GD

中华人民共和国广播电影电视行业暂行技术文件

GD/J 044—2012

广播电视相关信息系统安全等级保护测评要求

Evaluation requirement for classified protection

Of broadcasting related information system

2012-11－07 发布　　2012-11-07 实施

国家广播电影电视总局科技司　　发布

目 次

前　言

本技术文件依据《中华人民共和国计算机信息系统安全保护条例》（国务院147号令）、《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）、GD/J037-2011 《广播电视相关信息系统安全等级保护定级指南》、GD/J038-2011 《广播电视相关信息系统安全等级保护基本要求》、《广播电视安全播出管理规定》（总局62号令）及实施细则等有关文件要求，制定本技术文件。

本技术文件是广播电视相关信息系统安全等级保护技术文件之一。

与本技术文件相关的系列文件包括：

GD/J 037-2011 广播电视相关信息系统安全等级保护定级指南

GD/J 038-2011 广播电视相关信息系统安全等级保护基本要求

在本标准文本中，黑体字的测评要求表示该要求出现在当前等级而在低于当前等级信息系统的测评要求中没有出现过。

本技术文件给出了等级测评结论中应包括的主要内容，未规定给出测评结论的具体方法和量化指标。

本技术文件按照GB/T 1.1-2009给出的规则起草。

本技术文件由国家广播电影电视总局科技司归口。

本技术文件起草单位：国家广播电影电视总局监管中心、北京数字认证股份有限公司。

本技术文件主要起草人：张瑞芝、姜峰、李炎、杨波、段垚、蒋晓敏、柴晓瑜、彭海龙、翟建军、罗桂民、白旭东、郝金鹏

广播电视相关信息系统安全等级保护测评要求

1 范围

本技术文件规定了对广播电视相关信息系统安全等级保护状况进行安全测试评估的要求，包括对第一级信息系统、第二级信息系统、第三级信息系统和第四级信息系统进行安全测试评估的单元测评要求和信息系统整体测评要求。

本技术文件指导测评单位人员从信息安全等级保护的角度对信息系统进行测试评估，指导广播电视相关信息系统运营使用单位对信息系统安全等级保护状况进行安全等级测试自评估，信息安全监管职能部门进行信息安全等级保护监督检查。

2 规范性引用文件

下列文件对于本技术文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本技术文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本技术文件。

GB/T 5271.8 信息技术 词汇 第8部分：安全

GB/T 25069 信息安全技术 术语

GB 50174 电子信息系统机房设计规范

GY 5067 广播电视建筑设计防火规范

GD/J 037-2011 广播电视相关信息系统安全等级保护定级指南

GD/J 038-2011 广播电视相关信息系统安全等级保护基本要求

3 术语和定义

GB/T 5271.8、GB/T 25069、GD/J 037-2011和GD/J 038-2011所界定的以及下列术语和定义适用于本标准。

3.1 测评力度

测评工作实际投入力量的表征，可以由测评广度和深度来描述。

4 总则

4.1 测评原则

a) 最小影响原则

测评工作应服从安全播出管理的相关要求，测评工作可管可控。测评机构应围绕广播电视安全播出科学化和规范化管理，结合广播电视信息系统特点，开展广播电视信息系统安全等级测评工作。测评机

构人员应熟悉广播电视信息系统特点和业务流程，规避因测评引入安全播出风险。测评实施过程所使用的测评工具、测评方式应不影响安全播出。

b) 客观性和公正性原则

测评人员应当在没有偏见和最小主观判断情形下，按照测评双方相互认可的测评方案，基于明确定义的测评方法和过程，实施测评活动。

c) 可重复性和可再现性原则

不同的测评人员，依照同样的要求，使用同样的方法，对同样的测评实施过程的重复执行都应该得到同样的测评结果。可重复性体现在同一测评者重复执行相同测评的结果的一致性。可再现性体现在不同测评者执行相同测评的结果的一致性。

d) 符合性原则

测评所产生的结果应当是在对测评指标的正确理解下所取得的良好的判断。测评实施过程应当使用正确的方法以确保其满足了测评指标的要求。

4.2 测评内容

信息系统安全等级测评主要包括单元测评和整体测评两部分。

单元测评是等级测评工作的基本活动，每个单元测评包括测评指标、测评实施和结果判定三个要素与环节。其中，测评指标来源于GD/J 038-2011中的各基本要求项，测评实施则是使用具体的测评方法，进行测评取证的活动，结果判定分为符合、部分符合、不符合三种类别。访谈不作为判定项，以检查、测试结果作为判定项。针对每一个单元测评，所有测评指标结果判定均为是，则该单元测评结果判定为符合；根据广播电视业务系统特点及安全播出要求，影响该安全控制点基本防护能力的测评指标一项或多项结果判定为否，则该单元测评结果判定为不符合；测评结果判定为符合、不符合之外的其它情况判定为部分符合。

整体测评是在单元测评的基础上，结合信息系统的实际情况和安全播出要求，进一步分析信息系统的整体安全性，对信息系统的综合安全测评。整体测评主要包括安全控制点间、层面间和区域间相互作用的安全测评以及系统结构的安全测评。

4.3 测评流程

等级测评过程分为四个基本测评活动：测评准备、方案编制、现场测评、分析及报告编制。测评双方之间的沟通与洽谈应贯穿整个测评过程。等级测评过程见图1。

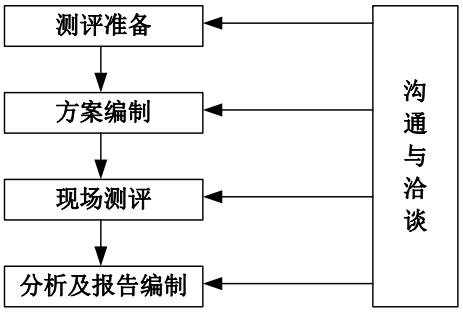

图1 等级测评过程

a) 测评准备活动是开展等级测评工作的前提和基础，是整个等级测评过程有效性的保证。测评准备活动是否充分直接关系到后续工作能否顺利展开。本活动的主要任务是掌握被测系统的详细情况，准备测评所需的相关材料（资料主要是信息方面的，材料可以包含工具类），为实施测评做好文档及测试工具等方面的准备。

测评准备活动的基本工作流程见图 2。

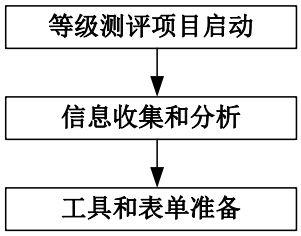

图2 测评准备活动的基本工作流程

b) 方案编制活动是开展等级测评工作的关键，为现场测评提供最基本的文档和指导方案。本活动的主要任务是整理测评准备活动中获取的信息系统相关资料，开发与被测信息系统相适应的测评内容、测评实施手册等，为现场测评活动提供最基本的文档和指导方案。

方案编制活动的基本工作流程见图 3。

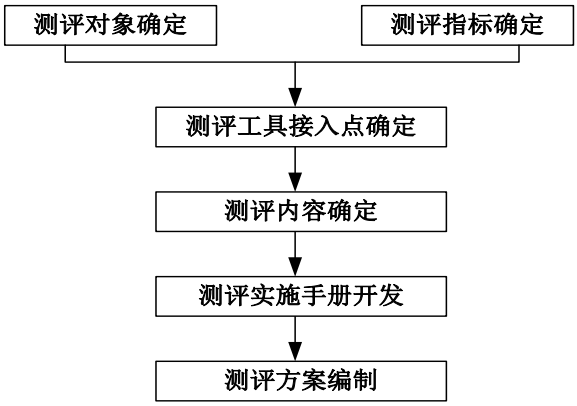

图3 方案编制活动的基本工作流程

c) 现场测评活动是开展等级测评工作的核心。本活动的主要任务是按照测评方案的总体要求，严格执行测评实施手册，分步实施所有测评指标，包括单元测评和系统整体测评两个方面，以了解系统的真实保护情况，取得分析与报告编制活动所需的、足够的证据和资料，发现系统可能存在的安全问题。

现场测评活动的基本工作流程见图 4。

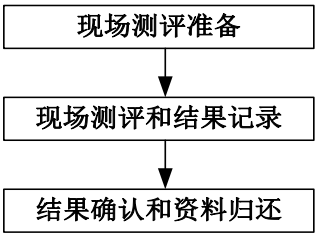

图4 现场测评活动的基本工作流程

d) 分析及报告编制活动是等级测评工作的结果，是总结被测系统整体安全保护能力的综合评价活动。本活动的主要任务是根据现场测评结果和本测评要求，通过单元测评结果判定和整体测评分析等方法，分析整个系统的安全保护现状与相应等级的保护要求之间可能存在的差距，综合评价被测信息系统保护状况，并形成等级测评结论，编制测评报告。

分析与报告编制活动的基本工作流程见图 5：

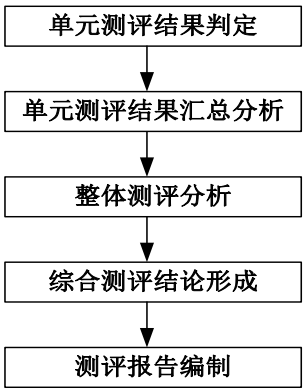

图5 分析与报告编制活动的基本工作流程

4.4 测评方法

测评方法主要包括访谈、检查和测试三种测评方法。其中，访谈是指测评人员通过引导信息系统相关人员进行有针对性的交流以帮助测评人员理解、分析和取得证据的过程，检查是指测评人员通过对测评对象（如管理制度、操作记录、安全配置等）进行观察、调阅、查验、分析以帮助测评人员理解、分析和取得证据的过程，测试是测评人员使用预定的方法/工具使测评对象产生特定的行为，通过查看和分析对象反馈以帮助测评人员获取证据的过程。需要使用测试测评方法时，应根据广播电视业务系统运行情况，在被测系统小范围内使用。

4.5 测评力度

测评力度反映测评的广度和深度，体现为测评工作的实际投入程度。测评广度越大，测评实施的范围越大，测评实施包含的测评对象就越多；测评深度越深，越需要在细节上展开，测评就越严格，因此就越需要更多的投入。测评的广度和深度落实到访谈、检查和测试三种不同的测评方法上，能体现出测评实施过程中访谈、检查和测试的投入程度的不同。

为了检验不同安全保护等级的信息系统是否具有相应等级的安全保护能力，是否满足相应等级的保护要求，需要实施与其安全保护等级相适应的测评，达到应有的测评力度。第一级到第四级信息系统的测评力度反映在访谈、检查和测试等三种基本测评方法的测评广度和深度上，落实在不同单元测评中具体的测评实施上。不同安全保护等级的信息系统在总体上所对应的测评力度在附录A中描述。

4.6 使用方法

根据技术文件GD/J 038-2011 信息系统技术安全层面测评分为基础网络安全、边界安全、终端系统安全、服务端系统安全、应用安全、数据安全与备份恢复六部分。基础网络安全的安全控制点包括结构安全、安全审计、网络设备防护等；边界安全的安全控制点包括访问控制、安全数据交换、入侵防范等；

终端系统安全的安全控制点包括身份鉴别、访问控制、安全审计等；服务端系统安全的安全控制点包括身份鉴别、访问控制、安全审计等；应用安全的安全控制点包括身份鉴别、访问控制、安全审计等；数据安全与备份恢复的安全控制点包括数据完整性、数据保密性、备份与恢复等。每个安全控制点的测评包括具体安全要求项（在本技术文件中被称为“测评指标”）。第三级和第四级信息系统的安全层面测评还包括安全管理中心。

根据技术文件GD/J 038-2011 通用物理安全控制点测评包括物理位置的选择、物理访问控制、防盗窃和防破坏、机房环境、机房消防设施、电力供应六部分，每个安全控制点的测评包括具体安全要求项。

根据技术文件GD/J 038-2011 通用管理安全层面测评分为总要求、安全管理机构、人员安全管理、系统建设管理、系统运维管理五个部分，每个安全层面的测评包括安全控制点测评，每个安全控制点测评包括具体安全要求项。

本技术文件中针对每一个安全控制点的测评就构成一个单元测评，单元测评中的每一个具体测评实施要求项（以下简称“测评指标”）是与安全控制点下面所包括的要求项（测评指标）相对应的。在对每一要求项进行测评时，可能用到访谈、检查和测试三种测评方法，也可能用到其中一种或两种，使用时，应当从单元测评的测评实施中抽取出对于GD/J 038-2011中每一个要求项的测评要求，并按照这些测评要求开发测评指导书，以规范和指导安全等级测评活动。

测评过程中，测评人员应注意对测评记录和证据的采集、处理、存储和销毁，保护其在测评期间免遭破坏、更改或遗失，并保守秘密。

等级测评的最终输出是测评报告，测评报告应结合第11章的要求给出等级测评结论。

5 第一级信息系统单元测评

5.1 基础网络安全

5.1.1 结构安全

5.1.1.1. 测评指标

见GD/J 038-2011 5.1.1。

5.1.1.2. 测评实施

本项要求包括：

a) 应访谈网络管理员，询问关键网络设备的业务处理能力和网络带宽是否满足业务需要；
b) 应检查网络拓扑图、网络设计或验收文档，是否有主要网络设备业务处理能力、接入网络及核心网络的带宽满足业务需要以及不存在带宽瓶颈等方面的设计或描述；
c) 应检查网络拓扑结构图与当前运行的实际网络结构是否一致。

5.1.1.3. 结果判定

a) 如果 5.1.1.2. b)、c)为肯定，则信息系统符合本单元测评指标要求。
b) 如果 5.1.1.2. b)、c)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

5.1.2 网络设备防护

5.1.2.1.测评指标

见GD/J 038-2011 5.1.2。

5.1.2.2.测评实施

本项要求包括：

a) 应访谈网络管理员，询问边界网络设备和关键网络设备的防护措施有哪些；采用何种方式验证用户身份；是否关闭了不必要的服务和端口；是否采取了安全远程管理手段；
b) 应检查边界网络设备和关键网络设备，查看是否配置了对登录用户进行身份鉴别的功能；
c) 应检查边界网络设备和关键网络设备，查看是否配置了鉴别失败处理功能；
d) 应检查边界网络设备和关键网络设备，查看是否关闭了不必要的服务和端口；
e) 应检查边界网络设备和关键网络设备，查看是否采用了 HTTPS、SSH 等安全远程管理手段。

5.1.2.3.结果判定

a) 如果 5.1.2.2. b)-e)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 5.1.2.2. b)-e)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

5.2 边界安全

5.2.1 访问控制

5.2.1.1.测评指标

见GD/J 038-2011 5.2.1。

5.2.1.2.测评实施

本项要求包括：

a) 应访谈安全管理员，询问采用了哪些网络访问控制设备；启用了哪些访问控制策略；询问外部网络用户安全接入方式有哪些；
b) 应检查访问控制设备，是否启用了基于网段级的允许/拒绝访问控制策略；
c) 应检查外部网络用户是否采取安全方式接入，是否基于用户组级对用户权限进行管理。

5.2.1.3.结果判定

a) 如果 5.2.1.2. b)、c)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 5.2.1.2. b)为肯定，c)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 5.2.1.2. b)为否定，则信息系统不符合本单元测评指标要求。

5.2.2 安全数据交换

5.2.2.1.测评指标

见GD/J 038-2011 5.2.2。

5.2.2.2.测评实施

本项要求包括：

a) 应访谈播出系统管理员，询问播出系统与其它信息系统之间交换的文件类型及格式；
b) 应访谈安全管理员，询问是否限定可以通过移动介质交换数据的主机；询问通过其它移动介质上载的内容是否经过两种或两种以上的防恶意代码产品进行恶意代码检查；询问蓝光、P2 等专业移动介质上载是否采用了特定防护机制；
c) 应检查是否采用限定的文件类型及格式与播出系统进行数据交换；
d) 应检查是否限定了可以通过移动介质交换数据的主机；
e) 应检查是否安装有两种或两种以上的防恶意代码产品进行恶意代码检查；
f) 应检查蓝光、P2 等专业移动介质上载是否采用了特定防护机制。

5.2.2.3.结果判定

a) 如果 5.2.2.2. c)-f）均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 5.2.2.2. c)-f）中一项或多项为否定，则信息系统不符合本单元测评指标要求。

5.3 终端系统安全

5.3.1 身份鉴别

5.3.1.1.测评指标

见GD/J 038-2011 5.3.1。

5.3.1.2.测评实施

本项要求包括：

a) 应访谈安全管理员，询问终端操作系统采用了何种身份标识和鉴别机制；
b) 应检查终端操作系统是否采取了身份标识和鉴别措施。

5.3.1.3.结果判定

a) 如果 5.3.1.2. b)为肯定，则信息系统符合本单元测评指标要求。
b) 如果 5.3.1.2. b)为否定，则信息系统不符合本单元测评指标要求。

5.3.2 访问控制

5.3.2.1.测评指标

见GD/J 038-2011 5.3.2。

5.3.2.2.测评实施

本项要求包括：

a) 应访谈安全管理员，是否制定了资源访问安全策略，是否禁止通过 USB 等外设进行数据交换；
b) 应检查终端的资源访问安全策略，查看是否关闭系统不必要的服务和端口，是否禁止通过 USB 等外设进行数据交换。

5.3.2.3.结果判定

a) 如果 5.3.2.2. b)为肯定，则信息系统符合本单元测评指标要求。
b) 如果 5.3.2.2. b)为否定，则信息系统不符合本单元测评指标要求。

5.3.3 恶意代码防范

5.3.3.1.测评指标

见GD/J 038-2011 5.3.3。

5.3.3.2.测评实施

本项要求包括：

a) 应访谈安全管理员，询问终端是否部署了防恶意代码软件；
b) 应检查终端是否安装了防恶意代码软件；
c) 应检查终端是否及时更新恶意代码库和防恶意代码软件版本。

5.3.3.3.结果判定

a) 如果 5.3.3.2. b)、c）为肯定，则信息系统符合本单元测评指标要求。
b) 如果 5.3.3.2. b)、c)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

5.4 服务端系统安全

5.4.1 身份鉴别

5.4.1.1.测评指标

见GD/J 038-2011 5.4.1。

5.4.1.2.测评实施

本项要求包括：

a) 应访谈系统管理员和数据库管理员,询问操作系统和数据库系统中的用户是否采取了身份标识和鉴别措施，口令是否定期更换；
b) 应检查关键服务器操作系统和数据库系统，是否采取了身份标识和鉴别措施；身份鉴别信息是否具有不易被冒用的特点；
c) 检查关键服务器用户登录失败处理功能，是否采取结束会话、自动退出、限制非法登录次数等措施。

5.4.1.3.结果判定

a) 如果 5.4.1.2. b)、c)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 5.4.1.2. b)、c)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

5.4.2 访问控制

5.4.2.1.测评指标

见GD/J 038-2011 5.4.2。

5.4.2.2.测评实施

本项要求包括：

a) 应访谈安全管理员，是否制定了服务器操作系统和数据库系统的访问控制策略；是否控制用户对资源的访问，限定外设数据交换方式，关闭不必要的服务和端口等；
b) 应检查关键服务器操作系统和数据库系统的安全策略配置，查看是否对资源的访问进行了限制，关闭不必要的服务和端口；
c) 应检查关键服务器操作系统和数据库系统中相应的用户配置，查看是否限制默认帐户的访问权限、重命名系统默认帐户，并修改默认口令；
d) 应检查关键服务器操作系统和数据库系统的帐户设置情况，查看是否删除多余的、过期的帐户，避免存在共享帐户。

5.4.2.3.结果判定

a) 如果 5.4.2.2. b)-d)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 5.4.2.2. b)-d)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

5.4.3 恶意代码防范

5.4.3.1.测评指标

见GD/J 038-2011 5.4.3。

5.4.3.2.测评实施

本项要求包括：

a) 应访谈安全管理员，依据何种原则在哪些服务器上部署了防恶意代码软件；
b) 应检查服务器是否安装了防恶意代码软件；
c) 应检查服务器的恶意代码库和防恶意代码软件版本是否及时更新。

5.4.3.3.结果判定

a) 如果 5.4.3.2. b)、c）为肯定，则信息系统符合本单元测评指标要求。
b) 如果 5.4.3.2. b)、c)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

5.4.4 入侵防范

5.4.4.1.测评指标

见 GD/J 038-2011 5.4.4。

5.4.4.2.测评实施

本项要求包括：

a) 应访谈安全管理员，是否制定了服务器操作系统安装规范和流程，是否遵循最小安装原则，依据何种原则在哪些服务器上进行了补丁更新；
b) 应检查操作系统是否遵循最小安装原则，仅安装需要的组件和应用程序；
c) 应检查操作系统是否及时更新系统补丁。

5.4.4.3.结果判定

a) 如果5.4.4.2. b)、c）为肯定，则信息系统符合本单元测评指标要求。
b) 如果5.4.4.2. b)、c)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

5.5 应用安全

5.5.1 身份鉴别

5.5.1.1.测评指标

见GD/J 038-2011 5.5.1。

5.5.1.2.测评实施

本项要求包括：

a) 应访谈应用系统管理员和安全管理员，是否采取了身份鉴别措施和用户管理策略；
b) 应检查应用系统是否采取了身份鉴别措施，身份鉴别信息是否具有不易被冒用的特点；
c) 应检查应用系统用户登录失败处理功能，是否采取结束会话、自动退出、限制非法登录次数等措施。

5.5.1.3.结果判定

a) 如果5.5.1.2. b)、c)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果5.5.1.2. b)、c)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

5.5.2 访问控制

5.5.2.1.测评指标

见GD/J 038-2011 5.5.2。

5.5.2.2.测评实施

本项要求包括：

a) 应访谈安全管理员，是否采取了访问控制措施，启用了哪些访问控制策略；
b) 应检查应用系统是否采用了基于用户级的资源访问控制策略，
c) 应检查应用系统帐户设置情况，查看是否删除临时账户、测试帐户，禁止匿名用户登录，修改默认账户及口令，限制其访问权限。

5.5.2.3.结果判定

a) 如果5.5.2.2. b)、c)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果5.5.2.2. b)、c)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

5.5.3 软件容错

5.5.3.1.测评指标

见GD/J 038-2011 5.5.3。

5.5.3.2.测评实施

本项要求包括：

a) 应访谈应用系统管理员，询问应用系统是否具有软件容错能力的措施，具体措施有哪些；
b) 应检查应用系统，查看应用系统是否具有对人机接口输入或通信接口输入的数据进行有效性检验的功能；
c) 应测试主要应用系统，可通过对人机接口输入的不同长度或格式的数据，查看系统的反应，验证系统人机接口有效性检验功能是否正确。

5.5.3.3.结果判定

a) 如果 5.5.3.2. b)、c)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 5.5.3.2. b)为肯定，c)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 5.5.3.2. b)为否定，则信息系统不符合本单元测评指标要求。

5.6 数据安全及备份恢复

5.6.1 数据完整性

5.6.1.1.测评指标

见 GD/J 038-2011 5.6.1。

5.6.1.2.测评实施

本项要求包括：

a) 应访谈安全管理员，询问用户身份鉴别信息、调度信息、播出节目等重要业务数据在传输过程中是否具有完整性保证措施，具体措施有哪些；
b) 应检查应用系统，查看其是否能够检测到用户身份鉴别信息、调度信息、播出节目等重要业务数据在传输过程中完整性受到破坏。

5.6.1.3.结果判定

a) 如果 5.6.1.2. b)为肯定，则信息系统符合本单元测评指标要求。
b) 如果 5.6.1.2. b)为否定，则信息系统不符合本单元测评指标要求。

5.6.2 数据保密性

5.6.2.1.测评指标

见 GD/J 038-2011 5.6.2。

5.6.2.2.测评实施

本项要求包括：

a) 应分别访谈网络管理员、系统管理员、数据库管理员和安全管理员，询问是否对用户身份鉴别信息采取存储保密措施；

b) 应检查关键服务器操作系统、关键网络设备操作系统、关键数据库管理系统和关键应用系统，查看用户身份鉴别信息是否采取了存储保密措施。

5.6.2.3.结果判定

a) 如果 5.6.2.2. b)为肯定，则信息系统符合本单元测评指标要求。
b) 如果 5.6.2.2. b)为否定，则信息系统不符合本单元测评指标要求。

5.6.3 备份和恢复

5.6.3.1.测评指标

见 GD/J 038-2011 5.6.3。

5.6.3.2 测评实施

本项要求包括：

a) 应分别访谈应用系统管理员和安全管理员，询问是否对重要业务信息、关键数据进行备份，备份和恢复策略是什么；
b) 应检查应用系统，查看是否具备备份与恢复重要业务信息和关键数据的功能，并查看实际备份结果是否与备份策略一致。

5.6.3.3.结果判定

a) 如果 5.6.3.2. b)为肯定，则信息系统符合本单元测评指标要求。
b) 如果 5.6.3.2. b)为否定，则信息系统不符合本单元测评指标要求。

6 第二级信息系统单元测评

6.1 基础网络安全

6.1.1 结构安全

6.1.1.1.测评指标

见 GD/J 038-2011 6.1.1。

6.1.1.2.测评实施

本项要求包括：

a) 应访谈网络管理员，询问关键网络设备的性能以及目前业务高峰流量情况，**网络中带宽控制情况以及带宽分配的原则；询问新闻制播系统、播出整备系统、播出系统等播出直接相关系统的核心交换机、汇聚交换机等关键网络设备是否配置冗余；询问新闻制播系统中的直播演播室系统、播出整备系统、播出系统等播出直接相关系统是否位于纵深结构内部，询问系统内部是否没有通过无线方式组网；询问网络安全域划分情况、网段划分情况以及划分的原则，询问重要网段有哪些，其具体的部署位置，与其他网段的隔离措施有哪些；**
b) 应检查网络设计或验收文档，是否有主要网络设备业务处理能力、接入网络及核心网络的带宽满足业务高峰期的需要以及不存在带宽瓶颈等方面的设计或描述；

c) **应检查新闻制播系统、播出整备系统、播出系统等播出直接相关系统的核心交换机、汇聚交换机等关键网络设备是否配置冗余；**
d) **应检查网络拓扑图、网络设计或验收文档，是否根据各信息系统与播出的相关程度进行层次化结构设计，形成网络纵深防护体系，新闻制播系统中的直播演播室系统、播出整备系统、播出系统等播出直接相关系统是否位于纵深结构内部，查看系统内部是否没有通过无线方式进行组网；**
e) 应检查网络拓扑结构图与当前运行的实际网络结构是否一致；
f) **应检查网络设计或验收文档，是否根据信息系统功能、业务流程、网络结构层次、业务服务对象等合理划分网络安全域，安全域内是否根据业务类型、业务重要性、物理位置等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段；**
g) **应检查边界网络设备和关键网络设备，重要网段是否采取了技术隔离手段与与其它网段隔离。**

6.1.1.3.结果判定

a) 如果 6.1.1.2. b)-g)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 6.1.1.2. b)-g)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

6.1.2 安全审计

6.1.2.1.测评指标

见 GD/J 038-2011 6.1.2。

6.1.2.2.测评实施

本项要求包括：

a) **应访谈安全审计员，询问关键网络设备是否开启审计功能，审计内容包括哪些项；询问审计记录的主要内容有哪些，对审计记录的处理方式有哪些；**
b) **应检查关键网络设备或安全审计设备，查看审计策略是否包括网络设备运行状况、用户行为等；**
c) **应检查关键网络设备或安全审计设备，查看事件审计记录是否包括：事件的日期和时间、用户名、IP 地址、事件类型、事件成功情况及其他与审计相关的信息；**
d) **应检查关键网络设备或安全审计设备的审计记录，是否至少保存 90 天；**
e) **应检查对事件审计记录进行分析的记录，查看是否定期对审计记录进行分析；**
f) **应测试关键网络设备或安全审计设备，可通过以某个用户登录系统，试图删除、修改或覆盖审计记录，验证安全审计的保护情况与要求是否一致。**

6.1.2.3.结果判定

a) 如果 7.1.2.2. b)-g)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.1.2.2. b)-d)均为肯定，e)、g)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 7.1.2.2. b)-d)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

6.1.3 网络设备防护

6.1.3.1.测评指标

见 GD/J 038-2011 6.1.3。

6.1.3.2. 测评实施

本项要求包括：

a) 应访谈网络管理员，询问网络设备的防护措施有哪些，采用何种方式验证用户身份，询问网络设备关闭了哪些不必要的服务和端口，远程管理设备时采取何种安全管理手段；
b) 应检查边界网络设备和关键网络设备，查看是否启用了对登录用户进行身份鉴别的功能，**口令是否有复杂度要求并定期更换，用户名和口令禁止相同**；
c) 应检查边界网络设备和关键网络设备，查看是否配置了结束会话、限制非法登录次数、远程超时自动退出等鉴别失败处理功能；
d) 应检查边界网络设备和关键网络设备，查看是否关闭了不必要的服务和端口；
e) **应检查边界网络设备和关键网络设备，查看是否对网络设备的管理员登录地址进行限制，仅允许指定 IP 地址或 IP 段访问；**
f) 应检查边界网络设备和关键网络设备，查看网络设备是否采用 HTTPS、SSH 等安全的远程管理手段。

6.1.3.3. 结果判定

a) 如果 6.1.3.2. b)-f)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 6.1.3.2. b)-f)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

6.2 边界安全

6.2.1 访问控制

6.2.1.1. 测评指标

见 GD/J 038-2011 6.2.1。

6.2.1.2. 测评实施

本项要求包括：

a) 应访谈安全管理员，询问采取了哪些网络访问控制措施；启用了哪些网络访问控制策略；询问外部用户安全接入方式有哪些；
b) 应检查访问控制设备，是否启用了基于网段级的允许/拒绝访问控制策略；
c) 应检查外部网络用户是否采取安全接入方式，是否对用户权限进行管理，**控制粒度是否为用户级；**
d) **应针对网络访问控制措施进行渗透测试，可通过采用多种渗透测试技术，验证网络访问控制措施是否不存在明显的弱点。**

6.2.1.3. 结果判定

a) 如果 6.2.1.2. b)-d)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 6.2.1.2. b)为肯定，c)、d)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 6.2.1.2. b)为否定，则信息系统不符合本单元测评指标要求。

6.2.2 安全数据交换

6.2.2.1.测评指标

见 GD/J 038-2011 6.2.2。

6.2.2.2.测评实施

本项要求包括：

a) 应访谈播出系统管理员，询问播出系统与其它信息系统之间交换的文件类型及格式；
b) 应访谈安全管理员，询问是否限定可以通过移动介质交换数据的主机；询问通过其它移动介质上载的内容是否经过两种以上的防恶意代码产品进行恶意代码检查；询问蓝光、P2 等专业移动介质上载是否采用了特定防护机制；
c) 应检查是否采用限定的文件类型及格式与播出系统进行数据交换；
d) 应检查是否限定了可以通过移动介质交换数据的主机，是否安装有两种以上的防恶意代码产品进行恶意代码检查，蓝光、P2 等专业移动介质上载是否采用了特定防护机制。
e) **应检查信息系统与外部网络进行数据交换时，是否通过数据交换区或专用数据交换设备等完成内外网数据的安全交换；**
f) **应检查数据交换区对外是否通过访问控制设备与外部网络进行安全隔离，对内是否采用安全的方式进行数据交换。**

6.2.2.3.结果判定

a) 如果 6.2.2.2. c)-f)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 6.2.2.2. c)-f)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

6.2.3 入侵防范

6.2.3.1.测评指标

见 GD/J 038-2011 6.2.3。

6.2.3.2.测评实施

本项要求包括：

a) **应访谈安全管理员，询问与外部网络连接的网络边界处入侵防范措施有哪些，是否有专门设备对网络入侵进行防范；询问网络入侵防范规则库的升级方式；**
b) **应检查网络入侵防范设备，查看是否能检测以下攻击行为：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、网络蠕虫攻击等；**
c) **应检查网络入侵防范设备，查看其规则库是否及时更新；**
d) **应测试网络入侵防范设备，验证其检测策略是否有效。**

6.2.3.3.结果判定

a) 如果 6.2.3.2. b)-d)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 6.2.3.2. b)-d)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

6.2.4 恶意代码防范

6.2.4.1.测评指标

见 GD/J 038-2011 6.2.4。

6.2.4.2.测评实施

本项要求包括：

a) **应访谈安全管理员，询问网络边界处恶意代码防范措施有哪些，恶意代码库的更新策略；**
b) **应检查在信息系统网络边界处是否有相应的防恶意代码措施；**
c) **应检查信息系统网络边界处的防恶意代码产品与信息系统内部防恶意代码产品是否具有不同的恶意代码库；**
d) **应检查防恶意代码产品，查看其运行是否正常，恶意代码库是否及时更新。**

6.2.4.3.结果判定

a) 如果 6.2.4.2. b)-d)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 6.2.4.2. b)-d)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

6.2.5 安全审计

6.2.5.1.测评指标

见 GD/J 038-2011 6.2.5。

6.2.5.2.测评实施

本项要求包括：

a) **应访谈安全审计员，询问与外部网络连接的边界处安全审计措施有哪些；审计内容包括哪些项；询问审计记录的主要内容有哪些，对审计记录的处理方式有哪些；**
b) **应检查与外部网络连接的边界处安全审计设备，是否对数据通信行为进行审计；**
c) **应检查与外部网络连接的边界处安全审计设备，查看事件审计记录是否包括：事件的日期和时间、用户名、IP 地址、事件类型、事件成功情况及其他与审计相关的信息，**
d) **应检查与外部网络连接的边界处安全审计设备，查看审计记录是否至少保存 90 天；**
e) **应检查对事件审计记录进行分析的记录，查看是否定期对审计记录进行分析；**
f) **应测试与外部网络连接的边界处安全审计设备，可通过以某个用户登录系统，试图删除、修改或覆盖审计记录，验证安全审计的保护情况与要求是否一致。**

6.2.5.3.结果判定

a) 如果 6.2.5.2. b)-f)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 6.2.5.2. b)-d)均为肯定，e)、f)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 6.2.5.2. b)-d)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

6.2.6 边界完整性

6.2.6.1.测评指标

见 GD/J 038-2011 6.2.6。

6.2.6.2.测评实施

本项要求包括：

a) **应访谈安全管理员，询问内部网络用户联到外部网络的行为有哪些；**
b) **应检查边界完整性检查设备，是否能够对内部网络用户私自联到外部网络的行为检查；**
c) **应测试边界完整性检查设备，测试是否能够对私自联到外部网络的内部网络用户进行检查。**

6.2.6.3.结果判定

a) 如果 6.2.6.2. b)、c)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 6.2.6.2. b)、c)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

6.3 终端系统安全

6.3.1 身份鉴别

6.3.1.1.测评指标

见 GD/J 038-2011 6.3.1。

6.3.1.2.测评实施

本项要求包括：

a) 应访谈安全管理员，询问终端操作系统采用了何种身份标识和鉴别机制；
b) 应检查终端操作系统，是否提供了身份标识和鉴别措施；
c) **应检查终端操作系统是否设置口令复杂度要求，口令是否定期进行更换，用户名和口令是否禁止相同。**

6.3.1.3.结果判定

a) 如果 6.3.1.2. b)、c)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 6.3.1.2. b)、c)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

6.3.2 访问控制

6.3.2.1.测评指标

见 GD/J 038-2011 6.3.2。

6.3.2.2.测评实施

本项要求包括：

a) 应访谈安全管理员，制定的资源访问安全策略有哪些；
b) 应检查终端的资源访问安全策略，查看是否禁止通过 USB 等外设进行数据交换，是否关闭系统不必要的服务和端口等。

6.3.2.3.结果判定

a) 如果 6.3.2.2. b)为肯定，则信息系统符合本单元测评指标要求。
b) 如果 6.3.2.2. b)为否定，则信息系统不符合本单元测评指标要求。

6.3.3 入侵防范

6.3.3.1.测评指标

见 GD/J 038-2011 6.3.3。

6.3.3.2.测评实施

本项要求包括：

a) **应访谈安全管理员，终端操作系统的入侵防范措施有哪些；采取何种方式更新补丁；**
b) **应检查终端操作系统是否遵循最小安装原则，仅安装需要的组件和应用程序，是否及时更新系统补丁。**

6.3.3.3.结果判定

a) 如果 6.3.3.2. b)为肯定，则信息系统符合本单元测评指标要求。
b) 如果 6.3.3.2. b)为否定，则信息系统不符合本单元测评指标要求。
c) 对于新闻制播系统、播出整备系统、播出系统等播出直接相关系统的终端本单元测评可根据需要进行。

6.3.4 恶意代码防范

6.3.4.1.测评指标

见 GD/J 038-2011 6.3.4。

6.3.4.2.测评实施

本项要求包括：

a) 应访谈安全管理员，终端防恶意代码软件是否统一集中管理；
b) 应检查**统一集中管理功能的**防恶意代码软件版本和恶意代码库是否定期进行更新。

6.3.4.3.结果判定

a) 如果 6.3.4.2. b)为肯定，则信息系统符合本单元测评指标要求。
b) 如果 6.3.4.2. b)为否定，则信息系统不符合本单元测评指标要求。
c) 对于新闻制播系统、播出整备系统、播出系统等播出直接相关系统的终端本单元测评可根据需要进行。

6.4 服务端系统安全

6.4.1 身份鉴别

6.4.1.1.测评指标

见 GD/J 038-2011 6.4.1。

6.4.1.2.测评实施

本项要求包括：

a) 应访谈系统管理员和数据库管理员，询问服务器操作系统和数据库系统的防护措施有哪些，采用何种方式验证用户身份，关闭了哪些不必要的服务和端口，采取何种安全远程管理手段，是否存在共用帐号现象；
b) 应检查服务器操作系统和数据库系统，查看是否配置了对登录用户进行身份鉴别的功能，口令是否有复杂度要求并定期更换，用户名和口令禁止相同；
c) 应检查服务器操作系统和数据库系，查看是否配置了结束会话、限制非法登录次数、远程超时自动退出等鉴别失败处理功能；
d) 应检查服务器操作系统和数据库系，**查看是否采用 HTTPS、SSH 等安全的远程管理手段**。

6.4.1.3. 结果判定

a) 如果 6.4.1.2. b)-d)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 6.4.1.2. b)、c)均为肯定，d)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 6.4.1.2. b)、c)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

6.4.2 访问控制

6.4.2.1. 测评指标

见 GD/J 038-2011 6.4.2。

6.4.2.2. 测评实施

本项要求包括：

a) 应访谈安全管理员，服务器操作系统和数据库系统的访问控制策略有哪些；
b) 应检查服务器操作系统和数据库系统的安全策略，是否控制用户对资源的访问，是否关闭不必要的服务和端口等；
c) 应检查服务器操作系统和数据库系统的安全策略，**特权用户权限是否分离**；
d) 应检查服务器操作系统和数据库管理系统的安全策略，查看是否限制默认帐户的访问权限、windows 系统默认帐户是否重新命名、是否修改帐户的默认口令；
e) 应检查服务器操作系统和数据库系统的帐户设置情况，查看是否及时删除或禁用了系统不必要的帐户、系统过期的帐户。

6.4.2.3. 结果判定

a) 如果 6.4.2.2. b)-e)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 6.4.2.2. b)-e)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

6.4.3 安全审计

6.4.3.1. 测评指标

见 GD/J 038-2011 6.4.3。

6.4.3.2. 测评实施

本项要求包括：

a) **应访谈安全审计员，询问系统安全审计范围包括哪些，审计粒度是否为用户级；询问审计的内容有哪些；询问审计记录有哪些；**
b) **应检查接口服务器、Web 服务器、应用服务器、数据库服务器等重要服务器的审计内容，是否包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；**
c) **应检查接口服务器、Web 服务器、应用服务器、数据库服务器等重要服务器的安全审计记录施，审计记录是否包括：事件的日期、时间、类型、用户名、客户端 IP 地址、访问对象、结果等，是否至少保存 90 天；**
d) **应检查对事件审计记录进行分析的记录，查看是否定期对审计记录进行分析；**
e) **应测试接口服务器、Web 服务器、应用服务器、数据库服务器等重要服务器，可通过某个帐户试图删除、修改或覆盖审计记录，验证审计记录是否受到保护。**

6.4.3.3.结果判定

a) 如果 6.4.3.2. b)-f)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 6.4.3.2. b)、c)均为肯定，d)、e)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 6.4.3.2. b)、c)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

6.4.4 入侵防范

6.4.4.1.测评指标

见 GD/J 038-2011 6.4.4。

6.4.4.2.测评实施

本项要求包括：

a) 应访谈安全管理员，操作系统的安全策略有哪些；采取何种方式更新补丁；
b) 应检查操作系统是否遵循最小安装原则，仅安装需要的组件和应用程序，是否及时更新系统补丁。

6.4.4.3.结果判定

a) 如果 6.4.4.2. b)为肯定，则信息系统符合本单元测评指标要求。
b) 如果 6.4.4.2. b)为否定，则信息系统不符合本单元测评指标要求。
c) 对于新闻制播系统、播出整备系统、播出系统等播出直接相关系统的核心服务器本单元测评可根据需要进行。

6.4.5 恶意代码防范

6.4.5.1.测评指标

见 GD/J 038-2011 6.4.5。

6.4.5.2.测评实施

本项要求包括：

a) 应访谈安全管理员，服务器防恶意代码软件是否统一集中管理；
b) 应**检查统一集中管理功能的**防恶意代码软件版本和恶意代码库是否定期进行更新。

6.4.5.3.结果判定

a) 如果 6.4.5.2. b)为肯定，则信息系统符合本单元测评指标要求。
b) 如果 6.4.5.2. b)为否定，则信息系统不符合本单元测评指标要求。
c) 对于新闻制播系统、播出整备系统、播出系统等播出直接相关系统的核心服务器本单元测评可根据需要进行。

6.4.6 资源控制

6.4.6.1.测评指标

见 GD/J 038-2011 6.4.6。

6.4.6.2.测评实施

本项要求包括：

a) **应访谈安全管理员，询问资源控制相关的策略有哪些；**
b) **应检查服务器，是否通过设定终端接入方式、网络地址范围等条件限制终端登录服务器；**
c) **应检查能够访问服务器的终端，是否依据安全策略设置了操作超时锁定的配置；**
d) **应检查服务器，是否设置了单个用户对系统资源的最大或最小使用限度的阈值。**

6.4.6.3.结果判定

a) 如果 6.4.6.2. b)-d)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 6.4.6.2. b)、c)均为肯定，d)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 6.4.6.2. b)、c)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

6.4.7 冗余配置

6.4.7.1.测评指标

见 GD/J 038-2011 6.4.7。

6.4.7.2.测评实施

本项要求包括：

a) **应访谈系统管理员，询问新闻制播系统、播出整备系统、播出系统等播出直接相关系统的核心服务器具有哪些冗余配置措施；**
b) **应检查新闻制播系统、播出整备系统、播出系统等播出直接相关系统的核心服务器是否具有冗余配置。**

6.4.7.3.结果判定

a) 如果 6.4.7.2. b)为肯定，则信息系统符合本单元测评指标要求。
b) 如果 6.4.7.2. b)为否定，则信息系统不符合本单元测评指标要求。

6.5 应用安全

6.5.1 身份鉴别

6.5.1.1.测评指标

见 GD/J 038-2011 6.5.1。

6.5.1.2.测评实施

本项要求包括：

a) 应访谈应用系统管理员，询问应用系统登录控制具体措施有哪些；采用何种验证方式；是否存在共用帐号现象；
b) 应检查应用系统，**查看是否具有独立的登录控制模块或者将登录控制模块集成到统一的门户认证系统中；**
c) 应检查系统管理用户身份鉴别信息是否具有不易被冒用的特点，口令是否定期更换，用户名和口令禁止相同；
d) 应测试应用系统，**是否提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识；**
e) 应测试同一用户名连续登录失败次数超限时是否有限制，是否有结束会话机制、自动退出机制等措施。

6.5.1.3.结果判定

a) 如果 6.5.1.2. b)-e)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 6.5.1.2. c)-e)均为肯定，b)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 6.5.1.2. c)-e)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

6.5.2 访问控制

6.5.2.1.测评指标

见 GD/J 038-2011 6.5.2。

6.5.2.2.测评实施

本项要求包括：

a) 应访谈应用系统管理员，应用系统的访问控制策略有哪些；
b) 应检查应用系统的访问控制功能，是否依据安全策略控制用户对资源的访问，**控制粒度是否为文件、数据库表级**；
c) 应检查应用系统，查看其是否删除临时帐户和测试帐户，重命名默认帐户，修改其默认口令，限制其访问权限；
d) 应测试应用系统，可通过以不同权限的用户登录系统，查看其拥有的权限是否与系统赋予的权限一致，验证应用系统访问控制功能是否有效；
e) 应测试应用系统，可通过以默认用户登录系统，并进行一些合法和非法操作，验证系统是否严格限制了默认帐户的访问权限；
f) 应测试应用系统，可通过以匿名用户登录系统，验证系统是否不允许匿名用户登录。

6.5.2.3.结果判定

a) 如果6.5.2.2. b)-g)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果6.5.2.2. b)、c)、e)、f)均为肯定，d)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果6.5.2.2. b)、c)、e)、f)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

6.5.3 安全审计

6.5.3.1.测评指标

见GD/J 038-2011 6.5.3。

6.5.3.2.测评实施

本项要求包括：

a) **应访谈安全审计员，询问新闻制播系统、播出整备系统、播出系统等播出直接相关系统是否开启审计功能；询问审计的内容有哪些；询问审计记录有哪些；**
b) **应检查应用系统的审计内容，是否包括审计内容应包括用户登录、修改配置、核心业务操作等重要行为，以及系统资源的异常使用等；**
c) **应检查应用系统的安全审计记录，查看审计记录至少是否包括事件的日期和时间、事件类型、客户端IP地址、描述和结果；**
d) **应检查应用系统的安全审计记录，查看审计记录是否至少保存90天；**
e) **应测试新闻制播系统、播出整备系统、播出系统等播出直接相关系统，可通过某个帐户试图删除、修改或覆盖审计记录，验证审计记录是否受到保护。**

6.5.3.3.结果判定

a) 如果6.5.3.2. b)-e)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果6.5.3.2. b)-d)均为肯定，e)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果6.5.3.2. b)-d)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

6.5.4 通信完整性

6.5.4.1.测评指标

见GD/J 038-2011 6.5.4。

6.5.4.2.测评实施

本项要求包括：

a) **应访谈安全管理员，询问信息系统与外部网络通信时，有哪些保护数据完整性的措施；**
b) **应检查设计或验收文档，查看其是否有关于保护通信完整性的说明，如果有则查看文档中描述的保护措施是否与依据验证码判断对方数据包的有效性的措施相一致；**
c) **应测试主要应用系统，可通过获取与外部网络通信的数据包，查看其在通信过程中是否采用校验码技术、特定的音视频文件格式、特定协议或等同强度的技术手段等进行传输。**

6.5.4.3.结果判定

a) 如果 6.5.4.2. b)、c)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 6.5.4.2. b)为肯定，c)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 6.5.4.2. b)为否定，则信息系统不符合本单元测评指标要求。

6.5.5 通信保密性

6.5.5.1.测评指标

见 GD/J 038-2011 6.5.5。

6.5.5.2.测评实施

本项要求包括：

a) **应访谈安全管理员，询问应用系统与外部网络进行通信时有哪些保密措施；**
b) **应检查应用系统，系统在通信过程中，敏感信息字段是否加密；**
c) **应测试应用系统，通过查看应用系统与外部网络通信时通信双方数据包的内容，查看系统是否能在通信双方建立连接之前，利用密码技术进行会话初始化验证。**

6.5.5.3.结果判定

a) 如果 6.5.5.2. b)、c)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 6.5.5.2. b)为肯定，c)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 6.5.5.2. b)为否定，则信息系统不符合本单元测评指标要求。

6.5.6 软件容错

6.5.6.1 测评指标

见 GD/J 038-2011 6.5.6。

6.5.6.2.测评实施

本项要求包括：

a) 应访谈应用系统管理员，询问应用系统是否具有保证软件容错能力的措施，具体措施有哪些；
b) 应检查应用系统，查看应用系统是否对人机接口输入或通信接口输入的数据进行有效性检验；
c) 应测试应用系统，可通过对人机接口输入的不同长度或格式的数据，查看系统的反应，验证系统人机接口有效性检验功能是否正确，**查看是否对非法输入及进行明确的错误提示并报警；**

6.5.6.3.结果判定

a) 如果 6.5.6.2. b)、c)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 6.5.6.2. b)为肯定，c)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 6.5.6.2. b)为否定，则信息系统不符合本单元测评指标要求。

6.5.7 资源控制

6.5.7.1.测评指标

见 GD/J 038-2011 6.5.7。

6.5.7.2.测评实施

本项要求包括：

a) **应访谈应用系统管理员，询问应用系统的资源控制措施有哪些；**
b) **应检查应用系统，查看系统是否有最大并发会话连接数的限制，是否对单个帐户的多重并发会话进行限制；**
c) **应测试应用系统，当应用系统的通信双方中的一方在一段时间内未作任何响应，查看另一方是否能够自动结束会话。**

6.5.7.3.结果判定

a) 如果 6.5.7.2. b)、c)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 6.5.7.2. b)、c)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

6.6 数据安全与备份恢复

6.6.1 数据完整性

6.6.1.1.测评指标

见 GD/J 038-2011 6.6.1。

6.6.1.2.测评实施

本项要求包括：

a) 应访谈安全管理员，询问用户身份鉴别信息、调度信息、播出节目等重要业务数据在传输过程中完整性保证措施有哪些；
b) 应检查应用系统，查看用户身份鉴别信息、调度信息、播出节目等重要业务数据在传输过程中是否具有完整性保证功能。

6.6.1.3.结果判定

a) 如果 6.6.1.2. b)为肯定，则信息系统符合本单元测评指标要求。
b) 如果 6.6.1.2. b)为否定，则信息系统不符合本单元测评指标要求。

6.6.2 数据保密性

6.6.2.1.测评指标

见 GD/J 038-2011 6.6.2。

6.6.2.2.测评实施

本项要求包括：

a) 应访谈网络管理员，询问网络设备的鉴别信息是否采用加密或其他有效措施实现存储保密性；
b) 应访谈系统管理员，询问主机操作系统的鉴别信息是否采用加密或其他有效措施实现存储保密性；

c) 应访谈数据库管理员，询问数据库管理系统的鉴别信息是否采用加密或其他有效措施实现存储保密性；
d) 应访谈安全管理员，询问应用系统的鉴别信息是否采用加密或其他有效措施实现存储保密性；
e) 应检查主机操作系统、网络设备操作系统、数据库管理系统和应用系统，查看其鉴别信息是否采用加密或其他有效措施实现存储保密性。

6.6.2.3.结果判定

a) 如果 6.6.2.2. e)为肯定，则信息系统符合本单元测评指标要求。
b) 如果 6.6.2.2. e)为否定，则信息系统不符合本单元测评指标要求。

6.6.3 备份与恢复

6.6.3.1.测评指标

见 GD/J 038-2011 6.6.3。

6.6.3.2.测评实施

本项要求包括：

a) 应访谈安全管理员，询问对重要业务信息的备份策略是什么；当其受到破坏时，恢复策略是什么；
b) 应检查备份措施，是否对重要业务信息提供备份和恢复功能。

6.6.3.3.结果判定

a) 如果 6.6.3.2. b)为肯定，则信息系统符合本单元测评指标要求。
b) 如果 6.6.3.2. b)为否定，则信息系统不符合本单元测评指标要求。

7 第三级信息系统单元测评

7.1 基础网络安全

7.1.1 结构安全

7.1.1.1.测评指标

见 GD/J 038-2011 7.1.1。

7.1.1.2.测评实施

本项要求包括：

a) 应访谈网络管理员，询问主要网络设备的性能以及目前业务高峰流量情况，网络中带宽控制情况以及带宽分配的原则；询问**信息系统的**核心交换机、汇聚交换机等关键网络设备是否配置冗余；询问播出整备系统、播出系统、新闻制播系统中的直播演播室系统等播出直接相关系统是否位于纵深结构内部；询问系统内部是否没有通过无线方式组网；询问网络安全域划分情况、网段划分情况以及划分的原则，询问重要网段有哪些，其具体的部署位置，与其他网段的隔离措施有哪些；

b) 应检查网络设计或验收文档，是否有主要网络设备业务处理能力、接入网络及核心网络的带宽满足设计业务高峰期的需要以及不存在带宽瓶颈等方面的设计或描述；
c) 应检查**信息系统**的核心交换机、汇聚交换机等主要网络设备是否配置冗余；
d) 应检查网络拓扑图、网络设计或验收文档，是否根据各信息系统与播出的相关程度进行层次化结构设计，形成网络纵深防护体系，新闻制播系统中的直播演播室系统、播出整备系统、播出系统等播出直接相关系统是否位于纵深结构内部，查看系统内部是否没有通过无线方式进行组网；
e) 应检查网络拓扑图是否与当前的实际网络结构一致；
f) 应检查网络设计或验收文档，是否根据信息系统功能、业务流程、网络结构层次、业务服务对象等合理划分网络安全域，安全域内是否根据业务类型、业务重要性、物理位置等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段；
g) 应检查边界网络设备和关键网络设备，重要网段是否采取了技术隔离手段与其它网段隔离。

7.1.1.3.结果判定

a) 如果 7.1.1.2. b)-g)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.1.1.2. b)-g)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

7.1.2 安全审计

7.1.2.1.测评指标

见 GD/J 038-2011 7.1.2。

7.1.2.2.测评实施

本项要求包括：

a) 应访谈安全审计员，询问关键网络设备是否开启审计功能，审计内容包括哪些项；询问审计记录的主要内容有哪些，对审计记录的处理方式有哪些；**询问关键网络设备或安全审计设备是否为安全管理中心提供集中管理的接口 ；**
b) 应检查关键网络设备或安全审计设备，查看审计策略是否包括网络设备运行状况、用户行为等；
c) 应检查关键网络设备或安全审计设备，查看事件审计记录是否包括：事件的日期和时间、用户名、IP 地址、事件类型、事件成功情况及其他与审计相关的信息；
d) 应检查关键网络设备或安全审计设备的审计记录，是否至少保存 90 天；
e) 应检查对事件审计记录进行分析的记录，查看是否定期对审计记录进行分析；
f) **应检查关键网络设备或安全审计设备，查看其是否为安全管理中心提供集中管理的接口；**
g) 应测试关键网络设备或安全审计设备，可通过以某个帐户登录系统，试图删除、修改或覆盖审计记录，验证安全审计的保护情况与要求是否一致。

7.1.2.3.结果判定

a) 如果 7.1.2.2. b)-g)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.1.2.2. b)-e)均为肯定，f)、g)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 7.1.2.2. b)-e)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

7.1.3 网络设备防护

7.1.3.1.测评指标

见 GD/J 038-2011 7.1.3。

7.1.3.2.测评实施

本项要求包括：

a) 应访谈网络管理员，询问网络设备的防护措施有哪些，采用何种方式验证用户身份，询问网络设备关闭了哪些不必要的服务和端口，远程管理设备时采取何种安全管理手段；**询问如何分配网络特权用户的权限；询问使用何种协议对网络设备进行管理；**

b) 应检查边界网络设备和关键网络设备，查看是否启用了对登录用户进行身份鉴别的功能，口令设置是否有复杂度和定期更换要求，用户名和口令是否禁止相同；

c) **应检查边界网络设备和关键网络设备，查看是否对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别；**

d) 应检查边界网络设备和关键网络设备，查看是否配置了结束会话、限制非法登录次数、远程超时自动退出等鉴别失败处理功能；

e) 应检查边界网络设备和关键网络设备，查看是否关闭了不必要的服务和端口；

f) 应检查边界网络设备和关键网络设备，查看是否对网络设备的管理员登录地址进行限制，仅允许指定 IP 地址或 IP 段访问；**查看是否实现设备特权用户的权限分离；**

g) 应检查远程管理的边界网络设备和关键网络设备，是否采用 HTTPS、SSH 等安全的远程管理手段；

h) **应检查边界网络设备和关键网络设备，是否能够通过安全的网络管理协议提供网络设备的监控与管理接口。**

7.1.3.3.结果判定

a) 如果 7.1.3.2. b)-h)均为肯定，则信息系统符合本单元测评指标要求。

b) 如果 7.1.3.2. b)、d)-h)均为肯定，c)为否定，则信息系统部分符合本单元测评指标要求。

c) 如果 7.1.3.2. b)、d)-h)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

7.2 边界安全

7.2.1 访问控制

7.2.1.1.测评指标

见 GD/J 038-2011 7.2.1。

7.2.1.2.测评实施

本项要求包括：

a) 应访谈安全管理员，询问采取了哪些网络访问控制措施；启用了哪些网络访问控制策略；询问外部网络用户的安全接入方式有哪些；**询问与外部网络数据交换时是否采取带宽分配策略保障重要业务运行；**

b) **应检查网络访问控制设备，是否启用了基于 IP 地址段及端口级的允许/拒绝访问控制策略；**

c) **应检查网络访问控制设备，是否仅允许信息系统使用的必要协议，禁止信息系统未使用的一切通信协议和端口；**
d) **应检查边界网络设备和关键网络设备，是否对重要网段采取网络地址与数据链路地址绑定或其它网络准入控制措施等技术手段防止地址欺骗；**
e) 应检查外部网络用户是否采取安全接入方式，是否基于用户级对用户权限进行管理；
f) 应针对网络访问控制措施进行渗透测试，可通过采用多种渗透测试技术，验证网络访问控制措施是否不存在明显的弱点。

7.2.1.3.结果判定

a) 如果 7.2.1.2. b)-f)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.2.1.2. b)-f)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

7.2.2 安全数据交换

7.2.2.1.测评指标

见 GD/J 038-2011 7.2.2。

7.2.2.2.测评实施

本项要求包括：

a) 应访谈播出系统管理员，询问播出系统与其它信息系统之间交换的文件类型及格式；
b) 应访谈安全管理员，询问是否限定可以通过移动介质交换数据的主机；询问通过其它移动介质上载的内容是否经过两种或两种以上的防恶意代码产品进行恶意代码检查；询问蓝光、P2 等专业移动介质上载是否采用了特定防护机制；
c) 应检查是否采用限定的文件类型及格式与播出系统进行数据交换；
d) 应检查是否限定了可以通过移动介质交换数据的主机，是否安装有两种或两种以上的防恶意代码产品进行恶意代码检查，蓝光、P2 等专业移动介质上载是否采用了特定防护机制；
e) 应检查信息系统与外部网络进行数据交换时，是否通过数据交换区或专用数据交换设备等完成内外网数据的安全交换；
f) 应检查数据交换区对外是否通过访问控制设备与外部网络进行安全隔离，对内是否采用安全的方式进行数据交换。

7.2.2.3.结果判定

a) 如果 7.2.2.2. c)-f)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.2.2.2. c)-f)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

7.2.3 入侵防范

7.2.3.1.测评指标

见 GD/J 038-2011 7.2.3。

7.2.3.2.测评实施

本项要求包括：

a) 应访谈安全管理员，询问网络入侵防范措施有哪些，是否有专门设备对网络入侵进行防范；询问网络入侵防范规则库的升级方式；
b) 应检查网络入侵防范设备，查看是否能检测以下攻击行为：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、网络蠕虫攻击等；
c) **应检查网络入侵防范设备，查看入侵事件记录中是否包括入侵的源 IP、攻击的类型、攻击目的、攻击时间等；**
d) 应检查网络入侵防范设备，查看其规则库是否及时更新；
e) 应测试网络入侵防范设备，验证其检测策略是否有效；
f) **应测试网络入侵防范设备，验证其报警策略是否有效。**

7.2.3.3.结果判定

a) 如果 7.2.3.2. b)-f)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.2.3.2. b)-f)中一项或多项为否定，则信息系统不符合本单元测评指标要求。
c) 对于播出整备系统、播出系统等信息系统本单元测评可根据需要进行。

7.2.4 恶意代码防范

7.2.4.1.测评指标

见 GD/J 038-2011 7.2.4。

7.2.4.2.测评实施

本项要求包括：

a) 应访谈安全管理员，询问网络边界处恶意代码防范措施有哪些，恶意代码库的更新策略；
b) 应检查在**信息系统**网络边界处是否有相应的防恶意代码措施；
c) 应检查**信息系统**网络边界处的防恶意代码产品与信息系统内部防恶意代码产品是否具有不同的恶意代码库；
d) 应检查防恶意代码产品，查看其运行是否正常，恶意代码库是否及时更新。

7.2.4.3.结果判定

a) 如果 7.2.4.2. b)-d)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.2.4.2. b)-d)中一项或多项为否定，则信息系统不符合本单元测评指标要求。
c) 对于播出整备系统、播出系统等播出直接相关系统本单元测评可根据需要进行。

7.2.5 安全审计

7.2.5.1.测评指标

见 GD/J 038-2011 7.2.5。

7.2.5.2.测评实施

本项要求包括：

a) 应访谈安全审计员，询问与外部网络连接的边界处安全审计措施有哪些；审计内容包括哪些项；询问审计记录的主要内容有哪些，对审计记录的处理方式有哪些；**询问安全审计设备是否为安全管理中心提供集中管理的接口 ；**
b) 应检查与外部网络连接的边界处安全审计设备，是否对数据通信行为进行审计；
c) 应检查与外部网络连接的边界处安全审计设备，查看事件审计记录是否包括：事件的日期和时间、用户名、IP 地址、事件类型、事件成功情况及其他与审计相关的信息；
d) 应检查与外部网络连接的边界处安全审计设备，审计记录设置是否满足至少保存 90 天；
e) 应检查对事件审计记录进行分析的记录，查看是否定期对审计记录进行分析；
f) **应检查与外部网络连接的边界处安全审计设备，查看其是否为安全管理中心提供集中管理的接口；**
g) 应测试与外部网络连接的边界处安全审计设备，可通过以某个帐户登录系统，试图删除、修改或覆盖审计记录，验证安全审计的保护情况与要求是否一致。

7.2.5.3.结果判定

a) 如果 7.2.5.2. b)-g)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.2.5.2. b)-e)均为肯定，f)、g)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 7.2.5.2. b)-e)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

7.2.6 边界完整性

7.2.6.1.测评指标

见 GD/J 038-2011 7.2.6。

7.2.6.2.测评实施

本项要求包括：

a) 应访谈安全管理员，**询问非授权设备私自联到内部网络的行为检查措施有哪些**；询问内部网络用户联到外部网络的行为有哪些；
b) **应检查边界完整性检查措施，是否能够对内部网络用户私自联到外部网络的行为检查；**
c) **应检查边界完整性检查措施，是否能够对非授权设备私自联到内部网络的行为进行有效阻断；**
d) 应测试边界完整性检查措施，是否能够对内部网络用户私自联到外部网络的行为**进行有效的阻断；**
e) 应测试边界完整性检查措施，是否能够**对非授权设备私自联到内部网络的行为**进行有效的阻断。

7.2.6.3.结果判定

a) 如果 7.2.6.2. b)-e)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.2.6.2. b)-e)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

7.3 终端系统安全

7.3.1 身份鉴别

7.3.1.1.测评指标

见 GD/J 038-2011 7.3.1。

7.3.1.2.测评实施

本项要求包括：

a) 应访谈安全管理员，询问终端操作系统采用了何种身份标识和鉴别机制；
b) 应检查终端操作系统，是否提供了身份标识和鉴别措施；
c) 应检查终端操作系统，是否设置口令复杂度要求，口令是否定期进行更换，用户名和口令是否禁止相同。

7.3.1.3.结果判定

a) 如果 7.3.1.2. b)、c)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.3.1.2. b)、c)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

7.3.2 访问控制

7.3.2.1.测评指标

见 GD/J 038-2011 7.3.2。

7.3.2.2.测评实施

本项要求包括：

a) 应访谈安全管理员，是否制定了资源访问的安全策略；
b) 应检查终端的资源访问安全策略，查看是否禁止通过 USB、**光驱**等外设进行数据交换，是否关闭系统不必要的服务和端口等。

7.3.2.3.结果判定

a) 如果 7.3.2.2. b)为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.3.2.2. b)为否定，则信息系统不符合本单元测评指标要求。

7.3.3 安全审计

7.3.3.1.测评指标

见 GD/J 038-2011 7.3.3。

7.3.3.2.测评实施

本项要求包括：

a) **应访谈安全审计员，询问对重要终端是否进行审计，审计粒度是否为用户级；询问审计的内容有哪些；询问审计记录有哪些；询问安全审计设备是否为安全管理中心提供集中管理的接口；**
b) **应检查重要终端的审计内容，是否包括重要用户行为、系统资源的异常使用和重要系统命令的使用及其它与审计相关的信息等；**

c) **应检查重要终端的安全审计措施，查看审计记录是否包括：事件的日期、时间、用户名、访问对象、结果等；**
d) **应检查重要终端的安全审计记录，是否至少保存 90 天；**
e) **应检查对事件审计记录进行分析的记录，查看是否定期对审计记录进行分析；**
f) **应检查重要终端的安全审计措施，查看其是否为安全管理中心提供集中管理的接口；**
g) **应测试重要终端的安全审计措施，可通过以某个帐户登录系统，试图删除、修改或覆盖审计记录，验证安全审计的保护情况与要求是否一致；**
h) **应测试重要终端操作系统可通过某个帐户试图中断审计进程，验证审计进程是否受到保护。**

7.3.3.3.结果判定

a) 如果 7.3.3.2. b)-h)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.3.3.2. b)-d)均为肯定，e)-h)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 7.3.3.2. b)-d)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

7.3.4 入侵防范

7.3.4.1.测评指标

见 GD/J 038-2011 7.3.4。

7.3.4.2.测评实施

本项要求包括：

a) 应访谈安全管理员，终端操作系统的入侵防范措施有哪些；采取何种方式更新补丁；
b) 应检查终端操作系统是否遵循最小安装原则，仅安装需要的组件和应用程序，是否及时更新系统补丁；
c) **应检查补丁升级服务器，是否定期更新操作系统补丁。**

7.3.4.3.结果判定

a) 如果 7.3.4.2. b)、c)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.3.4.2 b)为肯定，c)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 7.3.4.2. b)中一项或多项为否定，则信息系统不符合本单元测评指标要求。
d) 对于新闻制播系统、播出整备系统、播出系统等播出直接相关系统的终端本单元测评可根据需要进行。

7.3.5 恶意代码防范

7.3.5.1.测评指标

见 GD/J 038-2011 7.3.5。

7.3.5.2.测评实施

本项要求包括：

a) 应访谈安全管理员，是否部署具有统一集中管理功能的终端防恶意代码软件；

b) 应检查统一集中管理功能的防恶意代码软件版本和恶意代码库是否定期进行更新。

7.3.5.3.结果判定

a) 如果 7.3.5.2. b)为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.3.5.2. b)为否定，则信息系统不符合本单元测评指标要求。
c) 对于新闻制播系统、播出整备系统、播出系统等播出直接相关系统的终端本单元测评可根据需要进行。

7.4 服务端系统安全

7.4.1 身份鉴别

7.4.1.1.测评指标

见 GD/J 038-2011 7.4.1。

7.4.1.2.测评实施

本项要求包括：

a) 应分别访谈系统管理员和数据库管理员，询问服务器操作系统和数据库系统的防护措施有哪些，采用何种方式验证用户身份，关闭了哪些不必要的服务和端口，采取何种安全远程管理手段，是否存在共用帐号现象；
b) 应检查服务器操作系统和数据库系统，查看是否配置了对登录用户进行身份鉴别的功能，口令设置是否有复杂度和定期更换要求，用户名和口令是否禁止相同；
c) **应检查服务器操作系统和数据库系统，查看是否对管理用户采用两种或两种以上组合的鉴别技术来进行身份鉴别；**
d) 应检查服务器操作系统和数据库系统，查看是否配置了结束会话、限制非法登录次数、远程超时自动退出等鉴别失败处理功能；
e) 应检查服务器操作系统和数据库系统，查看是否采用 HTTPS、SSH 等安全的远程管理手段。

7.4.1.3.结果判定

a) 如果 7.4.1.2. b)-e)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.4.1.2. b)、d)均为肯定，c)、e)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 7.4.1.2. b)、d)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

7.4.2 访问控制

7.4.2.1.测评指标

见 GD/J 038-2011 7.4.2。

7.4.2.2.测评实施

本项要求包括：

a) 应访谈安全管理员，询问服务器操作系统和数据库系统的访问控制策略有哪些，是否存在共用帐户现象；
b) 应检查服务器操作系统和数据库系统的安全策略，查看是否控制用户对资源的访问，是否关闭不必要的服务和端口等；
c) 应检查服务器操作系统和数据库系统的安全策略，查看是否**根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限，**特权用户权限是否分离；
d) 应检查服务器操作系统和数据库管理系统的安全策略，查看是否限制默认帐户的访问权限、windows 系统默认帐户是否重新命名、是否修改帐户的默认口令；
e) 应检查服务器操作系统和数据库系统的帐户设置情况，查看是否及时删除或禁用了系统不必要的帐户、系统过期的帐户；
f) **应检查服务器操作系统和数据库管理系统，查看是否对高风险服务器的重要信息资源设置敏感标记，是否依据安全策略严格控制用户对有敏感标记的重要信息资源的操作。**

7.4.2.3.结果判定

a) 如果 7.4.2.2. b)-f)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.4.2.2. b)-e)均为肯定，f)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 7.4.2.2. b)-e)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

7.4.3 安全审计

7.4.3.1.测评指标

见 GD/J 038-2011 7.4.3。

7.4.3.2.测评实施

本项要求包括：

a) 应访谈安全审计员，询问系统安全审计范围、内容、记录各有哪些；**询问安全审计设备是否为安全管理中心提供集中管理的接口；**
b) 应检查接口服务器、Web 服务器、应用服务器、数据库服务器等重要服务器的审计内容，是否包括重要用户行为、系统资源的异常使用和重要系统命令的使用及其它与审计相关的信息等，审计粒度是否为用户级；
c) 应检查接口服务器、Web 服务器、应用服务器、数据库服务器等重要服务器的安全审计记录，审计记录是否包括：事件的日期、时间、类型、用户名、客户端 IP 地址、访问对象、结果等，是否至少保存 90 天；
d) 应检查对事件审计记录进行分析的记录，查看是否定期对审计记录进行分析；
e) **应检查与接口服务器、Web 服务器、应用服务器、数据库服务器等重要服务器端的安全审计措施，查看其是否为安全管理中心提供集中管理的接口；**
f) 应测试接口服务器、Web 服务器、应用服务器、数据库服务器等重要服务器，可通过某个帐户试图中断审计进程，验证审计进程是否受到保护；
g) 应测试接口服务器、Web 服务器、应用服务器、数据库服务器等重要服务器，可通过某个帐户试图删除、修改或覆盖审计记录，验证审计记录是否受到保护。

7.4.3.3.结果判定

a) 如果 7.4.3.2. b)-g)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.4.3.2. b)-d)均为肯定，e)-g)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 7.4.3.2. b)-d)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

7.4.4 入侵防范

7.4.4.1.测评指标

见 GD/J 038-2011 7.4.4。

7.4.4.2.测评实施

本项要求包括：

a) 应访谈安全管理员，操作系统的入侵防范措施有哪些；采取何种方式更新补丁；
b) 应检查操作系统是否遵循最小安装原则，仅安装必要的组件和应用程序，是否及时更新系统补丁；
c) **应检查补丁升级服务器，是否定期更新操作系统补丁；**
d) **应检查针对重要服务器的入侵防范措施，在发生严重入侵事件时提供报警，查看入侵事件记录中是否包括入侵的源 IP、目的 IP、攻击的类型和时间等；**
e) 应检查针对**重要服务器的入侵防范措施**，查看其规则库是否及时更新。

7.4.4.3.结果判定

a) 如果 7.4.4.2. b)-e)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.4.4.2. b)、d)为肯定，c)、e)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 7.4.4.2. b)、d)中一项或多项为否定，则信息系统不符合本单元测评指标要求；
d) 对于新闻制播系统、播出整备系统、播出系统等播出直接相关系统的核心服务器本单元测评可根据需要进行。

7.4.5 恶意代码防范

7.4.5.1.测评指标

见 GD/J 038-2011 7.4.5。

7.4.5.2.测评实施

本项要求包括：

a) 应访谈安全管理员，服务器防恶意代码软件是否统一集中管理；
b) 应检查统一集中管理功能的防恶意代码软件版本和恶意代码库是否定期进行更新。

7.4.5.3.结果判定

a) 如果 7.4.5.2. b)为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.4.5.2. b)为否定，则信息系统不符合本单元测评指标要求。
c) 对于新闻制播系统、播出整备系统、播出系统等播出直接相关系统的核心服务器本单元测评可根据需要进行。

7.4.6 资源控制

7.4.6.1.测评指标

见 GD/J 038-2011 7.4.6。

7.4.6.2.测评实施

本项要求包括：

a) 应访谈安全管理员，资源控制相关的策略有哪些；
b) 应检查服务器，是否通过设定终端接入方式、网络地址范围等条件限制终端登录服务器；
c) 应检查服务器，是否依据安全策略配置了操作超时锁定；
d) 应检查服务器，是否设置了单个用户对系统资源的最大或最小使用限度的阈值。

7.4.6.3.结果判定

a) 如果 7.4.6.2. b)-d)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.4.6.2. b)、c)均为肯定，d)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 7.4.6.2. b)、c)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

7.4.7 冗余配置

7.4.7.1 测评指标

见 GD/J 038-2011 7.4.7。

7.4.7.2.测评实施

本项要求包括：

a) 应访谈系统管理员，询问新闻制播系统、播出整备系统、播出系统等播出直接相关系统的核心服务器采取了哪些冗余配置措施；
b) 应检查新闻制播系统、播出整备系统、播出系统等播出直接相关系统的核心服务器是否部署了冗余配置措施，并**具备切换机制**。

7.4.7.3 结果判定

c) 如果 7.4.7.2. b)为肯定，则信息系统符合本单元测评指标要求。
d) 如果 7.4.7.2. b)为否定，则信息系统不符合本单元测评指标要求。

7.5 应用安全

7.5.1 身份鉴别

7.5.1.1.测评指标

见 GD/J 038-2011 7.5.1。

7.5.1.2.测评实施

本项要求包括：

a) 应访谈应用系统管理员，询问应用系统登录控制措施有哪些，采用何种验证方式，是否存在共用帐号现象；
b) 应检查应用系统，查看是否具有独立的登录控制模块或者将登录控制模块集成到统一的门户认证系统中；
c) 应检查应用系统，查看管理用户口令是否要求定期更换，用户名和口令禁止相同；
d) 应检查应用系统，查看其是否**对管理用户和重要业务操作用户采用两种或两种以上组合的鉴别技术对其身份进行鉴别；**
e) 应测试应用系统，是否提供用户身份标识唯一和鉴别信息复杂度检查功能；
f) 应测试同一用户连续登录失败次数是否有限制，是否有结束会话机制、自动退出机制等措施。

7.5.1.3.结果判定

a) 如果 7.5.1.2. b)-f)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.5.1.2. c)-f)均为肯定，b)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 7.5.1.2. c)-f)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

7.5.2 访问控制

7.5.2.1.测评指标

见 GD/J 038-2011 7.5.2。

7.5.2.2.测评实施

本项要求包括：

a) 应访谈应用系统管理员，询问应用系统的访问控制策略有哪些；
b) 应检查应用系统的访问控制功能，是否依据安全策略控制用户对资源的访问，控制粒度是否为文件、数据库表级；
c) 应检查应用系统，查看其是否删除测试帐户和不再使用的临时帐户，是否重命名默认帐户，修改其默认口令，限制其访问权限；
d) **应检查高风险服务器的重要信息资源是否设置敏感标记，查看是否依据安全策略控制用户对有敏感标记的重要信息资源的操作；**
e) 应测试应用系统，可通过以不同权限的用户登录系统，查看其拥有的权限是否与系统赋予的权限一致，验证应用系统访问控制功能是否有效；
f) 应测试应用系统，尝试以默认用户登录系统，并进行一些合法和非法操作，验证系统是否严格限制了默认帐户的访问权限；
g) 应测试应用系统，尝试以匿名用户登录系统，验证系统是否不允许匿名用户登录。

7.5.2.3.结果判定

a) 如果 7.5.2.2. b)-g)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.5.2.2. b)、c)、e)-g)均为肯定，d)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 7.5.2.2. b)、c)、e)-g)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

7.5.3 安全审计

7.5.3.1.测评指标

见 GD/J 038-2011 7.5.3。

7.5.3.2.测评实施

本项要求包括：

a) 应访谈安全审计员，询问对应用系统是否开启审计功能，**审计粒度是否为用户级**；询问审计的内容有哪些；询问审计记录有哪些；**询问安全审计设备是否为安全管理中心提供集中管理的接口；**
b) 应检查应用系统的审计内容，是否包括审计内容应包括用户登录、修改配置、核心业务操作等重要行为，以及系统资源的异常使用等；
c) 应检查应用系统的安全审计记录，查看审计记录是否至少包括事件的日期和时间、事件类型、客户端 IP 地址、描述和结果；
d) 应检查应用系统的安全审计记录，查看审计记录是否至少保存 90 天；
e) 应检查应用系统的安全审计功能，**对审计记录数据是否提供统计、查询、分析及生成审计报表的功能；**
f) **应检查与应用系统的安全审计功能，查看其是否为安全管理中心提供集中管理的接口；**
g) **应测试应用系统的安全审计功能，尝试以某个帐户试图中断审计进程，验证审计进程是否受到保护；**
h) 应测试应用系统的安全审计功能，尝试以某个帐户删除、修改或覆盖审计记录，验证审计记录是否受到保护。

7.5.3.3.结果判定

a) 如果 7.5.3.2. b)-h)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.5.3.2. b)-d)均为肯定，e)-h)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 7.5.3.2. b)-d)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

7.5.4 通信完整性

7.5.4.1.测评指标

见 GD/J 038-2011 7.5.4。

7.5.4.2.测评实施

本项要求包括：

a) 应访谈安全管理员，询问有哪些完整性保护措施；
b) 应检查设计或验收文档，查看其是否有关于保护通信完整性的说明；
c) 应测试主要应用系统，尝试获取通信双方的数据包，查看其在通信过程中是否采用校验码技术、特定的音视频文件格式、特定协议或等同强度的技术手段等进行传输。

7.5.4.3.结果判定

a) 如果 7.5.4.2. b)、c)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.5.4.2. b)为肯定，c)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 7.5.4.2. b)为否定，则信息系统不符合本单元测评指标要求。

7.5.5 通信保密性

7.5.5.1.测评指标

见 GD/J 038-2011 7.5.5。

7.5.5.2.测评实施

本项要求包括：

a) 应访谈安全管理员，询问应用系统与外部网络进行通信时有哪些保密措施；
b) 应检查应用系统，系统在通信过程中，敏感信息字段是否加密；
c) 应测试应用系统，查看应用系统与外部网络通信时通信双方数据包的内容，查看系统是否能在通信双方建立连接之前，利用密码技术进行会话初始化验证。

7.5.5.3.结果判定

a) 如果 7.5.5.2. b)、c)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.5.5.2. b)为肯定，c)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 7.5.5.2. b)为否定，则信息系统不符合本单元测评指标要求。

7.5.6 软件容错

7.5.6.1.测评指标

见 GD/J 038-2011 7.5.6。

7.5.6.2.测评实施

本项要求包括：

a) 应访谈应用系统管理员，询问应用系统保证软件容错的措施有哪些；
b) 应检查应用系统，查看应用系统是否对人机接口输入或通信接口输入的数据进行有效性检验；
c) 应测试应用系统，尝试对人机接口输入的不同长度或格式的数据，查看系统的反应，验证系统人机接口有效性检验功能是否正确，查看是否对非法输入及进行明确的错误提示并报警。

7.5.6.3.结果判定

a) 如果 7.5.6.2. b)、c)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.5.6.2. b)为肯定，c)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 7.5.6.2. b)为否定，则信息系统不符合本单元测评指标要求。

7.5.7 资源控制

7.5.7.1 测评指标

见 GD/J 038-2011 7.5.7。

7.5.7.2.测评实施

本项要求包括：

a) 应访谈应用系统管理员，询问应用系统资源控制措施有哪些；
b) 应检查应用系统，查看系统是否有最大并发会话连接数的限制，是否对单个帐户的多重并发会话进行限制；
c) 应检查应用系统，**查看是否对一个时间段内可能的并发会话连接数进行限制；**
d) 应检查应用系统，**查看是否对一个访问帐户或一个请求进程占用的资源分配最大限额和最小限额；**
e) 应测试应用系统，当应用系统的通信双方中的一方在一段时间内未作任何响应，查看另一方是否能够自动结束会话。

7.5.7.3.结果判定

a) 如果 7.5.7.2. b)-e)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.5.7.2. b)、e)均为肯定，c)、d)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 7.5.7.2. b)、e)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

7.6 数据安全与备份恢复

7.6.1 数据完整性

7.6.1.1 测评指标

见 GD/J 038-2011 7.6.1。

7.6.1.2.测评实施

本项要求包括：

a) 应访谈安全管理员，询问**系统管理数据**、用户身份鉴别信息、调度信息、播出节目等重要业务数据在传输和**存储**过程中完整性保证措施有哪些；**在检测到完整性破坏时，恢复措施有哪些**；
b) 应检查应用系统，查看系统管理数据、用户身份鉴别信息、调度信息、播出节目等重要业务数据在传输和存储过程中是否具有完整性保证功能；
c) **应检查应用系统，查看重要业务数据在传输和存储过程中完整性破坏时是否采取必要的恢复措施。**

7.6.1.3.结果判定

a) 如果 7.6.1.2. b)、c)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.6.1.2. b)为肯定，c)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 7.6.1.2. b)为否定，则信息系统不符合本单元测评指标要求。

7.6.2 数据保密性

7.6.2.1.测评指标

见 GD/J 038-2011 7.6.2。

7.6.2.2.测评实施

本项要求包括：

a) 应访谈网络管理员，询问网络设备的鉴别信息否采用加密或其他有效措施实现存储保密性；
b) 应访谈系统管理员，询问主机操作系统的鉴别信息否采用加密或其他有效措施实现存储保密性；
c) 应访谈数据库管理员，询问数据库管理系统的鉴别信息否采用加密或其他有效措施实现存储保密性；
d) 应访谈安全管理员，询问应用系统的鉴别信息否采用加密或其他有效措施实现存储保密性；
e) 应检查主机操作系统、网络设备操作系统、数据库管理系统和应用系统，查看其鉴别信息否采用加密或其他有效措施实现存储保密性。

7.6.2.3.结果判定

a) 如果 7.6.2.2. e)为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.6.2.2. e)为否定，则信息系统不符合本单元测评指标要求。

7.6.3 备份与恢复

7.6.3.1.测评指标

见 GD/J 038-2011 7.6.3。

7.6.3.2.测评实施

本项要求包括：

a) 应访谈网络管理员，询问是否对网络设备中的配置文件进行备份，备份策略是什么；当其受到破坏时，恢复策略是什么；是否提供主要网络设备的硬件冗余；
b) 应访谈系统管理员，询问是否对操作系统中的重要信息进行备份，备份策略是什么；当其受到破坏时，恢复策略是什么；是否提供主要服务器的硬件冗余；
c) 应访谈数据库管理员，询问是否对数据库管理系统中的数据进行备份，备份策略是什么；当其受到破坏时，恢复策略是什么；
d) 应访谈安全管理员，询问是否对应用系统中的应用程序进行备份，备份策略是什么；当其受到破坏时，恢复策略是什么；
e) 应检查设计或验收文档，查看其是否有关于重要业务数据、系统配置数据本地和异地备份和恢复功能及策略的描述，**完全数据备份至少每周一次，增量备份或差分备份至少每天一次，备份介质应在数据执行所在场地外存放；**
f) 应检查主机操作系统、网络设备、数据库管理系统和应用系统，查看其是否提供备份和恢复功能，其配置是否正确，并且查看其备份结果是否与备份策略一致。

7.6.3.3.结果判定

a) 如果 7.6.3.2. e)、f)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.6.3.2. e)、f)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

7.7 安全管理中心

7.7.1 运行监测

7.7.1.1.测评指标

见 GD/J 038-2011 7.7.1。

7.7.1.2.测评实施

本项要求包括：

a) **应访谈系统管理员、网络管理员、应用系统管理员、数据库管理员，询问是否具有安全运行监测措施，安全运行监测的功能和范围包括哪些；**
b) **应检查安全管理中心，是否对网络及网络设备包括链路状态、核心交换机、汇聚交换机等主要设备的设备状态、设备端口状态、端口 IP、关键节点的网络流量等进行监控；**
c) **应检查安全管理中心，是否监控重要服务器的各项资源指标，包括：CPU、内存、进程和磁盘等使用情况；**
d) **应检查安全管理中心，是否监控数据库的运行状态、进程占用 CPU 时间及内存大小、配置和告警数据等进行监控；**
e) **应检查安全管理中心，是否对重要应用软件的运行状态、响应时间等进行监控；**
f) **应检查安全管理中心，是否对终端的非法接入和非法外联进行监控；**
g) **应检查监控记录，查看是否记录监控对象、监控内容、监控的异常现象处理等方面。**

7.7.1.3.结果判定

a) 如果 7.7.1.2. b)-g)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.7.1.2. b)-d)为肯定，e)-g)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 7.7.1.2. b)-d)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

7.7.2 安全管理

7.7.2.1.测评指标

见 GD/J 038-2011 7.7.2。

7.7.2.2.测评实施

本项要求包括：

a) **应访谈安全管理员，询问是否具有安全管理措施，安全管理的功能和范围包括哪些；**
b) **应检查安全管理中心，是否对信息系统的恶意代码、补丁升级等进行集中统一管理；**
c) **应检查信息系统的恶意代码、补丁升级是否集中统一管理；**
d) **应检查是否具有时钟同步措施，查看是否能够对信息系统网络设备、终端、服务器以及应用等采取时钟同步措施；**
e) **应检查是否能够对网络设备、服务器、应用系统、安全设备等的安全事件信息进行关联分析及风险预警。**

7.7.2.3.结果判定

a) 如果 7.7.2.2. b)-e)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.7.2.2. b)-d)均为肯定，e)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 7.7.2.2. b)-d)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

7.7.3 审计管理

7.7.3.1.测评指标

见 GD/J 038-2011 7.7.3。

7.7.3.2.测评实施

本项要求包括：

a) **应访谈安全审计员，询问安全审计的功能和范围包括哪些；**
b) **应检查安全审计措施，是否对审计记录进行统计、查询、分析及生成审计报表；**
c) **应检查安全审计措施，是否对 90 天以上的审计日志进行归档，归档日志至少保存一年以上；**
d) **应检查基础网络、边界安全、服务器及应用系统的安全审计是否进行集中管理。**

7.7.3.3.结果判定

a) 如果 7.7.3.2. b)-d)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 7.7.3.2. b)、d)为肯定，c)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 7.7.3.2. b)、d)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

8 第四级信息系统单元测评

8.1 基础网络安全

8.1.1 结构安全

8.1.1.1.测评指标

见 GD/J 038-2011 8.1.1。

8.1.1.2.测评实施

本项要求包括：

a) 应访谈网络管理员，询问**网络设备**的性能以及目前业务高峰流量情况，网络中带宽控制情况以及带宽分配的原则；询问信息系统的核心交换机、汇聚交换机等网络设备和通信线路是否配置冗余；询问是否根据各信息系统的播出相关度进行层次化网络结构设计，**四级信息系统是否位于纵深结构内部**，询问系统内部是否没有通过无线方式组网；询问网络安全域划分情况、网段划分情况以及划分的原则，询问重要网段有哪些，其具体的部署位置，与其他网段的隔离措施有哪些；
b) 应检查网络设计或验收文档，是否有网络设备业务处理能力、接入网络及核心网络的带宽满足业务高峰期的需要以及不存在带宽瓶颈等方面的设计或描述；
c) 应检查信息系统的核心交换机、汇聚交换机等网络设备和**通信线路**是否配置冗余；

d) 应检查网络拓扑图、网络设计或验收文档，是否根据各信息系统的播出相关度进行层次化网络结构设计，形成网络纵深防护体系，**四级信息系统是否位于纵深结构内部，**查看系统内部是否没有通过无线方式进行组网；
e) 应检查网络拓扑结构图是否与当前的实际网络结构一致；
f) 应检查网络设计或验收文档，是否根据信息系统功能、业务流程、网络结构层次、业务服务对象等合理划分网络安全域，安全域内是否根据业务类型、业务重要性、物理位置等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段；
g) 应检查网络设备，重要网段是否采取了技术隔离手段与与其它网段隔离。

8.1.1.3.结果判定

a) 如果 8.1.1.2. b)-g)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 8.1.1.2. b)-g)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

8.1.2 安全审计

8.1.2.1.测评指标

见 GD/J 038-2011 8.1.2。

8.1.2.2.测评实施

本项要求包括：

a) 应访谈安全审计员，询问**网络设备**是否开启审计功能，审计内容包括哪些项；询问审计记录的主要内容有哪些，对审计记录的处理方式有哪些；询问网络设备或安全审计设备是否为安全管理中心提供集中管理的接口 ；
b) 应检查**网络设备**或安全审计设备，查看审计策略是否包括网络设备运行状况、用户行为等；
c) 应检查**网络设备**或安全审计设备，查看事件审计记录是否包括：事件的日期和时间、用户名、IP 地址、事件类型、事件成功情况及其他与审计相关的信息；
d) 应检查**网络设备**或安全审计设备，是否提供安全审计记录存储等功能，审计记录是否满足至少保存 90 天；
e) **应检查是否定期对审计记录进行分析，是否生成审计报表；**
f) 应检查**网络设备**或安全审计设备，查看其是否为安全管理中心提供集中管理的接口；
g) 应测试**网络设备**或安全审计设备，可通过以某个用户登录系统，试图删除、修改或覆盖审计记录，验证安全审计的保护情况与要求是否一致。

8.1.2.3.结果判定

a) 如果 8.1.2.2. b)-g)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 8.1.2.2. b)-e)均为肯定，f)、g)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 8.1.2.2. b)-e)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

8.1.3 网络设备防护

8.1.3.1.测评指标

见 GD/J 038-2011 8.1.3。

8.1.3.2.测评实施

本项要求包括：

a) 应访谈网络管理员，询问网络设备的防护措施有哪些，采用何种方式验证用户身份，关闭了哪些不必要的服务和端口，远程管理设备时采取何种安全管理手段；**询问如何分配网络特权用户的权限；询问使用何种协议对网络设备进行管理；**
b) 应检查边界网络设备和关键网络设备，查看是否启用了对登录用户进行身份鉴别的功能，口令是否有复杂度要求并定期更换，用户名和口令是否禁止相同；
c) 应检查边界网络设备和关键网络设备，查看是否对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别，**身份鉴别信息至少有一种是不可伪造的；**
d) 应检查边界网络设备和关键网络设备，查看是否配置了结束会话、限制非法登录次数、远程超时自动退出等鉴别失败处理功能；
e) 应检查边界网络设备和关键网络设备，查看是否关闭了不必要的服务和端口；
f) 应检查边界网络设备和关键网络设备，查看是否对网络设备的管理员登录地址进行限制，**至少控制到 IP 地址；**查看是否实现设备特权用户的权限分离；
g) 应检查边界网络设备和关键网络设备，查看网络设备是否采用 HTTPS、SSH 等安全的远程管理手段；
h) 应检查边界网络设备和关键网络设备，是否能够通过安全的网络管理协议提供网络设备的监控与管理接口。

8.1.3.3.结果判定

a) 如果 8.1.3.2. b)-h)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 8.1.3.2. b)、d)-h)均为肯定，c)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 8.1.3.2. b)、d)-h)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

8.2 边界安全

8.2.1 访问控制

8.2.1.1.测评指标

见 GD/J 038-2011 8.2.1。

8.2.1.2.测评实施

本项要求包括：

a) 应访谈安全管理员，询问采取了哪些网络访问控制措施；启用了哪些网络访问控制策略；
b) 应检查网络访问控制设备，是否仅允许信息系统使用的必要协议，禁止信息系统未使用的一切通信协议和端口；
c) 应检查边界网络设备和关键网络设备，是否对重要网段采取网络地址与数据链路地址绑定或其它网络准入控制措施等技术手段防止地址欺骗；

d) 应对网络访问控制措施进行渗透测试，可通过采用多种渗透测试技术，验证网络访问控制措施是否不存在明显的弱点。

8.2.1.3.结果判定

a) 如果 8.2.1.2. b)-d)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 8.2.1.2. b)-d)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

8.2.2 安全数据交换

8.2.2.1.测评指标

见 GD/J 038-2011 8.2.2。

8.2.2.2.测评实施

本项要求包括：

a) 应访谈播出系统管理员，询问播出系统与其它信息系统之间交换的文件类型及格式；
b) 应访谈安全管理员，询问是否限定可以通过移动介质交换数据的主机；询问通过其它移动介质上载的内容是否经过两种或两种以上的防恶意代码产品进行恶意代码检查；询问蓝光、P2 等专业移动介质上载是否采用了特定防护机制；
c) 应检查是否采用限定的文件类型及格式与播出系统进行数据交换；
d) 应检查是否限定了可以通过移动介质交换数据的主机，是否安装有两种或两种以上的防恶意代码产品进行恶意代码检查，蓝光、P2 等专业移动介质上载是否采用了特定防护机制；
e) **应检查网络边界处对媒体数据和其它数据是否进行区分，视频媒体数据外的其它数据是否通过协议转换的手段，以信息摆渡的方式实现数据交换；**
f) 应检查专用数据交换设备的配置，查看关键数据是否以信息摆渡的方式实现数据交换。

8.2.2.3.结果判定

a) 如果 8.2.2.2. c)-f)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 8.2.2.2. c)-f)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

8.2.3 入侵防范

8.2.3.1.测评指标

见 GD/J 038-2011 8.2.3。

8.2.3.2.测评实施

本项要求包括：

a) 应访谈安全管理员，询问网络入侵防范措施有哪些，是否有专门设备对网络入侵进行防范；询问网络入侵防范规则库的升级方式；
b) 应检查网络入侵防范设备，查看是否能检测以下攻击行为：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、网络蠕虫攻击等；
c) 应检查网络入侵防范设备，查看入侵事件记录中是否包括入侵的源 IP、攻击的类型、攻击目的、攻击时间，在**发生严重入侵事件时，是否提供报警并自动采取相应动作**；

d) 应检查网络入侵防范设备，查看其规则库是否为最新；
e) 应测试网络入侵防范设备，验证其检测策略是否有效；
f) 应测试网络入侵防范设备，验证其报警策略是否有效。

8.2.3.3.结果判定

a) 如果 8.2.3.2. b)-f)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 8.2.3.2. b)-f)中一项或多项为否定，则信息系统不符合本单元测评指标要求。
c) 本单元测评可根据需要进行。

8.2.4 恶意代码防范

8.2.4.1.测评指标

见 GD/J 038-2011 8.2.4。

8.2.4.2.测评实施

本项要求包括：

a) 应访谈安全管理员，询问网络边界处恶意代码防范措施有哪些，恶意代码库的更新策略；
b) 应检查网络设计或验收文档，**查看是否有在信息系统的网络边界处对媒体数据和信息数据进行区分的描述；**
c) 应检查在信息系统网络边界处是否有相应的防恶意代码措施；
d) 应检查防恶意代码产品，查看**是否采用离线方式更新、手工更新的方式进行恶意代码库更新；**
e) 应检查信息系统网络边界处的防恶意代码产品与信息系统内部防恶意代码产品是否具有不同的恶意代码库。

8.2.4.3.结果判定

a) 如果 8.2.4.2. b)-e)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 8.2.4.2. b)-e)中一项或多项为否定，则信息系统不符合本单元测评指标要求。
c) 本单元测评指标可根据需要进行测评。

8.2.5 边界完整性

8.2.5.1.测评指标

见 GD/J 038-2011 8.2.5。

8.2.5.2.测评实施

本项要求包括：

a) 应访谈安全管理员，询问非授权设备私自联到内部网络的行为检查措施有哪些；询问内部网络用户联到外部网络的行为有哪些；
b) 应检查边界完整性检查措施，是否能够对非授权设备私自联到内部网络的行为检查，**准确定出位置**，并对其进行有效的阻断；
c) 应检查边界完整性检查措施，是否能够对内部网络用户私自联到外部网络的行为检查，**准确定出位置，**并对其进行有效的阻断；

d) 应测试边界完整性检查措施，测试是否能够对私自联到内部网络的非授权设备进行检查，并对其进行有效阻断；
e) 应测试边界完整性检查措施，测试是否能够对私自联到外部网络的内部网络用户进行检查，并对其进行有效阻断。

8.2.5.3.结果判定

a) 如果 8.2.5.2. b)-e)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 8.2.5.2. b)-e)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

8.3 终端系统安全

8.3.1 身份鉴别

8.3.1.1.测评指标

见 GD/J 038-2011 8.3.1。

8.3.1.2.测评实施

本项要求包括：

a) 应访谈安全管理员，询问终端操作系统采用了何种身份标识和鉴别机制；
b) 应检查终端操作系统，是否提供了身份标识和鉴别措施；
c) 应检查终端操作系统是否设置口令复杂度要求，口令是否定期进行更换，用户名和口令禁止相同。

8.3.1.3.结果判定

a) 如果 8.3.1.2. b)、c)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 8.3.1.2. b)、c)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

8.3.2 访问控制

8.3.2.1.测评指标

见 GD/J 038-2011 8.3.2。

8.3.2.2.测评实施

本项要求包括：

a) 应访谈安全管理员，是否制定了资源访问的安全策略；
b) 应检查终端的资源访问安全策略，查看是否禁止通过 USB、光驱等外设进行数据交换，是否关闭系统不必要的服务和端口等。

8.3.2.3.结果判定

a) 如果 8.3.2.2. b)为肯定，则信息系统符合本单元测评指标要求。
b) 如果 8.3.2.2. b)为否定，则信息系统不符合本单元测评指标要求。

8.3.3 安全审计

8.3.3.1.测评指标

见 GD/J 038-2011 8.3.3。

8.3.3.2.测评实施

本项要求包括：

a) 应访谈安全审计员，询问对重要终端是否进行审计，审计粒度是否为用户级；询问审计的内容有哪些；询问审计记录有哪些；询问安全审计设备是否为安全管理中心提供集中管理的接口；
b) 应检查重要终端的审计内容，是否包括重要用户行为、系统资源的异常使用和重要系统命令的使用及其它与审计相关的信息等；
c) 应检查重要终端的安全审计措施，查看审计记录是否包括：事件的日期、时间、用户名、访问对象、结果；
d) 应检查重要终端的安全审计记录，是否至少保存 90 天；
e) 应检查对事件审计记录进行分析的记录，查看是否定期对审计记录进行分析；
f) 应检查与重要终端的安全审计措施，查看其是否为安全管理中心提供集中管理的接口；
g) 应测试重要终端的安全审计措施，可通过以某个帐户登录系统，试图删除、修改或覆盖审计记录，验证安全审计的保护情况与要求是否一致；
h) 应测试重要终端操作系统可通过某个帐户试图中断审计进程，验证审计进程是否受到保护。

8.3.3.3.结果判定

a) 如果 8.3.3.2. b)-h)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 8.3.3.2. b)-e)均为肯定，f)-h)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 8.3.3.2. b)-e)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

8.3.4 入侵防范

8.3.4.1.测评指标

见 GD/J 038-2011 8.3.4。

8.3.4.2.测评实施

本**项要求包括：**

a) 应访谈安全管理员，终端操作系统的入侵防范措施有哪些；采取何种方式更新补丁；
b) 应检查终端操作系统是否遵循最小安装原则，仅安装需要的组件和应用程序；
c) **应检查终端操作系统是否利用离线更新、手工更新的方式进行操作系统补丁的更新。**

8.3.4.3.结果判定

a) 如果 8.3.4.2. b)、c)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 8.3.4.2. b)、c)中一项或多项为否定，则信息系统不符合本单元测评指标要求。
c) 本单元测评指标可根据需要进行测评。

8.3.5 恶意代码防范

8.3.5.1.测评指标

见 GD/J 038-2011 8.3.5。

8.3.5.2.测评实施

本项要求包括：

a) 应访谈安全管理员，是否部署具有统一集中管理功能的终端防恶意代码软件；
b) **应检查恶意代码库是否利用离线更新、手工更新的方式进行更新。**

8.3.5.3.结果判定

a) 如果 8.3.5.2. b)为肯定，则信息系统符合本单元测评指标要求。
b) 如果 8.3.5.2. b)为否定，则信息系统不符合本单元测评指标要求。
c) 本单元测评指标可根据需要进行测评。

8.4 服务端系统安全

8.4.1 身份鉴别

8.4.1.1.测评指标

见 GD/J 038-2011 8.4.1。

8.4.1.2.测评实施

本项要求包括：

a) 应分别访谈系统管理员和数据库管理员，询问服务器操作系统和数据库系统的防护措施有哪些，采用何种方式验证用户身份，关闭了哪些不必要的服务和端口，采取何种安全远程管理手段，是否存在共用帐号现象；
b) 应检查服务器操作系统和数据库系统，查看是否配置了对登录用户进行身份鉴别的功能，身份鉴别信息是否不易被冒用，口令是否有复杂度要求并定期更换，用户名和口令是否禁止相同；
c) 应检查服务器操作系统和数据库系，查看是否对管理用户选择两种或两种以上组合的鉴别技术来进行身份鉴别，**身份鉴别信息至少有一种不可伪造**；
d) 应检查服务器操作系统和数据库系，查看是否配置了结束会话、限制非法登录次数、远程超时自动退出等鉴别失败处理功能；
e) 应检查服务器操作系统和数据库系，查看是否采用 HTTPS、SSH 等安全的远程管理手段。

8.4.1.3.结果判定

a) 如果 8.4.1.2. b)-e)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 8.4.1.2. b)、d)均为肯定，c)、e)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 8.4.1.2. b)、d)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

8.4.2 安全标记

8.4.2.1.测评指标

见 GD/J 038-2011 8.4.2。

8.4.2.2.测评实施

本项要求包括：

a) **应访谈安全管理员、系统管理员，信息系统中有哪些接口服务器，系统边界的高风险服务器有哪些；**

b) **应检查接口服务器等系统边界的高风险服务器的主体和客体是否设置敏感标记。**

8.4.2.3.结果判定

a) 如果 8.4.2.2. b)为肯定，则信息系统符合本单元测评指标要求。

b) 如果 8.4.2.2. b)为否定，则信息系统不符合本单元测评指标要求。

c) 本单元测评可根据需要进行。

8.4.3 访问控制

8.4.3.1.测评指标

见 GD/J 038-2011 8.4.3。

8.4.3.2.测评实施

本项要求包括：

a) 应访谈安全管理员，询问服务器操作系统和数据库系统的访问控制策略有哪些，是否存在共用帐户现象；

b) 应检查服务器操作系统和数据库系统的安全策略，是否控制用户对资源的访问，是否关闭不必要的服务和端口等；

c) 应检查服务器操作系统和数据库系统的安全策略，是否根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限，特权用户权限是否分离；

d) 应检查服务器操作系统和数据库管理系统的安全策略，查看是否限制默认帐户的访问权限、windows 系统默认帐户是否重新命名、是否修改帐户的默认口令；

e) 应检查服务器操作系统和数据库系统的帐户设置情况，查看是否及时删除或禁用了系统不必要的帐户、系统过期的帐户；

f) **应检查服务器操作系统和数据库系统的安全策略，是否依据安全策略和敏感标记控制主体对客体的访问，控制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、记录和字段级。**

8.4.3.3.结果判定

a) 如果 8.4.3.2. b)-f)均为肯定，则信息系统符合本单元测评指标要求。

b) 如果 8.4.3.2. b)-e)均为肯定，f)为否定，则信息系统部分符合本单元测评指标要求。

c) 如果 8.4.3.2 b)-e)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

8.4.4 安全审计

8.4.4.1.测评指标

见 GD/J 038-2011 8.4.4。

8.4.4.2.测评实施

本项要求包括：

a) 应访谈安全审计员，询问系统安全审计范围包括哪些，审计粒度是否为用户级；询问审计的内容有哪些;询问审计记录有哪些;询问安全审计设备是否为安全管理中心提供集中管理的接口；
b) 应检查接口服务器、Web 服务器、应用服务器、数据库服务器等重要服务器的审计内容，是否包括重要用户行为、系统资源的异常使用和重要系统命令的使用及其它与审计相关的信息等；
c) 应检查接口服务器、Web 服务器、应用服务器、数据库服务器等重要服务器的安全审计记录，审计记录是否包括：事件的日期、时间、类型、用户名、客户端 IP 地址、访问对象、结果等；
d) 应检查接口服务器、Web 服务器、应用服务器、数据库服务器等重要服务器的安全审计记录，查看审计记录是否至少保存 90 天；
e) 应检查对事件审计记录进行分析的记录，查看是否定期对审计记录进行分析；
f) 应检查与接口服务器、Web 服务器、应用服务器、数据库服务器等重要服务器端的安全审计措施，查看其是否为安全管理中心提供集中管理的接口；
g) 应测试接口服务器、Web 服务器、应用服务器、数据库服务器等重要服务器，可通过某个帐户试图中断审计进程，验证审计进程是否受到保护。
h) 应测试接口服务器、Web 服务器、应用服务器、数据库服务器等重要服务器，可通过某个帐户试图删除、修改或覆盖审计记录，验证审计记录是否受到保护。

8.4.4.3.结果判定

a) 如果 8.4.4.2. b)-h)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 8.4.4.2. b)-e)均为肯定，f)、g)、h）中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 8.4.4.2. b)-e)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

8.4.5 入侵防范

8.4.5.1.测评指标

见 GD/J 038-2011 8.4.5。

8.4.5.2.测评实施

本项要求包括：

a) 应访谈安全管理员，操作系统的入侵防范措施有哪些；采取何种方式更新补丁；
b) 应检查操作系统是否遵循最小安装原则，仅安装需要的组件和应用程序，是否及时更新系统补丁；
c) **应检查服务器是否利用离线更新、手工更新的方式进行补丁更新；**
d) 应检查服务器的入侵防范措施，在发生严重入侵事件时提供报警，查看入侵事件记录中是否包括入侵的源 IP、目的 IP、攻击的类型和时间等；
e) 应检查服务器的入侵防范措施，查看其规则库是否及时更新。

8.4.5.3.结果判定

a) 如果 8.4.5.2. b)-e 均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 8.4.5.2. b)、d)均为肯定，c)、e)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 8.4.5.2. b)、d)中一项或多项为否定，则信息系统不符合本单元测评指标要求。
d) 8.4.5.2. c)可根据需要进行测评。

8.4.6 恶意代码防范

8.4.6.1.测评指标

见 GD/J 038-2011 8.4.6。

8.4.6.2.测评实施

本项要求包括：

a) 应访谈安全管理员，服务器防恶意代码软件是否统一集中管理；
b) **应检查恶意代码库是否利用离线更新、手工更新的方式进行更新。**

8.4.6.3.结果判定

a) 如果 8.4.6.2. b)为肯定，则信息系统符合本单元测评指标要求。
b) 如果 8.4.6.2. b)为否定，则信息系统不符合本单元测评指标要求。
c) 本单元测评可根据需要进行。

8.4.7 资源控制

8.4.7.1.测评指标

见 GD/J 038-2011 8.4.7。

8.4.7.2.测评实施

本项要求包括：

a) 应访谈安全管理员，资源控制相关的策略有哪些；
b) 应检查服务器，是否通过设定终端接入方式、网络地址范围等条件限制终端登录服务器；
c) 应检查能够访问服务器的终端，是否依据安全策略设置了操作超时锁定的配置；
d) 应检查服务器，是否设置了单个用户对系统资源的最大或最小使用限度的阈值。

8.4.7.3.结果判定

a) 如果 8.4.7.2. b)-d)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 8.4.7.2. b)、c)均为肯定，d)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 8.4.7.2. b)、c)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

8.4.8 冗余配置

8.4.8.1.测评指标

见 GD/J 038-2011 8.4.8。

8.4.8.2.测评实施

本项要求包括：

a) 应访谈系统管理员，询问业务服务器具有哪些冗余配置措施；
b) 应检查**业务服务器**是否具有冗余配置，并具备切换机制。

8.4.8.3.结果判定

a) 如果 8.4.8.2. b)为肯定，则信息系统符合本单元测评指标要求。
b) 如果 8.4.8.2. b)为否定，则信息系统不符合本单元测评指标要求。

8.5 应用安全

8.5.1 身份鉴别

8.5.1.1.测评指标

见 GD/J 038-2011 8.5.1。

8.5.1.2.测评实施

本项要求包括：

a) 应访谈应用系统管理员，询问应用系统登录控制措施有哪些，采用何种验证方式，是否存在共用帐号现象；
b) 应检查应用系统，查看是否具有独立的登录控制模块或者将登录控制模块集成到统一的门户认证系统中；
c) 应检查系统管理用户身份鉴别信息是否具有不易被冒用的特点，口令是否定期更换，用户名和口令禁止相同；
d) 应检查应用系统，查看其是否对管理用户和重要业务操作用户采用两种或两种以上组合的鉴别技术对其身份进行鉴别，**其中一种不可伪造**；
e) 应测试应用系统，是否提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识；
f) 应测试同一用户名连续登录失败次数超限时是否有限制，是否有结束会话机制、自动退出机制等措施。

8.5.1.3.结果判定

a) 如果 8.5.1.2. b)-f)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 8.5.1.2. c)-f)均为肯定，b)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 8.5.1.2. c)-f)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

8.5.2 安全标记

8.5.2.1.测评指标

见 GD/J 038-2011 8.5.2。

8.5.2.2.测评实施

本项要求包括：

a) **应访谈安全管理员、系统管理员，信息系统中有哪些接口服务器，系统边界的高风险服务器有哪些；**
b) **应检查接口服务器等系统边界的高风险服务器承载的业务应用的主体和客体是否设置安全标记。**

8.5.2.3.结果判定

a) 如果 8.5.2.2. b)为肯定，则信息系统符合本单元测评指标要求。
b) 如果 8.5.2.2. b)为否定，则信息系统不符合本单元测评指标要求。
c) 本单元测评可根据需要进行。

8.5.3 访问控制

8.5.3.1.测评指标

见 GD/J 038-2011 8.5.3。

8.5.3.2.测评实施

本项要求包括：

a) 应访谈系统管理员，应用系统的访问控制策略有哪些；
b) 应检查应用系统的自主访问控制功能，是否依据安全策略控制用户对资源的访问，控制粒度是否为文件、数据库表级；
c) 应检查应用系统，查看其是否删除临时帐户和测试帐户，重命名默认帐户，修改其默认口令，限制其访问权限；
d) **应检查是否通过比较安全标记来确定授予还是拒绝主体对客体的访问；**
e) 应测试应用系统，可通过以不同权限的用户登录系统，查看其拥有的权限是否与系统赋予的权限一致，验证应用系统访问控制功能是否有效；
f) 应测试应用系统，可通过以默认用户登录系统，并进行一些合法和非法操作，验证系统是否严格限制了默认帐户的访问权限；
g) 应测试应用系统，可通过以匿名用户登录系统，验证系统是否不允许匿名用户登录。

8.5.3.3.结果判定

a) 如果 8.5.2.2. b)-g)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 8.5.2.2. b)、c)、e)、g)均为肯定，d)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 8.5.2.2. b)、c)、e)、g)中一项或多项为否定，则信息系统不符合本单元测评指标要求。
d) 8.5.2.2. d)可根据需要进行测评。

8.5.4 安全审计

8.5.4.1.测评指标

见 GD/J 038-2011 8.5.4。

8.5.4.2.测评实施

本项要求包括：

a) 应访谈安全审计员，询问对应用系统是否开启审计功能，审计粒度是否为用户级；询问审计的内容有哪些；询问审计记录有哪些；询问安全审计设备是否为安全管理中心提供集中管理的接口；
b) 应检查应用系统的审计内容，是否包括审计内容应包括用户登录、修改配置、核心业务操作等重要行为，以及系统资源的异常使用等；
c) 应检查应用系统的安全审计记录，查看审计记录至少是否包括事件的日期和时间、事件类型、客户端 IP 地址、描述和结果等；
d) 应检查应用系统的安全审计记录，查看是否要求至少保存 90 天；
e) 应检查应用系统的安全审计功能，**查看审计记录是否得到存储与保护，**对审计记录数据是否提供统计、查询、分析及生成审计报表的功能；
f) 应检查与应用系统的安全审计功能，查看其是否为安全管理中心提供集中管理的接口；
g) 应测试与外部网络连接的边界处安全审计设备，可通过以某个帐户登录系统，试图删除、修改或覆盖审计记录，验证安全审计的保护情况与要求是否一致；
h) 应测试应用系统的安全审计功能，可通过某个帐户试图中断审计进程，验证审计进程是否受到保护。

8.5.4.3.结果判定

a) 如果 8.5.4.2. b)-h)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 8.5.4.2. b)-d)均为肯定，e)-h)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 8.5.4.2. b)-d)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

8.5.5 通信完整性

8.5.5.1.测评指标

见 GD/J 038-2011 8.5.5。

8.5.5.2.测评实施

本项要求包括：

a) 应访谈安全管理员，询问应用系统在数据传输过程中有哪些保护其完整性的措施；
b) 应检查设计或验收文档，查看其是否有关于保护通信完整性的说明；
c) 应测试主要应用系统，可通过获取通信双方的数据包，查看其在通信过程中是否采用校验码技术、特定的音视频文件格式、特定协议或等同强度的技术手段等进行传输。

8.5.5.3.结果判定

a) 如果 8.5.5.2. b)、c)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 8.5.5.2. b)为肯定，c)为否定，则信息系统部分符合本单元测评指标要求。

c) 如果 8.5.5.2. b)为否定，则信息系统不符合本单元测评指标要求。

8.5.6 软件容错

8.5.6.1.测评指标

见 GD/J 038-2011 8.5.6。

8.5.6.2.测评实施

本项要求包括：

a) 应访谈应用系统管理员，询问应用系统是否具有保证软件容错能力的措施，具体措施有哪些；

b) 应检查应用系统，查看应用系统是否对人机接口输入或通信接口输入的数据进行有效性检验；

c) 应测试应用系统，可通过对人机接口输入的不同长度或格式的数据，查看系统的反应，验证系统人机接口有效性检验功能是否正确，查看是否对非法输入及进行明确的错误提示并报警。

8.5.6.3.结果判定

a) 如果8.5.6.2. b)、c)均为肯定，则信息系统符合本单元测评指标要求。

b) 如果8.5.6.2. b)为肯定，c)为否定，则信息系统部分符合本单元测评指标要求。

c) 如果8.5.6.2. b)为否定，则信息系统不符合本单元测评指标要求。

8.5.7 资源控制

8.5.7.1.测评指标

见 GD/J 038-2011 8.5.7。

8.5.7.2.测评实施

本项要求包括：

a) 应访谈应用系统管理员，询问应用系统资源控制措施有哪些；
b) 应检查应用系统，查看系统是否有最大并发会话连接数的限制，是否对单个帐户的多重并发会话进行限制；
c) 应检查应用系统，查看是否对一个时间段内可能的并发会话连接数进行限制；
d) 应检查应用系统，查看是否对一个访问帐户或一个请求进程占用的资源分配最大限额和最小限额；
e) 应测试应用系统，当应用系统通信双方中的一方在一段时间内未作任何响应，查看另一方是否能够自动结束会话。

8.5.7.3.结果判定

a) 如果 8.5.7.2. b)-e)均为肯定，则信息系统符合本单元测评指标要求。

b) 如果 8.5.7.2. b)、e)均为肯定，c)、d)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。

c) 如果 8.5.7.2. b)、e)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

8.6 数据安全与备份恢复

8.6.1 数据完整性

8.6.1.1.测评指标

见 GD/J 038-2011 8.6.1。

8.6.1.2.测评实施

本项要求包括：

a) 应访谈安全管理员，询问系统管理数据、用户身份鉴别信息、调度信息、播出节目等重要业务数据在传输和存储过程中的完整性保证措施有哪些;在检测到完整性错误时,恢复措施有哪些;对信息系统的网络边界处通信协议方式有哪些;

b) 应检查应用系统，查看系统管理数据、用户身份鉴别信息、调度信息、播出节目等重要业务数据在传输和存储过程中是否具有完整性保证功能;

c) 应检查应用系统,查看重要业务数据在传输和存储过程中完整性破坏时是否采取必要的恢复措施;

d) **应检查在信息系统的网络边界处的重要通信是否采用了专用通信协议或安全通信协议。**

8.6.1.3.结果判定

a) 如果8.6.1.2. b)-d)均为肯定，则信息系统符合本单元测评指标要求。

b) 如果8.6.1.2. b)、d)均为肯定，c)为否定，则信息系统部分符合本单元测评指标要求。

c) 如果8.6.1.2. b)、d)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

8.6.2 数据保密性

8.6.2.1.测评指标

见 GD/J 038-2011 8.6.2。

8.6.2.2 测评实施

本项要求包括：

a) 应访谈网络管理员，询问网络设备的鉴别信息否采用加密或其他有效措施实现存储保密性;

b) 应访谈系统管理员，询问主机操作系统的鉴别信息否采用加密或其他有效措施实现存储保密性;

c) 应访谈数据库管理员,询问数据库管理系统的鉴别信息否采用加密或其他有效措施实现存储保密性;

d) 应访谈安全管理员，询问应用系统的鉴别信息否采用加密或其他有效措施实现存储保密性;

e) 应检查主机操作系统、网络设备操作系统、数据库管理系统和应用系统，查看其鉴别信息否采用加密或其他有效措施实现存储保密性。

8.6.2.3.结果判定

a) 如果 8.6.2.2. e)为肯定，则信息系统符合本单元测评指标要求。
b) 如果 8.6.2.2. e)为否定，则信息系统不符合本单元测评指标要求。

8.6.3 备份与恢复

8.6.3.1.测评指标

见 GD/J 038-2011 8.6.3。

8.6.3.2.测评实施

本项要求包括：

a) 应访谈网络管理员，询问是否对网络设备中的配置文件进行备份，备份策略是什么；当其受到破坏时，恢复策略是什么；是否提供主要网络设备的硬件冗余；
b) 应访谈系统管理员，询问是否对操作系统中的重要信息进行备份，备份策略是什么；当其受到破坏时，恢复策略是什么；是否提供主要服务器的硬件冗余；
c) 应访谈数据库管理员，询问是否对数据库管理系统中的数据进行备份，备份策略是什么；当其受到破坏时，恢复策略是什么；
d) 应访谈安全管理员，询问是否对应用系统中的应用程序进行备份，备份策略是什么；当其受到破坏时，恢复策略是什么；
e) **应访谈安全管理员，询问是否已建立异地灾难备份中心；**
f) **应访谈安全管理员，询问是否提供数据存储系统的硬件冗余；**
g) 应检查设计或验收文档，查看其是否有关于重要业务数据、系统配置数据本地和异地备份和恢复功能及策略的描述，完全数据备份至少每周一次，增量备份或差分备份至少每天一次，备份介质应在数据执行所在场地外存放；
h) 应检查主机操作系统、网络设备、数据库管理系统和应用系统，查看其是否提供备份和恢复功能，其配置是否正确，并且查看其备份结果是否与备份策略一致；
i) 应检查网络设备、通信线路和数据处理系统是否采用硬件冗余、软件配置等技术手段提供系统的高可用性；
j) **应检查是否建立了异地灾难备份中心，是否配备灾难恢复所需的通信线路、网络设备和数据处理设备；**
k) **应检查数据存储系统的硬件是否冗余。**

8.6.3.3.结果判定

a) 如果 8.6.3.2. g)-k)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 8.6.3.2. g)-i)、k)均为肯定，j)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 8.6.3.2. g)-i)、k)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

8.7 安全管理中心

8.7.1 运行监测

8.7.1.1.测评指标

见 GD/J 038-2011 8.7.1。

8.7.1.2.测评实施

本项要求包括：

a) 应访谈系统管理员、网络管理员、应用系统管理员、数据库管理员，询问是否具有安全运行监测措施，安全运行监测的功能和范围包括哪些；
b) 应检查安全管理中心，是否对网络及网络设备包括链路状态、核心交换机、汇聚交换机等主要设备的设备状态、设备端口状态、端口 IP、关键节点的网络流量等进行监控；
c) 应检查安全管理中心，是否监控重要服务器的各项资源指标，包括：CPU、内存、进程和磁盘等使用情况；
d) 应检查安全管理中心，是否监控数据库的运行状态、进程占用 CPU 时间及内存大小、配置和告警数据等进行监控；
e) 应检查安全管理中心，是否对重要应用软件的运行状态、响应时间等进行监控；
f) 应检查安全管理中心，是否对终端的非法接入和非法外联进行监控；
g) 应检查监控记录，查看是否记录监控对象、监控内容、监控的异常现象处理等方面。

8.7.1.3.结果判定

a) 如果 8.7.1.2. b)-g)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 8.7.1.2. b)-d)均为肯定，e)-g)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 8.7.1.2. b)-d)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

8.7.2 安全管理

8.7.2.1.测评指标

见 GD/J 038-2011 8.7.2。

8.7.2.2.测评实施

本项要求包括：

a) 应访谈安全管理员，询问是否具有安全管理措施，安全管理的功能和范围包括哪些；
b) 应检查安全管理中心，是否对信息系统的恶意代码、补丁升级等进行集中统一管理；是否对网络设备、服务器、应用系统、安全设备等的安全事件信息进行关联分析及风险预警；
c) 应检查信息系统的恶意代码、补丁升级是否集中统一管理；
d) 应检查是否具有时钟同步措施，查看是否能够对信息系统网络设备、终端、服务器以及应用等采取时钟同步措施；
e) 应检查是否能够对网络设备、服务器、应用系统、安全设备等的安全事件信息进行关联分析及风险预警。

8.7.2.3 结果判定

a) 如果 8.7.2.2. b)-e)均为肯定，则信息系统符合本单元测评指标要求。

b) 如果 8.7.2.2. b)-d)均为肯定，e)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 8.7.2.2. b)-d)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

8.7.3 审计管理

8.7.3.1.测评指标

见 GD/J 038-2011 8.7.3。

8.7.3.2.测评实施

本项要求包括：

a) 应访谈安全审计员，询问是否具有安全审计的功能和范围包括哪些；
b) 应检查安全审计措施，是否对审计记录进行统计、查询、分析及生成审计报表；
c) 应检查安全审计措施，是否对 90 天以上的审计日志进行归档，归档日志至少保存三年以上；
d) 应检查基础网络、边界安全、服务器及应用系统的安全审计是否进行集中管理。

8.7.3.3.结果判定

a) 如果 8.7.3.2. b)-d)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 8.7.3.2. b)、d)均为肯定，c)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 8.7.3.2. b)、d)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

9 第五级信息系统单元测评

（略）。

10 通用物理安全测评

10.1 物理位置的选择

10.1.1 测评指标

见 GD/J 038-2011 10.1。

10.1.2 测评实施

本项要求包括：

a) 应访谈物理安全负责人，询问现有机房和办公场地（放置终端计算机设备）的环境条件是否具有基本的防震、防风和防雨等能力；
b) 应访谈物理安全负责人，询问现有的机房位置选择是否满足《电子信息系统机房设计规范》（GB50174）的要求；
c) 应访谈机房维护人员，如果存在因机房和办公场地环境条件引发的安全事件或安全隐患，是否及时采取了补救措施；
d) 应检查机房和办公场地的设计或验收文档，查看是否有机房和办公场地所在建筑能够具有防震、防风和防雨等能力的说明；查看是否有机房场地的选址说明；

e) 应检查机房和办公场地所在建筑是否具有防震、防风和防雨等能力；
f) 应检查机房场地是否不在建筑物的高层或地下室，不在用水设备的下层或隔壁；
g) 应检查机房场地是否远离产生粉尘、油烟、有害气体以及生产或贮存具有腐蚀性、易燃、易爆物品的工厂、仓库、堆场等。

10.1.3 结果判定

a) 如果 10.1.2. c)中“如果”条件不成立，则该项为不适用。
b) 如果 10.1.2. b)-g)均为肯定，则信息系统符合本单元测评指标要求。
c) 如果 10.1.2. b)-c)、e)-g)均为肯定，d)为否定，则信息系统部分符合本单元测评指标要求。
d) 如果 10.1.2. b)-c)、e)-g)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

10.2 物理访问控制

10.2.1 测评指标

见 GD/J 038-2011 10.2。

10.2.2 测评实施

本项要求包括：

a) 应访谈物理安全负责人，询问机房物理访问控制措施有哪些；
b) 应检查机房出入口是否配置电子门禁系统，是否有验收文档或产品安全认证资质；
c) 应检查电子门禁系统是否正常工作（不考虑断电后的工作情况）；查看是否有电子门禁系统运行和维护记录；查看监控进入机房的电子门禁系统记录，是否能够鉴别和记录进入人员的身份；
d) 应检查机房安全管理制度，查看是否有关于机房出入方面的规定；
e) 如果本单位具有第四级信息系统的机房，应检查机房出入口是否有专人值守；
f) 应检查是否有来访人员进入播出机房的审批记录，查看审批记录是否包括来访人员的活动范围。

10.2.3 结果判定

a) 如果10.2.2. e)中“如果”条件不成立，则该项为不适用。

b) 如果10.2.2. b)-f)均为肯定，则信息系统符合本单元测评指标要求。

c) 如果10.2.2. b)-f)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

10.3 防盗窃和防破坏

10.3.1 测评指标

见 GD/J 038-2011 10.3。

10.3.2 测评实施

本项要求包括：

a) 应访谈物理安全负责人，询问采取了哪些防止设备、介质等丢失与破坏的保护措施；

b) 应访谈机房维护人员，询问设备或主要部件放置位置是否做到安全可控，设备或主要部件是否进行了固定和标记，公共区域信号线缆是否铺设在隐蔽处；是否对机房防盗报警系统和监控报警系统定期检查维护；
c) 应检查设备或主要部件是否放置在机房或其它不易被盗窃和破坏的可控范围内；检查设备或主要部件的固定情况，查看其是否不易被移动或被搬走，是否设置明显的不易除去的标记；
d) 应检查公共区域信号线缆铺设是否在隐蔽处；
e) 应检查是否已安装利用光、电等技术的机房防盗报警系统，机房防盗报警设施是否正常运行，查看是否有运行和报警记录；
f) 应检查与播出相关机房的摄像、传感等安防监控报警系统是否正常运行，查看是否有运行记录、监控记录和报警记录；
g) 应检查是否有机房防盗报警设施和安防监控报警设施的安全资质材料、安装测试和验收报告。

10.3.3 结果判定

a) 如果 10.3.2. c)-g)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 10.3.2. c)-d)、f)均为肯定，e)、g)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 10.3.2. c)-d)、f)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

10.4 机房环境

10.4.1 测评指标

见 GD/J 038-2011 10.4。

10.4.2 测评实施

本项要求包括：

a) 应访谈物理安全负责人，询问机房环境的保护措施有哪些；
b) 应检查机房环境的温湿度、防尘、防静电、电磁防护、接地、布线等是否按照国标《电子信息系统机房设计规范》（GB 50174）的有关规定执行；
c) 应检查机房的窗户、屋顶和墙壁等是否无漏水、渗透和返潮现象，机房及其环境是否不存在明显的漏水和返潮的威胁；
d) 应检查机房的窗户、屋顶和墙壁，如果出现漏水、渗透和返潮现象，则查看是否及时修复解决；
e) 应检查穿过主机房墙壁或楼板的管道是否采取必要的防渗防漏等防水保护措施；
f) 如果在湿度较高的地区，应检查机房是否有湿度记录，是否有除湿装置并能够正常运行，是否有防止出现机房地下积水的转移与渗透的措施，是否有防水防潮处理记录和除湿装置运行记录；
g) 如果本单位具有第四级信息系统，则应检查是否设置对水敏感的检测仪表或元件，对机房进行防水检测和报警，查看该仪表或元件是否正常运行，是否有运行记录，是否有人负责其运行管理工作；
h) 应检查温湿度自动调节设施是否能够正常运行，查看是否有温湿度记录、运行记录和维护记录；查看机房温湿度是否满足计算站场地的技术条件要求；
i) 应检查主要设备是否采用安全接地方式，防止外界电磁干扰和设备寄生耦合干扰；
j) 应检查机房布线，查看是否做到电源线和通信线缆隔离。

10.4.3 结果判定

a) 如果 10.4.2. d)、f)、g)中“如果”条件不成立，则该项为不适用。
b) 如果 10.4.2. b)-j)均为肯定，则信息系统符合本单元测评指标要求。
c) 如果 10.4.2. b)-i)均为肯定，j)为否定，则信息系统部分符合本单元测评指标要求。
d) 如果 10.4.2. b)-i)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

10.5 机房消防设施

10.5.1 测评指标

见 GD/J 038-2011 10.5。

10.5.2 测评实施

本项要求包括：

a) 应访谈物理安全负责人，询问机房消防设施有哪些，是否符合《广播电视建筑设计防火规范》（GY5067）的有关规定；
b) 应检查相关文档，是否有消防部门验收记录；
c) 应检查机房是否设置了自动检测火情、自动报警、自动灭火的自动消防系统，自动消防系统摆放位置是否合理，其有效期是否合格；
d) 应检查自动消防系统是否正常工作，查看是否有运行记录、报警记录、定期检查和维修记录；
e) 应检查机房及相关的工作房间和辅助房是否采用具有耐火等级的建筑材料；
f) 应检查机房是否采取区域隔离防火措施，将重要设备与其他设备隔离开。

10.5.3 结果判定

a) 如果 10.5.2. b)-f)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 10.5.2. b)-e)均为肯定，f)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 10.5.2. b)-e)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

10.6 电力供应

10.6.1 测评指标

见 GD/J 038-2011 10.6。

10.6.2 测评实施

本项要求包括：

a) 应检查机房的配电是否符合“广播电视安全播出管理规定实施细则”的相关要求。

10.6.3 结果判定

a) 如果 10.6.2. a)为肯定，则信息系统符合本单元测评指标要求。
b) 如果 10.6.2. a)为否定，则信息系统不符合本单元测评指标要求。

11 通用管理安全测评

11.1 安全管理总体要求

11.1.1 测评指标

见 GD/J 038-2011 11.1。

11.1.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问制定了哪些信息安全管理制度和操作规程；
b) 应检查信息安全工作的总体方针和安全策略文件，查看文件是否明确安全工作的总体目标、范围、原则和安全框架等；
c) 应检查部门、岗位职责文件，查看文件是否明确成立指导和管理信息安全工作的领导小组，是否设立信息安全管理工作的职能部门；
d) 应检查各项安全管理制度和操作规程，查看是否明确信息安全管理各项要求，是否形成由安全方针、管理制度、细化流程等构成的全面的信息安全管理制度体系。

11.1.3 结果判定

a) 如果 11.1.2. b)-d)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 11.1.2. b)-d)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

11.2 安全管理机构

11.2.1 岗位设置

11.2.1.1.测评指标

见 GD/J 038-2011 11.2.1。

11.2.1.2.测评实施

本项要求包括：

a) 应访谈安全主管，询问信息安全组织机构设立情况，信息安全管理职能部门设置情况；
b) 应检查信息安全管理委员会或领导小组最高领导是否具有委任授权书，查看授权书中是否有本单位主管领导的授权签字；
c) 应检查信息安全管理工作的职能部门和岗位职责文件，查看文件是否明确信息安全各项工作组织和落实，是否配置专职的安全管理员；
d) 如果本单位具有第三级及以上信息系统，则应检查岗位职责文件，查看是否设立系统管理员、网络管理员、安全管理员等岗位，是否明确各个工作岗位的职责、分工和技能要求。

11.2.1.3.结果判定

a) 如果 11.2.1.2. d)中“如果”条件不成立，则该项为不适用。
b) 如果 11.2.1.2. b)-d)均为肯定，则信息系统符合本单元测评指标要求。
c) 如果 11.2.1.2. b)-d)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

11.2.2 授权和审批

11.2.2.1.测评指标

见 GD/J 038-2011 11.2.2。

11.2.2.2.测评实施

本项要求包括：

a) 应访谈安全主管，询问其是否规定对信息系统中的关键活动进行审批，审批部门是何部门，批准人是何人，他们的审批活动是否得到授权；询问是否定期审查、更新审批项目，审查周期多长；
b) 应访谈安全主管，询问其对关键活动的审批范围包括哪些，审批程序如何；
c) 应检查审批管理制度文档，查看文档中是否明确审批事项、需逐级审批的事项、审批部门、批准人及审批程序等，是否明确对系统变更、重要操作、物理访问和系统接入等事项的审批流程；是否明确需定期审查、更新审批的项目、审批部门、批准人和审查周期等；
d) 应检查经逐级审批的文档，查看是否具有各级批准人的签字和审批部门的盖章；
e) 应检查关键活动的审批过程记录，查看记录的审批程序与文件要求是否一致。

11.2.2.3.结果判定

a) 如果11.2.2.2. b)-e)均为肯定，则信息系统符合本单元测评指标要求。

b) 如果11.2.2.2. b)-e)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

11.2.3 沟通和合作

11.2.3.1.测评指标

见 GD/J 038-2011 11.2.3。

11.2.3.2.测评实施

本项要求包括：

a) 应访谈安全主管，询问是否建立与系统内外相关工作单位的沟通、合作机制，与系统内外相关工作单位和其他部门有哪些合作内容，沟通、合作方式有哪些；与组织机构内其它部门之间及内部各部门管理人员之间是否建立沟通、合作机制，是否定期或不定期召开协调会议；
b) 如果本单位具有第三级及以上信息系统，则应访谈安全主管，询问是否聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等；
c) 应检查组织内部机构之间以及信息安全职能部门内部的安全工作会议文件或会议记录，查看是否有会议内容、会议时间、参加人员和会议结果等的描述；
d) 应检查与系统内外相关工作单位的安全工作会议文件或会议记录，查看是否有会议内容、会议时间、参加人员和会议结果等的描述；
e) 应检查是否有组织机构内部人员联系表；
f) 如果本单位具有第三级及以上信息系统，应检查是否具有安全顾问名单或者聘请安全顾问的证明文件，查看是否有安全顾问指导信息安全建设、参与安全规划和安全评审的相关文档或记录。

11.2.3.3.结果判定

a) 如果 11.2.3.2. b)、f）中“如果”条件不成立，则该项为不适用。
b) 如果 11.2.3.2. b)-f)均为肯定，则信息系统符合本单元测评指标要求。
c) 如果 11.2.3.2. b)-d)、f)均为肯定，e)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
d) 如果 11.2.3.2. b)-d)、f)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

11.2.4 审核和检查

11.2.4.1.测评指标

见 GD/J 038-2011 11.2.4。

11.2.4.2.测评实施

本项要求包括：

a) 应访谈安全主管，询问是否组织人员定期对信息系统进行全面安全检查，检查周期多长，检查内容有哪些；
b) 应访谈安全管理员，询问是否定期检查系统日常运行、系统漏洞和数据备份等情况，检查周期多长；询问系统全面安全检查情况，检查周期多长，检查人员有哪些，检查程序如何，是否对检查结果进行通报，通报形式、范围如何；
c) 应检查安全检查管理制度文档，查看文档是否规定定期进行全面安全检查，是否规定检查内容、检查程序和检查周期等，检查内容是否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；
d) 应检查全面安全检查报告，查看报告日期间隔与检查周期是否一致，报告中是否有检查内容、检查人员、检查数据汇总，是否对检查结果进行通报；
e) 应检查安全管理员定期实施安全检查的报告，查看报告日期间隔与检查周期是否一致，检查内容是否包括系统日常运行、系统漏洞和数据备份等情况。

11.2.4.3.结果判定

a) 如果 11.2.4.2. c)-e)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 11.2.4.2. c)-e)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

11.2.5 制度管理

11.2.5.1.测评指标

见 GD/J 038-2011 11.2.5。

11.2.5.2.测评实施

本项要求包括：

a) 应访谈安全主管，询问信息安全管理制度和操作规程的覆盖范围，管理制度版本的控制情况、评审修订情况以及发布情况；
b) 应检查各项安全管理制度，查看是否覆盖访问控制、系统设计、系统建设、系统验收、系统运维、应急处置、人员管理、文件档案管理、审核检查等方面规范各项信息安全管理工作；
c) 应检查管理制度评审记录，查看是否有专家或相关部门人员的评审意见；

d) 应检查各项安全管理制度文档，查看文档是否是正式发布的文档，是否注明适用和发布范围，是否有版本标识，是否有管理层的签字或单位盖章；查看各项制度文档格式是否统一；
e) 应检查安全管理制度的收发登记记录，查看收发是否通过正式、有效的方式（如正式发文、领导签署和单位盖章等），是否有发布范围要求。

11.2.5.3.结果判定

a) 如果 11.2.5.2. b)-e)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 11.2.5.2. b)-d)均为肯定，e)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 11.2.5.2. b)-d)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

11.3 人员安全管理

11.3.1 人员上岗

11.3.1.1.测评指标

见 GD/J 038-2011 11.3.1。

11.3.1.2.测评实施

本项要求包括：

a) 应访谈人事管理相关人员,询问在人员录用时对人员条件有哪些要求,是否对被录用人的身份、背景、专业资格和资质进行审查，对技术人员的技术技能进行考核，是否与被录用人员都签署保密协议；
b) 应检查人员录用要求管理文档，查看是否说明录用人员应具备的条件（如学历、学位要求，技术人员应具备的专业技术水平，管理人员应具备的安全管理知识等）；
c) 应检查是否具有人员录用时对录用人身份、背景、专业资格和资质等进行审查的相关文档或记录，查看是否记录审查内容和审查结果等；
d) 应检查人员录用时的技能考核文档或记录，查看是否记录考核内容和考核结果等；
e) 应检查保密协议，查看是否有保密范围、保密责任、违约责任、协议的有效期限和责任人的签字等内容；
f) 应检查岗位安全协议，查看是否有岗位安全责任、违约责任、协议的有效期限和责任人签字等内容。

11.3.1.3.结果判定

a) 如果 11.3.1.2. b)-f)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 11.3.1.2. b)-e)均为肯定，f)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 11.3.1.2. b)-e)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

11.3.2 人员离岗

11.3.2.1.测评指标

见 GD/J 038-2011 11.3.2。

11.3.2.2.测评实施

本项要求包括：

a) 应访谈安全主管，询问对即将离岗人员有哪些控制方法，是否及时终止离岗人员的所有访问权限，是否收回各种内部身份证件、钥匙、徽章以及机构提供的软硬件设备等；
b) 应访谈人事管理相关人员，询问调离手续包括哪些，是否要求所有人员调离时须承诺相关保密义务后方可离开，对于某些关键岗位人员调离是否采取更加严格的处理措施，如重新评估确定其调离后可能存在的安全风险，保密承诺要求更加严格等；
c) 应检查人员离岗的管理制度文档，查看是否说明人员离岗要求、人员离岗控制程序、人员调离手续等相关内容；
d) 应检查是否具有对离岗人员的安全处理记录（如交还内部身份证件、设备等的登记记录）；
e) 应检查是否具有按照离职程序办理调离手续的记录，查看调离手续与文件规定是否一致；
f) 应检查保密承诺文档，查看是否有调离人员的签字。

11.3.2.3.结果判定

a) 如果 11.3.2.2. c)-f)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 11.3.2.2. c)、f)均为肯定，d)、e)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 11.3.2.2. c)、f)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

11.3.3 培训与考核

11.3.3.1.测评指标

见 GD/J 038-2011 11.3.3。

11.3.3.2.测评实施

本项要求包括：

a) 应访谈安全主管，询问是否制定培训计划并按计划定期对各个岗位人员进行安全教育和培训，具体的培训方式有哪些;询问是否有人负责定期对各个岗位人员进行安全技能及安全知识的考核；
b) 应访谈人事管理相关人员，询问对各个岗位人员的考核情况，考核周期多长，考核内容有哪些；
c) 应检查是否具有安全教育和培训记录，查看记录是否有培训人员、培训内容、培训结果等的描述；查看培训内容是否包含安全意识教育、岗位技能培训和相关安全政策、技术培训；
d) 应检查考核文档和记录，查看记录的考核人员是否包括各个岗位的人员，考核内容是否包含安全技能、政策及安全认知。

11.3.3.3.结果判定

a) 如果 11.3.3.2. c)、d)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 11.3.3.2. c)为肯定，d)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 11.3.3.2. c)为否定，则信息系统不符合本单元测评指标要求。

11.3.4 外部人员访问管理

11.3.4.1.测评指标

见 GD/J 038-2011 11.3.4。

11.3.4.2.测评实施

本项要求包括：

a) 应访谈安全管理员，询问对外部人员访问重要区域（如访问机房、重要服务器或设备区、保密文档存放区等）采取了哪些安全措施，是否经有关部门或负责人批准，是否由专人全程陪同或监督，是否进行记录并备案管理；
b) 应检查外部人员访问管理文档，查看是否明确外部人员包括哪些人员，允许外部人员访问的范围（区域、系统、设备、信息等内容），外部人员进入的条件（对哪些重要区域的访问须提出书面申请批准后方可进入，对哪些关键区域不允许外部人员访问等），外部人员进入的访问控制措施（由专人全程陪同或监督等）和外部人员离开的条件等；
c) 应检查外部人员访问重要区域的批准文档，是否有批准人允许访问的批准签字等；
d) 应检查外部人员访问重要区域的登记记录，查看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、访问设备或信息及陪同人等信息。

11.3.4.3.结果判定

a) 如果 11.3.4.2. b)-d)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 11.3.4.2. b、c)均为肯定，d)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 11.3.4.2. b)、c)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

11.4 系统建设管理

11.4.1 系统定级

11.4.1.1.测评指标

见 GD/J 038-2011 11.4.1。

11.4.1.2.测评实施

本项要求包括：

a) 应访谈安全主管，询问信息系统的定级评审、审批、报备情况；
b) 应检查系统定级文档，查看是否按照国家和行业标准、规范确定信息系统的边界和安全保护等级；查看是否说明定级的方法和理由，查看定级结果是否有相关部门的批准盖章；
c) 应检查定级评审文档，查看是否有对定级评审结果的论证意见。

11.4.1.3.结果判定

a) 如果 11.4.1.2. b)、c)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 11.4.1.2. b)为肯定，c)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 11.4.1.2. b)为否定，则信息系统不符合本单元测评指标要求。

11.4.2 安全方案设计

11.4.2.1.测评指标

见 GD/J 038-2011 11.4.2。

11.4.2.2.测评实施

本项要求包括：

a) 应访谈安全主管，询问是否授权专门的部门对信息系统的安全建设进行总体规划，由何部门负责；
b) 应访谈系统建设负责人，询问是否根据信息系统的等级划分情况统一考虑总体安全策略、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，是否经过论证和审定，是否经过审批，是否根据等级测评、安全评估的结果调整和修订，维护周期多长；
c) 应检查系统总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案、近期安全建设计划和远期安全建设计划等配套文件，查看各个文件是否有机构管理层的批准；
d) 应检查专家论证文档，查看是否有相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的论证意见；
e) 应检查是否具有依据等级测评、安全评估的结果调整和修订信息安全的规划、建设方案等相关配套文件的维护记录或修订版本。

11.4.2.3.结果判定

a) 如果 11.4.2.2. c)-e)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 11.4.2.2. c)、d)均为肯定，e)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 11.4.2.2. c)、d)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

11.4.3 产品采购和使用

11.4.3.1.测评指标

见 GD/J 038-2011 11.4.3。

11.4.3.2.测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问信息安全产品的采购情况，采购产品前是否预先对产品进行选型测试确定产品的候选范围，是否有产品采购清单指导产品采购，采购过程如何控制；
b) 应访谈系统建设负责人，询问系统是否采用了密码产品，密码产品的采购和使用是否符合国家密码主管部门的要求；
c) 应检查产品采购管理文档，查看内容是否明确需要的产品性能指标，确定产品的候选范围，通过招投标等方式确定采购产品；
d) 应检查系统使用的有关信息安全产品是否符合国家的有关规定；
e) 应检查密码产品的使用情况是否符合国家密码主管部门的要求；
f) 应检查是否具有产品选型测试结果记录、候选产品名单审定记录。

11.4.3.3.结果判定

a) 如果 11.4.3.2. c)-f)均为肯定，则信息系统符合本单元测评指标要求。

b) 如果 11.4.3.2. c)-e)均为肯定，f)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 11.4.3.2. c)-e)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

11.4.4 自行软件开发

11.4.4.1.测评指标

见 GD/J 038-2011 11.4.4。

11.4.4.2.测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问是否进行自主开发软件，是否对程序资源库的修改、更新、发布进行授权和批准，授权部门是何部门，批准人是何人，是否要求开发人员不能做测试人员，自主开发软件是否在独立的模拟环境中编写、调试和完成；
b) 应访谈系统建设负责人，询问软件设计相关文档和使用指南是否由专人负责保管，负责人是何人，如何控制使用，测试数据和测试结果是否受到控制；
c) 应访谈软件开发人员，询问其是否参照代码编写安全规范进行软件开发，开发之后是否交给测试人员测试软件，是否审查软件中可能存在的后门漏洞等；
d) 应检查开发环境与实际运行环境是否物理分开；
e) 应检查软件开发管理制度，查看文件是否明确软件设计、开发、测试、验收过程的控制方法和人员行为准则，是否明确哪些开发活动应经过授权、审批，是否明确软件开发相关文档的管理等；
f) 应检查代码编写安全规范，查看规范中是否明确代码编写规则；
g) 应检查代码安全审计报告，查看是否对软件代码中的后门漏洞进行安全审查；
h) 应检查是否具有软件设计的相关文档、软件使用指南或操作手册和维护手册等；
i) 应检查对程序资源库的修改、更新、发布进行授权和审批的文档或记录，查看是否有批准人的签字；
j) 应检查是否具有软件开发相关文档的使用控制记录。

11.4.4.3.结果判定

a) 如果 11.4.4.2. d)-j)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 11.4.4.2. d)-f)、h)-j)均为肯定，g)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 11.4.4.2. d)-f)、h)-j)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

11.4.5 外包软件开发

11.4.5.1.测评指标

见 GD/J 038-2011 11.4.5。

11.4.5.2.测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问软件交付前是否依据国家、行业相关标准和开发需求的技术指标对软件功能和性能等进行验收测试，软件安装之前是否检测软件中的恶意代码，检测工具是否是第三方的商业产品；是否要求开发单位提供源代码，是否根据源代码对软件中可能存在的后门漏洞进行审查；
b) 应检查是否具有需求分析说明书、软件设计说明书、软件操作手册、软件源代码文档等软件开发文档和使用指南；
c) 应检查软件源代码审查记录，查看是否包括对可能存在后门漏洞等的审查结果。

11.4.5.3.结果判定

a) 如果 11.4.5.2. b)、c)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 11.4.5.2. b)、c)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

11.4.6 工程实施

11.4.6.1.测评指标

见 GD/J 038-2011 11.4.6。

11.4.6.2.测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问是否有专门部门或人员负责工程实施管理工作，由何部门/何人负责，是否按照工程实施方案的要求对工程实施过程进行进度和质量控制，是否要求工程实施单位提供其能够安全实施系统建设的资质证明和能力保证；
b) 应检查工程实施方案，查看其是否包括工程时间限制、进度控制和质量控制等方面内容；
c) 应检查是否具有按照实施方案形成的阶段性工程报告等文档；
d) 应检查工程实施管理制度，查看其是否包括工程实施过程的控制方法、实施参与人员的行为准则等方面内容。

11.4.6.3.结果判定

a) 如果 11.4.6.2. b)-d)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 11.4.6.2. b)为肯定，c)、d)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 11.4.6.2. b)为否定，则信息系统不符合本单元测评指标要求。

11.4.7 测试验收

11.4.7.1.测评指标

见 GD/J 038-2011 11.4.7。

11.4.7.2.测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问是否有专门的部门负责测试验收工作，由何部门负责；是否委托广播电视信息安全测评中心对信息系统进行独立的安全性测试；

b) 应访谈系统建设负责人，询问是否根据设计方案或合同要求组织相关部门和人员对系统测试验收报告进行审定；
c) 应检查工程测试验收方案，查看其是否明确说明参与测试的部门、人员、测试验收的内容、现场操作过程等内容；
d) 应检查测试验收记录是否详细记录了测试时间、人员、现场操作过程和测试验收结果等方面内容；
e) 应检查是否具有系统安全性测试报告，查看报告是否给出测试通过的结论，是否具有广播电视信息安全测评中心的签字或盖章；
f) 应检查是否具有系统测试验收报告，是否具有对测试验收报告的审定文档，查看文档是否相关人员的审定意见；
g) 应检查测试验收管理文档是否包括系统测试验收的过程控制方法、参与人员的行为规范等内容。

11.4.7.3.结果判定

a) 如果 11.4.7.2. c)-g)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 11.4.7.2. c)-e)均为肯定，f)、g)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 11.4.7.2. c)-e)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

11.4.8 系统交付

11.4.8.1.测评指标

见 GD/J 038-2011 11.4.8。

11.4.8.2.测评实施

本项要求包括：

a) 如果信息系统是由内部人员独立运行维护，应访谈系统建设负责人，系统运行前是否对运行维护人员进行过培训；
b) 应检查是否具有系统交付清单分类详细列项系统交付的各类设备、软件、文档等；
c) 应检查是否具有系统建设文档、指导用户进行系统运维的文档、系统培训手册等；
d) 应检查培训记录，查看是否包括培训内容、培训时间和参与人员等。

11.4.8.3.结果判定

a) 如果 11.4.8.2. a)中“如果”条件不成立，则该项为不适用。
b) 如果 11.4.8.2. b)-d)均为肯定，则信息系统符合本单元测评指标要求。
c) 如果 11.4.8.2. b)-d)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

11.4.9 系统备案

11.4.9.1.测评指标

见 GD/J 038-2011 11.4.9。

11.4.9.2.测评实施

本项要求包括：

a) 应访谈安全主管，询问是否有专门的部门或人员负责管理系统定级的相关文档，由何部门/何人负责；
b) 应访谈文档管理员，询问对系统定级相关备案文档是否采取控制措施；
c) 应检查是否具有将系统等级相关材料报主管部门备案的记录或备案文档；
d) 应检查是否具有将系统等级相关备案材料报相应公安机关备案的记录或证明；
e) 应检查是否具有系统定级相关材料的使用控制记录。

11.4.9.3.结果判定

a) 如果 11.4.9.2. c)-e)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 11.4.9.2. c)、d)为肯定， e)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 11.4.9.2. c)、d)为否定，则信息系统不符合本单元测评指标要求。

11.4.10 11.4.10.等级测评

11.4.10.1.测评指标

见 GD/J 038-2011 11.4.10。

11.4.10.2.测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问信息系统运行过程中，是否按照国家和行业标准、规范要求对系统进行等级测评；
b) 应检查是否具有广播电视信息安全测评中心出具的测评报告。
c) 应检查等级测评报告、系统整改方案或验收文档，查看是否对不符合相应等级保护标准要求的地方及时进行整改；
d) 应检查等级测评报告、系统变更报告或记录，查看是否在系统变更时进行等级测评，对不符合相应等级保护标准要求的地方及时整改；

11.4.10.3.结果判定

a) 如果 11.4.10.2. b)-d)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 11.4.10.2. b)-d)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

11.4.11 安全服务商选择

11.4.11.1.测评指标

见 GD/J 038-2011 11.4.11。

11.4.11.2.测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问信息系统选择的安全服务商有哪些，是否符合国家和行业有关规定；

b) 应检查是否具有与安全服务商签订的安全责任合同书或保密协议等文档，查看其内容是否包含保密范围、安全责任、违约责任、协议的有效期限和责任人的签字等；
c) 应检查是否具有与安全服务商签订的服务合同，查看是否包括服务内容、服务期限、双方签字或盖章等。

11.4.11.3.结果判定

a) 如果 11.4.11.2. b)、c)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 11.4.11.2. b)、c)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

11.5 系统运维管理

11.5.1 环境管理

11.5.1.1.测评指标

见 GD/J 038-2011 11.5.1。

11.5.1.2.测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否有专门的部门或人员对机房基础设施进行定期维护，由何部门或何人负责，维护周期多长，是否有专门的部门负责机房环境安全管理工作；
b) 应检查机房安全管理制度，查看其内容是否覆盖机房物理访问、物品带进和带出机房、机房环境安全和工作人员行为等方面；
c) 应检查机房基础设施维护记录，查看是否记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容。

11.5.1.3.结果判定

a) 如果 11.5.1.2. b)、c)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 11.5.1.2. b)、c)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

11.5.2 资产管理

11.5.2.1.测评指标

见 GD/J 038-2011 11.5.2。

11.5.2.2.测评实施

本项要求包括：

a) 应访谈安全主管，询问是否有资产管理的责任人员或部门，由何部门/何人负责；
b) 应访谈资产管理员，询问是否依据资产的重要程度对资产进行分类和标识管理，不同类别的资产是否采取不同的管理措施；
c) 应检查资产清单，查看其内容是否覆盖资产责任部门、责任人、所处位置和重要程度等方面；
d) 应检查资产安全管理制度，查看其是否明确信息资产管理的责任部门、责任人，查看其内容是否覆盖资产使用、传输、存储、维护等方面；

e) 应检查信息分类文档，查看其内容是否明确了信息分类标识的原则和方法。

11.5.2.3.结果判定

a) 如果 11.5.2.2. c)-e)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 11.5.2.2. c)、d)均为肯定，e)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 11.5.2.2. c)、d)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

11.5.3 介质管理

11.5.3.1.测评指标

见 GD/J 038-2011 11.5.3。

11.5.3.2.测评实施

本项要求包括：

a) 应访谈资产管理员，询问介质的存放环境是否采取保护措施防止被盗、被毁、介质内存储信息被未授权修改以及非法泄露等;是否根据所承载数据和软件的重要程度对介质进行分类和标识管理，进行了哪些相应的控制和保护；
b) 应访谈资产管理员，询问介质带出工作环境是否经过批准，对经批准带出工作环境的存储介质是否进行登记和监控管理；对保密性较高的介质销毁前是否有领导批准，对送出维修或销毁的介质在送出之前是否对介质内存储数据进行净化处理；
c) 应访谈资产管理员，询问是否对某些重要介质实行异地存储，异地存储环境是否与本地环境相同；
d) 应检查介质管理制度，查看其内容是否覆盖介质的存放环境、使用、维护和销毁等方面；
e) 应检查介质管理记录，查看其是否记录介质的存储、归档、送出维修及销毁等情况；
f) 应检查介质，查看是否对其进行了分类，并具有不同标识。

11.5.3.3.结果判定

a) 如果 11.5.3.2. d)-f)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 11.5.3.2. d)、e)均为肯定，f)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 11.5.3.2. d)、e)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

11.5.4 设备管理

11.5.4.1.测评指标

见 GD/J 038-2011 11.5.4。

11.5.4.2.测评实施

本项要求包括：

a) 应访谈资产管理员，询问是否对各种设备、线路进行定期维护，对各类测试工具进行有效性检查，由何部门/何人负责，维护周期多长；
b) 应访谈资产管理员，询问是否对设备选用的各个环节（选型、采购、发放和领用、涉外维修和服务及信息处理设备带离机构等）进行审批控制；

c) 应访谈安全审计员，询问对主要设备（包括备份和冗余设备）的操作是否建立日志，日志文件如何管理，是否定期检查管理情况；
d) 应检查设备安全管理制度，查看其内容是否明确对各种软硬件设备的选型、采购、发放和领用以及带离机构等环节进行申报和审批；
e) 应检查配套设施、软硬件维护方面的管理制度，查看其是否对配套设施、软硬件维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制管理等；
f) 应检查设备使用管理文档，查看其内容是否覆盖终端计算机、便携机和网络设备等使用、操作原则、注意事项等方面；
g) 应检查主要设备（包括备份和冗余设备）的操作规程，查看其内容是否覆盖服务器如何启动、停止、加电、断电等操作；
h) 应检查是否具有设备的选型、采购、发放和领用以及带离机构等的申报材料和审批报告；
i) 应检查是否具有设备维护记录和主要设备的操作日志。

11.5.4.3.结果判定

a) 如果 11.5.4.2. d)-i)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 11.5.4.2. d)-g)、i)均为肯定， h)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 11.5.4.2. d)-g)、i)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

11.5.5 网络安全管理

11.5.5.1.测评指标

见 GD/J 038-2011 11.5.5。

11.5.5.2.测评实施

本项要求包括：

a) 应访谈安全主管，询问是否指定专人负责维护网络运行日志、监控记录和分析处理报警信息等网络安全管理工作；网络的外联种类有哪些，是否都得到授权与批准，由何部门或何人批准；
b) 应访谈网络管理员，询问是否根据厂家提供的软件升级版本对网络设备进行过升级，目前的版本号为多少，升级前是否对重要文件（帐户数据、设备配置文件等）进行备份，采取什么方式；
c) 应访谈网络管理员，询问是否实现网络设备的最小服务配置，对配置文件是否进行定期离线备份，采取什么方式；是否定期检查非法接入和非法外联等违反网络安全策略的行为；
d) 应访谈安全管理员，询问是否定期对网络设备进行漏洞扫描，扫描周期多长，发现漏洞是否及时修补；
e) 应检查网络漏洞扫描报告，查看其内容是否包含网络存在的漏洞、严重级别和结果处理等方面，检查扫描时间间隔与扫描周期是否一致；
f) 应检查网络安全管理制度，查看其是否覆盖网络安全配置、安全策略、升级与打补丁、最小服
g) 务、授权访问、日志保存时间、口令更新周期、文件备份等方面内容；
h) 如果内部网络外联，应检查是否具有内部网络外联的授权批准书；
i) 应检查是否具有网络审计日志，检查日志是否在规定的保存时间范围内。

11.5.5.3.结果判定

a) 如果 11.5.5.2. g)中“如果”条件不成立，则该项为不适用。

b) 如果 11.5.5.2. e)-h)均为肯定，则信息系统符合本单元测评指标要求。
c) 如果 11.5.5.2. f)-h)均为肯定，e)为否定，则信息系统部分符合本单元测评指标要求。
d) 如果 11.5.5.2. f)-h)中一项或多项为否定，则信息系统不符合本单元测评指标要求。
e) 11.5.5.2 d）、e)对于播出直接相关的信息网络可根据需要进行测评。

11.5.6 系统安全管理

11.5.6.1.测评指标

见 GD/J 038-2011 11.5.6。

11.5.6.2.测评实施

本项要求包括：

a) 应访谈安全主管，询问是否指定专人对系统进行管理，对系统管理员用户是否进行分类，明确各个角色的权限、责任和风险，权限设定是否遵循最小授权原则；
b) 应访谈系统管理员，询问是否根据业务需求和系统安全分析制定系统的访问控制策略，控制分配信息系统、文件及服务的访问权限；
c) 应访谈系统管理员，询问是否定期对系统安装安全补丁程序，在安装系统补丁前是否对重要文件进行备份，采取什么方式进行，是否先在测试环境中测试通过再安装，播出直接相关的信息系统可根据需要有选择性地进行；
d) 应访谈安全管理员，询问是否定期对系统进行漏洞扫描，扫描周期多长，发现漏洞是否及时修补；
e) 应检查系统安全管理制度，查看其内容是否覆盖系统安全策略、安全配置、日志管理、日常操作流程等具体内容；
f) 应检查是否有详细操作日志(包括重要的日常操作、运行维护记录、参数的设置和修改等内容)；
g) 应检查是否有定期对运行日志和审计结果进行分析的分析报告，查看报告是否能够记录帐户的连续多次登录失败、非工作时间的登录、访问受限系统或文件的失败尝试、系统错误等非正常事件；
h) 应检查系统漏洞扫描报告，查看其内容是否包含系统存在的漏洞、严重级别和结果处理等方面，检查扫描时间间隔与扫描周期是否一致。

11.5.6.3.结果判定

a) 如果 11.5.6.2. e)-h)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 11.5.6.2.e)、f)均为肯定， g)、h)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 11.5.6.2. e)、f)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

11.5.7 恶意代码防范管理

11.5.7.1.测评指标

见 GD/J 038-2011 11.5.7。

11.5.7.2.测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否对员工进行基本恶意代码防范意识教育，是否告知应及时升级软件版本，使用外来设备、网络上接收文件和外来计算机或存储设备接入网络系统之前应进行病毒检查等；
b) 应访谈安全管理员，询问是否定期检查恶意代码库的升级情况，对截获的危险病毒或恶意代码是否及时进行分析处理，并形成书面的报表和总结汇报；
c) 应检查恶意代码防范管理文档，查看其内容是否覆盖防恶意代码软件的授权使用、恶意代码库升级、定期汇报等方面；
d) 应检查是否具有恶意代码检测记录、恶意代码库升级记录和分析报告，查看升级记录是否记录升级时间、升级版本等内容；查看分析报告是否描述恶意代码的特征、修补措施等内容。

11.5.7.3.结果判定

a) 如果 11.5.7.2. c)、d)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 11.5.7.2. c)为肯定，d)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 11.5.7.2. c)为否定，则信息系统不符合本单元测评指标要求。

11.5.8 密码管理

11.5.8.1.测评指标

见 GD/J 038-2011 11.5.8。

11.5.8.2.测评实施

本项要求包括：

a) 应访谈安全管理员，询问密码技术和产品的使用是否遵照国家密码管理规定；
b) 应检查是否具有密码使用管理制度。

11.5.8.3.结果判定

a) 如果 11.5.8.2. b)为肯定，则信息系统符合本单元测评指标要求。
b) 如果 11.5.8.2. b)为否定，则信息系统不符合本单元测评指标要求。

11.5.9 变更管理

11.5.9.1.测评指标

见 GD/J 038-2011 11.5.9。

11.5.9.2.测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否制定变更方案指导系统执行变更，目前系统发生过哪些变更，变更方案是否经过评审，变更过程是否文档化；
b) 应访谈系统运维负责人，询问重要系统变更前是否根据申报和审批程序得到有关领导的批准，由何人批准，对发生的变更情况是否通知了所有相关人员，以何种方式通知；

c) 应访谈系统运维负责人，询问变更失败后的恢复程序、工作方法和人员职责是否文档化，恢复过程是否经过演练；
d) 应检查系统变更方案，查看其是否覆盖变更类型、变更原因、变更过程、变更前评估等方面内容；
e) 应检查重要系统的变更申请书，查看其是否有主管领导的批准签字；
f) 应检查变更管理制度，查看其是否覆盖变更前审批、变更过程记录、变更后通报等方面内容；
g) 应检查变更控制的申报、审批程序，查看其是否规定需要申报的变更类型、申报流程、审批部门、批准人等方面内容；
h) 应检查变更失败恢复程序，查看其是否规定变更失败后的恢复流程；
i) 应检查是否具有变更方案评审记录和变更过程记录文档；
j) 应检查测试报告或记录，与播出直接相关的信息系统中，操作系统升级、应用软件升级、恶意代码库更新等是否在测试环境中测试通过，确认所升级内容对安全播出没有影响，方可在信息系统中应用。

11.5.9.3.结果判定

a) 如果 11.5.9.2. d)-j)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 11.5.9.2. d)-g)、i)、j)均为肯定，h)中一项或多项为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 11.5.9.2. d)-g)、i)、j)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

11.5.10 备份与恢复管理

11.5.10.1.测评指标

见 GD/J 038-2011 11.5.10。

11.5.10.2.测评实施

本项要求包括：

a) 应访谈系统管理员、数据库管理员和网络管理员，询问是否识别出需要定期备份的业务信息、系统数据及软件系统，主要有哪些；
b) 应访谈系统管理员、数据库管理员和网络管理员，本单位如果存在第三级及以上系统，询问是否定期执行恢复程序，周期多长，系统是否按照恢复程序完成恢复，如有问题，是否针对问题改进恢复程序或调整其他因素；
c) 应检查备份和恢复管理制度，查看其是否明确备份方式、备份频度、存储介质和保存期等方面内容；
d) 应检查数据备份和恢复策略文档，查看其内容是否覆盖数据的存放场所、文件命名规则、介质替换频率、数据离站传输方法等方面；
e) 应检查备份和恢复记录，其是否包含备份内容、备份操作、备份介质存放等内容，记录内容与备份和恢复策略是否一致。

11.5.10.3.结果判定

a) 如果 11.5.10.2. b)中“如果”条件不成立，则该项为不适用。
b) 如果 11.5.10.2. c)-e)均为肯定，则信息系统符合本单元测评指标要求。

c) 如果 11.5.10.2. c)、d)均为肯定，e)为否定，则信息系统部分符合本单元测评指标要求。
d) 如果 11.5.10.2. c)、d)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

11.5.11 安全事件处置

11.5.11.1.测评指标

见 GD/J 038-2011 11.5.11。

11.5.11.2.测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否制定安全事件报告和处置管理制度、响应处理程序；
b) 应检查信息安全事件和可疑事件上报文档或记录，查看上报事件是否按照国家和行业相关规定执行；
c) 应检查安全事件报告和处置管理制度，查看是否明确安全事件的类型，是否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；
d) 应检查安全事件报告和响应处理程序，是否确定事件的报告流程，响应和处置的范围、程度，以及处理方法等；
e) 应检查安全事件处置归档文件，查看是否分析和鉴定事件产生的原因，是否包括收集证据，记录处理过程，总结经验教训，制定防止再次发生的补救措施，是否妥善保存过程形成的所有文件和记录。

11.5.11.3.结果判定

a) 如果 11.5.11.2. b)-e)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 11.5.11.2. b)、c)、e)均为肯定，d)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 11.5.11.2. b)、c)、e)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

11.5.12 应急预案管理

11.5.12.1.测评指标

见 GD/J 038-2011 11.5.12。

11.5.12.2.测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否制定不同事件的应急预案，是否对系统相关人员进行应急预案培训，多长时间举办一次，是否定期对应急预案进行演练，演练周期多长，是否对应急预案定期进行更新；
b) 应访谈系统运维负责人，询问是否具有应急响应小组，是否具备应急设备并能正常工作，应急预案执行所需资金是否做过预算并能够落实；
c) 应检查应急预案框架，查看其内容是否覆盖启动应急预案的条件、应急处理流程、系统恢复流程、后处理等方面；
d) 应检查是否具有根据应急预案框架制定的不同事件的应急预案；

e) 应检查是否具有根据系统变更、管理要求的变化等及时更新应急预案的管理规定，查看是否明确应急预案根据实际情况及时更新的内容；
f) 应检查是否具有演练记录、每年度的应急预案培训记录。

11.5.12.3.结果判定

a) 如果 11.5.12.2. c)-f)均为肯定，则信息系统符合本单元测评指标要求。
b) 如果 11.5.12.2. c)、d)、f)均为肯定，e)为否定，则信息系统部分符合本单元测评指标要求。
c) 如果 11.5.12.2. c)、d)、f)中一项或多项为否定，则信息系统不符合本单元测评指标要求。

12 信息系统整体测评结论

12.1 概述

信息系统的整体测评，就是在单元测评的基础上，对单元测评中的不符合项和部分符合项进行综合分析，分析这些测评结果是否会影响到信息系统整体安全保护能力，信息系统是否具有相应等级的安全防护能力。

信息系统整体测评应从安全控制点间、层面间和区域间进行安全分析和测评，最后从系统结构安全方面进行综合分析，对系统结构进行安全测评。

安全控制点间测评是指对同一区域同一层面内的两个或两个以上不同安全控制点间的关联进行测评分析，其目的是确定这些关联对信息系统整体安全保护能力的影响。

层面间测评是指对同一区域内的两个或两个以上不同层面的关联进行测评分析，其目的是确定这些关联对信息系统整体安全保护能力的影响。

区域间测评是指对两个或两个以上不同物理或逻辑区域间的关联进行测评分析，其目的是确定这些关联对信息系统整体安全保护能力的影响。

12.2 安全控制点间测评

在单元测评完成后，如果信息系统某个单元测评中存在不符合项或部分符合项，应进行安全控制点间测评，应分析在同一功能区域同一层面内，是否存在其他安全控制点对该安全控制点具有补充作用(如物理访问控制和防盗窃、安全审计和抗抵赖等)，如该安全控制点所对应的系统安全保护能力没有缺失，单元测评中的不符合项或部分符合项没有造成系统整体安全保护能力的缺失，则应在对应的层面测评结论中予以体现。

12.3 层面间测评

在单元测评完成后，如果信息系统某个单元测评中存在不符合项或部分符合项，应进行层面间安全测评，重点分析其他层面上功能相同或相似的安全控制点是否对本安全控制点存在补充作用（如应用层加密与网络层加密、主机层与应用层上的身份鉴别等），以及技术与管理上各层面的关联关系（如主机安全与系统运维管理、应用安全与系统运维管理等），如该安全控制点所对应的系统安全保护能力没有缺失，单元测评中的不符合项或部分符合项没有造成系统整体安全保护能力的缺失，则应在对应的层面测评结论中予以体现。

12.4 区域间测评

在单元测评完成后，如果信息系统单元测评中存在不符合项或部分符合项，应进行区域间安全测评，重点分析系统中访问控制路径（如不同功能区域间的数据流流向和控制方式）是否存在区域间安全功能的相互补充作用，如该安全控制点所对应的系统安全保护能力没有缺失，单元测评中的不符合项或部分符合项没有造成系统整体安全保护能力的缺失，则应在对应的层面测评结论中予以体现。

12.5 系统结构安全测评

在完成安全控制点间、层面间和区域间安全测评后，应进行系统结构安全测评，系统结构安全测评应从信息系统整体结构的安全性和整体安全防范的合理性方面进行分析和测评。

在测评分析信息系统整体结构的安全性时，应掌握信息系统的物理布局、网络拓扑、业务逻辑（业务数据流）、系统实现和集成方式等各种情况，结合业务数据流分析物理布局与网络拓扑之间、网络拓扑与业务逻辑之间、物理布局与业务逻辑之间、不同信息系统之间存在的各种关系，明确系统结构可能面临的威胁、可能暴露的脆弱性等，综合判定信息系统的整体布局是否清晰、合理、安全有效。

在测评分析信息系统整体安全防范的合理性时，应熟悉广播电视安全播出要求、信息系统安全保护措施的具体实现方式和部署情况等，结合业务数据流分析不同区域和不同边界与安全保护措施的关系、重要业务和主要信息与安全保护措施的关系等，识别信息系统的安全防范是否实现纵深防御，突出重点，是否对广播电视播出业务造成影响，综合判定信息系统的整体安全防范措施是否恰当合理、协调一致。

12.6 各层面测评结论

汇总单元测评结果，结合安全控制点间、层面间、区域间测评分析，给出技术安全、物理安全、管理安全的测评结论。技术安全应从基础网络安全、边界安全、终端系统安全、服务端系统安全、应用安全、数据安全与备份恢复、安全管理中心（适用于三级、四级）层面给出安全控制措施的落实情况；物理安全应从物理位置的选择、物理访问控制、防盗窃和防破坏、机房环境、机房消防设施和电力供应层面给出安全控制措施的落实情况；管理安全应从总要求、安全管理机构、人员安全管理、系统建设管理和系统运维管理给出安全控制措施的落实情况。

12.7 整体保护能力的测评结论

等级测评报告应根据各层面的测评结论，给出信息系统整体安全保护能力的测评结论，确认信息系统达到相应等级保护要求的程度。整体安全保护能力的测评结论应包括技术安全、物理安全和管理安全措施的有效性、安全强度的一致性以及整体安全防御体系的完善程度等方面内容。

针对单元测评和整体测评后仍然存在的不符合项应进行风险分析，根据该不符合项对系统信息安全和安全播出的影响程度，将该不符合项引入的风险分为高级、中级、低级。通过全面的安全风险分析，提出整改建议。

附 录 A
（资料性附录）
测评力度

本标准在第 5 章到第 8 章描述了第一级到第四级信息系统的单元测评的具体测评实施过程要求。为了便于理解、对比不同测评方法的测评力度以及不同级别信息系统单元测评的测评力度增强情况，分别编制表 A.1 测评方法的测评力度描述和表 A.2 不同安全保护等级信息系统的测评力度要求表。

A.1 测评方法的测评力度描述

测评方法是测评人员依据测评内容选取的、实施特定测评操作的具体方法。本标准涉及访谈、检查和测试等三种基本测评方法。访谈、检查和测试等三种基本测评方法的测评力度可以通过其测评的深度和广度来描述，如表 A.1。

表A.1 测评方法的测评力度

测评方法	深度	广度
访谈	访谈的深度体现在访谈过程的严格和详细程度，可以分为四种：简要的、充分的、较全面的和全面的。简要访谈只包含通用和高级的问题;充分访谈包含通用和高级的问题以及一些较为详细的问题;较全面访谈包含通用和高级的问题以及一些有难度和探索性的问题;全面访谈包含通用和高级的问题以及较多有难度和探索性的问题。	访谈的广度体现在访谈人员的构成和数量上。访谈覆盖不同类型的人员和同一类人的数量多少，体现出访谈的广度不同。
检查	检查的深度体现在检查过程的严格和详细程度，可以分为四种：简要的、充分的、较全面的和全面的。简要检查主要是对功能级上的文档、机制和活动，使用简要的评审、观察或检查以及检查列表和其他相似手段的简短测评;充分检查有详细的分析、观察和研究，除了功能级上的文档、机制和活动外，还适当需要一些总体/概要设计信息；较全面检查有详细、彻底分析、观察和研究，除了功能级上的文档、机制和活动外，还需要总体/概要和一些详细设计以及实现上的相关信息；全面检查有详细、彻底分析、观察和研究，除了功能级上的文档、机制和活动外，还需要总体/概要和详细设计以及实现上的相关信息。	检查的广度体现在检查对象的种类（文档、机制等）和数量上。检查覆盖不同类型的对象和同一类对象的数量多少，体现出对象的广度不同。

表 A.1（续）

测评方法	深度	广度
测试	测试的深度体现在执行的测试类型上：功能/性能测试和渗透测试。功能/性能测试只涉及机制的功能规范、高级设计和操作规程；渗透测试涉及机制的所有可用文档，并试图智取进入信息系统。	测试的广度体现在被测试的机制种类和数量上。测试覆盖不同类型的机制以及同一类型机制的数量多少，体现出对象的广度不同。

A.2 信息系统测评力度

为了进一步理解不同等级信息系统在测评力度上的不同，表 A.2 在表 A.1 的基础上，从测评对象数量和种类以及测评深度等方面详细分析了不同测评方法的测评力度在不同安全保护等级信息系统安全测评中的具体体现。

表A.2 不同安全保护等级信息系统的测评力度要求

测评力度		信息系统安全保护等级			
		第一级	第二级	第三级	第四级
访谈	广度	测评对象在种类和数量上抽样，种类和数量都较少	测评对象在种类和数量上抽样，种类和数量都较多	测评对象在数量上抽样，在种类上基本覆盖	测评对象在数量上抽样，在种类上全部覆盖
	深度	简要	充分	较全面	全面
检查	广度	测评对象在种类和数量上抽样，种类和数量都较少	测评对象在种类和数量上抽样，种类和数量都较多	测评对象在数量上抽样，在种类上基本覆盖	测评对象在数量上抽样，在种类上全部覆盖
	深度	简要	充分	较全面	全面
测试	广度	测评在种类和数量、范围上抽样，种类和数量较少，范围小	测评对象在种类和数量、范围上抽样，种类和数量都较多，范围大	测评对象在数量和范围上抽样，在种类上基本覆盖	测评对象在数量、范围上抽样，在种类上基本覆盖
	深度	功能测试/性能测试	功能测试/性能测试	功能测试/性能测试，渗透测试	功能测试/性能测试，渗透测试

从表 A.2 可以看到，对不同等级的信息系统进行等级测评时，选择的测评对象的种类和数量是不同的，随着信息系统安全保护等级的增高，抽查的测评对象的种类和数量也随之增加。 对不同安全保护等级信息系统进行等级测评时，实际抽查测评对象的种类和数量，应当达到表 A.2 的要求，以满足相应等级的测评力度要求。在具体测评对象选择工作过程中，可参照遵循以下原则：

a) 完整性原则，选择的设备、措施等应能满足相应等级的测评力度要求；

b) 重要性原则，应抽查重要的服务器、数据库和网络设备等；

c) 安全性原则，应抽查对外暴露的网络边界；

d) 共享性原则，应抽查共享设备和数据交换平台/设备；

e) 代表性原则，抽查应尽量覆盖系统各种设备类型、操作系统类型、数据库系统类型和应用系统的类型。

参 考 文 献

[1] GB/T 28448-2012 信息安全技术 信息系统安全等级保护测评要求
[2] GB/T 28449-2012 信息安全技术 信息系统安全等级保护测评过程指南