的不同，选择不同的备分内容、备份方式等，数据恢复策略是指数据库在遭到各种事件导致数据丢失时利用介质备份数据进行恢复的方法和操作	1)核查是否有数据备份策略、备份程序 2)核查是否具有数据恢复策略、恢复程序	1)具有数据备份策略、备份程序 2)具有数据恢复策略、恢复程序	符合情况（全部满足）： 1）具有备份与恢复管理制度，且制度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、备份程序和恢复程序等 部分符合情况： 1）未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、备份程序和恢复程序等 不符合情况： 1）未根据 不适用情况：

备份与恢复管理	[关键]d)应每年至少进行一次重要信息系统专项应急切换演练，每三年至少进行一次重要信息系统全 面灾备切换演练，根据不同的应急恢复内容，确定演练的周期，并指定专人管理和维护应急 预案，根据人员、信息资源等变动情况以及演练情况适时予以更新和完善，确保应急预案的 有效性和灾难发生时的可获取性。（F3）	每年至少进行一次重要信息系统专项应急切换演练，每三年至少进行一次重要信息系统全 面灾备切换演练，根据不同的应急恢复内容，确定演练的周期，并指定专人管理和维护应急 预案，根据人员、信息资源等变动情况以及演练情况适时予以更新和完善，确保应急预案的 有效性和灾难发生时的可获取性	1)访谈是否每年至少进行一次重要信息系统专项应急切换演练，每三年至少进行一次重要信息系统全 面灾备切换演练，是否制定应急恢复内容 2)核查相关制度文档。 3)核查是否具备应急切换演练记录。	1每年至少进行一次重要信息系统专项应急切换演练，2每三年至少进行一次重要信息系统全 面灾备切换演练， 3根据不同的应急恢复内容，确定演练的周期，并指定专人管理和维护应急 预案，根据人员、信息资源等变动情况以及演练情况适时予以更新和完善，4 具备相关制度文档，具备应急切换演练记录。	符合情况：1每年至少进行一次重要信息系统专项应急切换演练， 2每三年至少进行一次重要信息系统全 面灾备切换演练， 3根据不同的应急恢复内容，确定演练的周期，并指定专人管理和维护应急 预案，根据人员、信息资源等变动情况以及演练情况适时予以更新和完善，4 具备相关制度文档，具备应急切换演练记录。 部分符合情况：满足1/2/3/4中一种或两种。 不符合情况：1/2/3/4均不满足
备份与恢复管理	[关键]e)应每季度对备份数据的有效性进行检查，备份数据要实行异地保存。（F3）	每季度对备份数据的有效性进行检查，备份数据要实行异地保存。	1)访谈是否每季度对备份数据的有效性进行检查，备份数据是否实行异地保存。 2)核查相关制度文档。 3)核查是否具备有效性检查记录。	1每季度对备份数据的有效性进行检查， 2备份数据实行异地保存。 3具备相关制度文档，具备有效性检查记录。	符合情况：1每季度对备份数据的有效性进行检查， 2备份数据实行异地保存。 3具备相关制度文档，具备有效性检查记录。 部分符合情况：满足1/2/3中一种或两种。 不符合情况：1/2/3均不满足
备份与恢复管理	[关键]f)恢复及使用备份数据时需要提供相关口令密码的，应把口令密码密封后与数据备份介质一并 妥善保管。（F3）	恢复及使用备份数据时需要提供相关口令密码的，把口令密码密封后与数据备份介质一并 妥善保管。	1)访谈恢复及使用备份数据时是否需要提供相关口令密码，口令密码密封后是否与数据备份介质一并 妥善保管。 2)核查相关制度文档。 3)核查是否具备使用、保存记录。	1恢复及使用备份数据时需要提供相关口令密码 2把口令密码密封后与数据备份介质一并 妥善保管。3 具备相关制度文档，具备使用、保存记录。	符合情况：1恢复及使用备份数据时需要提供相关口令密码 2把口令密码密封后与数据备份介质一并 妥善保管。3 具备相关制度文档，具备使用、保存记录。 部分符合情况：满足1/2/3中一种或两种。 不符合情况：1/2/3均不满足
备份与恢复管理	[关键]g)灾难恢复的需求应定期进行再分析，再分析周期最长为三年，当生产中心环境、生产系统或 业务流程发生重大变更时，单位应立即启动灾难恢复需求再分析工作，依据需求分析制定灾 难恢复策略。（F3）	灾难恢复的需求定期进行再分析，再分析周期最长为三年，当生产中心环境、生产系统或 业务流程发生重大变更时，单位应立即启动灾难恢复需求再分析工作，依据需求分析制定灾 难恢复策略。	1)访谈是否定期进行灾难恢复再分析，当生产中心环境、生产系统或业务流程发生重大变更时，单位是否立即启动灾难恢复需求再分析工作，依据需求分析制定灾 难恢复策略。 2)核查相关制度文档。 3)核查是否具备再分析记录。	1灾难恢复的需求定期进行再分析，再分析周期最长为三年， 2当生产中心环境、生产系统或 业务流程发生重大变更时，单位立即启动灾难恢复需求再分析工作，依据需求分析制定灾 难恢复策略。3 具备相关制度文档，具备再分析记录。	符合情况：1灾难恢复的需求定期进行再分析，再分析周期最长为三年， 2当生产中心环境、生产系统或 业务流程发生重大变更时，单位立即启动灾难恢复需求再分析工作，依据需求分析制定灾 难恢复策略。3 具备相关制度文档，具备再分析记录。 部分符合情况：满足1/2/3中一种或两种。 不符合情况：1/2/3均不满足
备份与恢复管理	[关键]h)应建立健全灾难恢复计划，恢复计划至少要包括灾难恢复范围和目标、灾难切换规程、灾后 重续运行操作指引、各系统灾难切换操作手册。（F3）	建立健全灾难恢复计划，恢复计划至少要包括灾难恢复范围和目标、灾难切换规程、灾后 重续运行操作指引、各系统灾难切换操作手册。	1)访谈是否建立健全灾难恢复计划， 2)核查相关制度文档。	1建立健全灾难恢复计划，2恢复计划至少要包括灾难恢复范围和目标、灾难切换规程、灾后 重续运行操作指引、各系统灾难切换操作手册。 3 具备相关制度文档	符合情况：1建立健全灾难恢复计划， 2恢复计划至少要包括灾难恢复范围和目标、灾难切换规程、灾后 重续运行操作指引、各系统灾难切换操作手册。 3 具备相关制度文档 部分符合情况：满足1/2/3中一种或两种。 不符合情况：1/2/3均不满足
备份与恢复管理	[关键]i)金融机构应根据信息系统的灾难恢复工作情况，确定审计频率，应每年至少组织一次内部灾 难恢复工作审计。（F3）	金融机构根据信息系统的灾难恢复工作情况，确定审计频率，应每年至少组织一次内部灾 难恢复工作审计。	1)访谈是否每年至少组织一次内部灾 难恢复工作审计。 2)核查相关制度文档。 3)核查是否具备审计记录。	1机构根据信息系统的灾难恢复工作情况，确定审计频率，每年至少组织一次内部灾 难恢复工作审计。 2具备相关制度文档,具备审计记录。	符合情况：1机构根据信息系统的灾难恢复工作情况，确定审计频率，每年至少组织一次内部灾 难恢复工作审计。 2具备相关制度文档,具备审计记录。 部分符合情况：满足1/2中一种。 不符合情况：1/2均不满足

备份与恢复管理	[关键]j)应定期开展灾难恢复培训，并根据实际情况进行灾难恢复演练。（F3）	定期开展灾难恢复培训，并根据实际情况进行灾难恢复演练。	1)访谈是否定期开展灾难恢复培训，是否根据实际情况进行灾难恢复演练。 2)核查相关制度文档。 3)核查是否具备培训、演练记录。	1定期开展灾难恢复培训 2根据实际情况进行灾难恢复演练。3具备相关制度文档，具备培训、演练记录。	符合情况：1定期开展灾难恢复培训 2根据实际情况进行灾难恢复演练。3具备相关制度文档,具备培训、演练记录。 部分符合情况：满足1/2/3中一种或两种。 不符合情况：1/2/3均不满足
备份与恢复管理	[关键]k)应建立灾难备份系统，主备系统实际切换时间应少于RTO时间，灾备系统处理能力应不低于主 用系统处理能力的50%，通信线路应分别接入主备系统，有条件时可采用主、备系统处理能力 相同、轮换交替使用的双系统模式。（F3）	建立灾难备份系统，主备系统实际切换时间应少于RTO时间，灾备系统处理能力应不低于主 用系统处理能力的50%，通信线路应分别接入主备系统，有条件时可采用主、备系统处理能力 相同、轮换交替使用的双系统模式。	1)访谈是否建立灾难备份系统，访谈主备系统实际切换时间、处理能力 2)核查相关制度文档。 3)核查是否具备切换记录、处理记录。	1建立灾难备份系统 2主备系统实际切换时间应少于RTO时间，灾备系统处理能力应不低于主 用系统处理能力的50%，3具备相关制度文档，具备切换记录、处理记录。	符合情况：1建立灾难备份系统 2主备系统实际切换时间应少于RTO时间，灾备系统处理能力应不低于主 用系统处理能力的50%，3具备相关制度文档，具备切换记录、处理记录。 部分符合情况：满足1/2/3中一种或两种。 不符合情况：1/2/3均不满足
安全事件处置	[一般]a)应及时向安全管理部门报告所发现的安全弱点和可疑事件。	如发现系统有潜在的弱点和可疑事件，应及时向安全主管部门汇报，并提交相应的报告或信息	1)核查运维管理制度中对于发现安全弱点和可疑事件后的汇报要求 2)核查以往发现过的安全弱点和可疑事件对应书面报告或记录	1)在网络安全事件管理相关规定中明确告知用户在发现安全弱点和可疑事及时向安全管理部门报告 2)具有XXX安全弱点和可疑事件对应的报告或记录文档	符合情况（全部满足）： 1）在网络安全事件管理相关规定中明确告知用户在发现安全弱点和可疑事及时向安全管理部门报告 部分符合情况： 1）无 不符合情况： 1）未见任何制度中有相关意识的描述。 不适用情况： 1）无
安全事件处置	[重要]b)应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，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等。	安全事件的分类分级标准可参考GB/T20986-2007《信息安全技术信息安全事件分类分级指南》	核查运维管理制度，其中明确了不同安全事件的报告，处置和响应流程,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等内容	1)在安全事件报告和处置管理制度明确了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 2)具有XXX安全事件报告的模板文件	符合情况（全部满足）： 1）在安全事件报告和处置管理制度明确了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 2）有安全事件记录文件 部分符合情况： 1）制度内容不全面 不符合情况： 1）未建立相关全事件报告和处置管理制度 不适用情况：

安全事件处置	[重要]c)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。	对安全事件报告和响应处理的过程应进行详细的记录，并对事件发生的原因进行分析和总结	1)核查以往的安全事件报告和响应处置记录或相关模板 2)文档的内容是否包括了引发安全事件的系统弱点，不同的安全事件发生的原因、处置过程、经验教训总结、补救措施等	1)未发生过网络安全事件，则具有XXX安全事件报告的模板文件。 2)发生过安全事件的，具有XXX安全事件报告和响应处置记录文件，文件内容符合XXX安全事件报告模板的相关要求，如安全事件发生的原因、处置过程、经验教训总结、补救措施等	符合情况（全部满足）： 1)未发生过网络安全事件，则具有XXX安全事件报告的模板文件。 2)发生过安全事件的，具有XXX安全事件报告和响应处置记录文件，文件内容符合XXX安全事件报告模板的相关要求，如安全事件发生的原因、处置过程、经验教训总结、补救措施等 部分符合情况： 1）发生过安全事件，但是未按模板进行安全事件记录 不符合情况： 1）未核查到安全事件报告的模板文件。 不适用情况： 1）无
安全事件处置	[重要]d)对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。	对不同的安全事件应制定不同的处理程序和报告程序	核查安全事件报告和处理程序文档，是否针对重大安全事件制定了不同的处理和报告程序，是否明确了具体报告方式、报告内容、报告人等	1)针对不同安全事件形成不同的报告流程	符合情况（全部满足）： 1）针对不同安全事件形成不同的报告流程 部分符合情况： 1）无 不符合情况： 1）未针对不同安全事件形成不同的报告流程 不适用情况： 1）无
应急预案管理	[关键]a)应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容，业务处理系统应急预案的编制工作应由相关业务部门和科技部门共同完成，并由预案涉及的相关机构签字确认。（F3）	应急预案框架一般为单位总体应急预案管理的顶层文件，明确应急组织构成员职责、应急预案启动条件、响应、后期处置、预案日常管理、资源保障等内容，与各类网络安全事件专项应急预案共同构成整个应急预案体系	核查应急预案框架，内容是否包括了启动应急预案的条件、应急组织构成、应急资源保障、事后教育和培训等	1)具有应急预案框架 2)应急预案框的框架覆盖了启动应急预案的条件、应急组织构成、应急资源保障、事后教育和培训等方面的内容	符合情况（全部满足）： 1)具有应急预案框架 2)应急预案框的框架覆盖了启动应急预案的条件、应急组织构成、应急资源保障、事后教育和培训等方面的内容 部分符合情况： 1）应急预案框架覆盖内容不全面 不符合情况： 1）未具有应急预案框架文件。 不适用情况：
应急预案管理	[重要]b)应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容。	对重要事件制定专定应急预案，并对处理流程、恢复流程进行定义	核查针对重要事件的应急预案，预案内容是否包括了应急处理流程、系统恢复流程等	1）具有重要事件的专项应急预案，如针对机房(供电、火灾、漏水等)、系统(病毒爆发、数据泄露等)、网络(断网、拥塞等)等各个层面 2）专项事件应急预案包含应急处理流程、恢复流程	符合情况（全部满足）： 1）具有重要事件的专项应急预案，如针对机房(供电、火灾、漏水等)、系统(病毒爆发、数据泄露等)、网络(断网、拥塞等)等各个层面 2）专项事件应急预案包含应急处理流程、恢复流程 部分符合情况： 1）专项应急预案与系统关联性不大，只有普遍的应急预案。 不符合情况： 1）未具有重要事件的专项应急预案 不适用情况：

应急预案管理	[关键]c)应每年对系统相关的人员进行应急预案培训，并进行应急预案的演练。（F3）	应急预案培训和演练是应急的重要环节。应定期组织相关人员予以培训和演练，以保障及时有效的处理应急事件	1)核查以往开展过应急预案培训所产生的记录,确认培训的频度,记录内容是否包括了培训对象、培训内容、培训结果等 2)核查以往开展过应急预案演练所产生的记录，确认演练的频度,记录内容是否包括了演练对象、演练内容、演练结果等	1)具有每年对相关人员进行应急预案培训和演练 2)具有应急预案演练所产生的记录，确认演练的频度,记录内容包括了演练对象、演练内容、演练结果等	符合情况（全部满足）： 1)具有每年对相关人员进行应急预案培训和演练 2)具有应急预案演练所产生的记录，确认演练的频度,记录内容包括了演练对象、演练内容、演练结果等 部分符合情况： 1）具有应急预案培训，但是未进行演练 不符合情况： 1）不对应急预案进行培训，且不进行演练 不适用情况： 1）无
应急预案管理	[关键]d)在与第三方合作的业务中，应建立并完善内部责任机制和与相关机构之间的协调机制，制定 完整的应急预案及应急协调预案，并定期参加联合演练。（F3）	在与第三方合作的业务中，建立并完善内部责任机制和与相关机构之间的协调机制，制定 完整的应急预案及应急协调预案，并定期参加联合演练。	1)访谈在与第三方合作的业务中，是否建立并完善内部责任机制和与相关机构之间的协调机制，是否制定 完整的应急预案及应急协调预案，并定期参加联合演练 2)核查相关制度文档。 3)核查是否具备演练记录。	1在与第三方合作的业务中，建立并完善内部责任机制和与相关机构之间的协调机制， 2制定 完整的应急预案及应急协调预案，并定期参加联合演练。 3具备相关制度文档,具备演练记录。	符合情况：1在与第三方合作的业务中，建立并完善内部责任机制和与相关机构之间的协调机制， 2制定 完整的应急预案及应急协调预案，并定期参加联合演练。 3具备相关制度文档,具备演练记录。 部分符合情况：满足1/2/3中一种或两种。 不符合情况：1/2/3均不满足
应急预案管理	[关键]e)突发事件应急处置领导小组应统一领导应急管理工作，指挥、决策重大应急处置事宜，并协 调应急资源，明确具体应急处置联络人，并将具体联系方式上报本行业网络安全监管部门。（F3）	突发事件应急处置领导小组统一领导应急管理工作，指挥、决策重大应急处置事宜，并协 调应急资源，明确具体应急处置联络人，并将具体联系方式上报本行业网络安全监管部门。	1)访谈是否由突发事件应急处置领导小组统一领导应急管理工作，是否明确具体应急处置联络人，是否将具体联系方式上报本行业网络安全监管部门。 2)核查相关制度文档。	1突发事件应急处置领导小组统一领导应急管理工作，指挥、决策重大应急处置事宜，并协 调应急资源，明确具体应急处置联络人，并将具体联系方式上报本行业网络安全监管部门。 2具备相关制度文档,具备上报记录	符合情况：1突发事件应急处置领导小组统一领导应急管理工作，指挥、决策重大应急处置事宜，并协 调应急资源，明确具体应急处置联络人，并将具体联系方式上报本行业网络安全监管部门。 2具备相关制度文档,具备上报记录。 部分符合情况：满足1/2中一种。 不符合情况：1/2均不满足
应急预案管理	[关键]f)突发事件应急处置领导小组应严格按照行业、机构的相关规定和要求对外发布信息，机构内 其他部门或者个人不得随意接受新闻媒体采访或对外发表个人看法。（F3）	突发事件应急处置领导小组严格按照行业、机构的相关规定和要求对外发布信息，机构内 其他部门或者个人不得随意接受新闻媒体采访或对外发表个人看法。	1)访谈突发事件应急处置领导小组是否严格按照行业、机构的相关规定和要求对外发布信息， 2)核查相关制度文档。 3)核查是否具备发布记录。	1突发事件应急处置领导小组严格按照行业、机构的相关规定和要求对外发布信息， 2机构内 其他部门或者个人不得随意接受新闻媒体采访或对外发表个人看法。 3具备相关制度文档,具备发布记录。	符合情况：1突发事件应急处置领导小组严格按照行业、机构的相关规定和要求对外发布信息， 2机构内 其他部门或者个人不得随意接受新闻媒体采访或对外发表个人看法。 3具备相关制度文档,具备发布记录。 部分符合情况：满足1/2/3中一种或两种。 不符合情况：1/2/3均不满足
应急预案管理	[关键]g)实施报告制度和启动应急预案的单位应实行重大突发事件24小时值班制度。（F3）	实施报告制度和启动应急预案的单位应实行重大突发事件24小时值班制度。	1)访谈是否实施报告制度和启动应急预案的单位应实行重大突发事件24小时值班制度。 2)核查相关制度文档。	1实施报告制度和启动应急预案的单位实行重大突发事件24小时值班制度。 2具备相关制度文档。	符合情况：1实施报告制度和启动应急预案的单位实行重大突发事件24小时值班制度。 2具备相关制度文档。 部分符合情况：满足1/2中一种。 不符合情况：1/2均不满足
应急预案管理	[一般]h)应定期对原有的应急预案重新评估，修订完善。（F2）	根据每次应急演练的情况，对应急预案进行重新评估和修订	核查应急预案修订记录,记录内容是否包括了修订时间、参与人、修订内容、评审情况等	1根据每次应急演练的情况，对应急预案进行重新评估和修订 2具备相关制度文档、具有评估修订记录	符合情况：1根据每次应急演练的情况，对应急预案进行重新评估和修订 2具备相关制度文档、具有评估修订记录 部分符合情况：满足1/2中一种。 不符合情况：1/2均不满足

应急预案管理	[关键]i)应急演练结束后，应撰写应急演练情况总结报告，总结报告包括但不限于：内容和目的、总体方案、参与人员、准备工作、主要过程和关键时间点记录、存在的问题、后续改进措施及实施计划、演练结论。（F3）	应急演练结束后，撰写应急演练情况总结报告，总结报告包括但不限于：内容和目的、总体方案、参与人员、准备工作、主要过程和关键时间点记录、存在的问题、后续改进措施及实施计划、演练结论。	1)访谈应急演练结束后，是否撰写应急演练情况总结报告。 2)核查相关制度文档。 3)核查是否具备总结报告。	1应急演练结束后，撰写应急演练情况总结报告， 2总结报告包括但不限于：内容和目的、总体方案、参与人员、准备工作、主要过程和关键时间点记录、存在的问题、后续改进措施及实施计划、演练结论。 3具备相关制度文档、具备总结报告	符合情况：1突发事件应急处置领导小组严格按照行业、机构的相关规定和要求对外发布信息， 2机构内 其他部门或者个人不得随意接受新闻媒体采访或对外发表个人看法。 3具备相关制度文档,具备发布记录。 部分符合情况：满足1/2/3中一种或两种。 不符合情况：1/2/3均不满足
外包运维管理	[关键]a)应确保外包运维服务商的选择符合国家的有关规定。	外包服务商应满足国家相关主管部门的相关规定和要求,以证明其具有相应的服务能力	1)访谈运维负责人是否有外包运维服务情况 2)如果采用外包运维服务，核查外包运维服务商是否符合国家的有关规定	1)无外包运维，则本条不适用 2)有外包运维，主要外包内容是什么，外包服务单位名称以及所承担服务的资质证明	符合情况（全部满足）： 1）进行外包运维，外包运维单位，主要外包内容是什么，外包服务单位名称以及所承担服务的资质证明 部分符合情况： 1）无 不符合情况： 1）外包运维单位没有相应资质 不适用情况： 1）无外包运维情况
外包运维管理	[一般]b)应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。	针对外包运维服务商提供那些服务内容，应在相关协议中予以明确	1)核查外包运维服务协议 2)协议是否包括了外包运维的范围和工作内容	1)具有外包运维服务协议 2)协议包括了外包运维的范围和工作内容	符合情况（全部满足）： 1）具有外包合同，外包协议，且具有相关工作范围 部分符合情况： 1）无 不符合情况 1）未能查件任何外包合同，外包协议。： 不适用情况： 1）无外包运维情况
外包运维管理	[重要]c)应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确。	外包服务运维服务商应具有按照等级保护要求的开展安全运维工作的能力，意味着该外包运维服务商以往具有根据等级保护开展运维工作的实例，选择方在考虑选择哪个服务商时，应着重考虑相关运维人员具备等级保护相关运维的能力(如进行过等级保护相关方面的培训)	核查外包运维服务协议是否包含了其具有按照等级保护要求的开展安全运维工作的能力要求	外包运维服务协议内容包括了服务商具有按照等级保护要求的开展安全运维工作的能力要求	符合情况（全部满足）： 1）外包运维服务协议内容包括了服务商具有按照等级保护要求的开展安全运维工作的能力要求 部分符合情况： 1）无 不符合情况： 1）外包运维服务协议内容不明确 不适用情况： 1）无外包运维情况

外包运维管理	[一般]d)应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对IT基础设施中断服务的应急保障要求等。	在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对IT基础设施中断服务的应急保障要求等。	1)访谈是否在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对IT基础设施中断服务的应急保障要求等。 2)核查相关制度文档。	外包运维服务协议内容包括了可能涉及对敏感信息的访问、处理、存储要求，IT基础设施中断服务的应急保障要求等	符合情况（全部满足）： 1）外包运维服务协议内容包括了可能涉及对敏感信息的访问、处理、存储要求，IT基础设施中断服务的应急保障要求等 部分符合情况： 1）外包运维服务协议内容只包含部分可能涉及对敏感信息的访问、处理、存储要求，对IT基础设施中断服务的应急保障要求等要求 不符合情况： 1）外包运维服务协议内容不包括可能涉及对敏感信息的访问、处理、存储要求，IT基础设施中断服务的应急保障要求等 不适用情况：
外包运维管理	[关键]e)应要求外包运维服务商保留操作痕迹、记录完整的日志，相关内容和保存期限应满足事件分析、安全取证、独立审计和监督检查需要。（F3）	要求外包运维服务商保留操作痕迹、记录完整的日志，相关内容和保存期限应满足事件分析、安全取证、独立审计和监督检查需要。	1)访谈是否要求外包运维服务商保留操作痕迹、记录完整的日志，相关内容和保存期限应满足事件分析、安全取证、独立审计和监督检查需要。 2)核查相关制度文档。 3)核查是否具备操作记录。	1 外包运维服务商保留操作痕迹、记录完整的日志，2相关内容和保存期限应满足事件分析、安全取证、独立审计和监督检查需要。 3具备相关制度文档，具备操作记录。	符合情况：1 外包运维服务商保留操作痕迹、记录完整的日志，2相关内容和保存期限应满足事件分析、安全取证、独立审计和监督检查需要。 3具备相关制度文档，具备操作记录。 部分符合情况：满足1/2/3中一种或两种。 不符合情况：1/2/3均不满足
外包运维管理	[关键]f)应制定数据中心外包服务应急计划，应对外包服务商破产、不可抗力或其他潜在问题导致服务中断或服务水平下降的情形，支持数据中心连续、可靠运行。（F3）	制定数据中心外包服务应急计划，应对外包服务商破产、不可抗力或其他潜在问题导致服务中断或服务水平下降的情形，支持数据中心连续、可靠运行。	1)访谈是否制定数据中心外包服务应急计划。 2)核查相关制度文档。	1制定数据中心外包服务应急计划 2具备相关制度文档。	符合情况：1制定数据中心外包服务应急计划 2具备相关制度文档。 部分符合情况：满足1/2中一种。 不符合情况：1/2均不满足