ICS 35.040
L80

中华人民共和国国家标准

GB/T ×××××—××××

信息安全技术
信息系统安全等级保护测评过程指南

Information security technology-

Testing and evaluation process guide for

classified protection of information system security

××××-××-××发布　　××××-××-××实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目 次

前 言 IV
引 言 V
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 等级测评概述 1
4.1 等级测评的作用 1
4.2 等级测评执行主体 2
4.3 等级测评风险 2
4.3.1 验证测试影响系统正常运行 2
4.3.2 工具测试影响系统正常运行 2
4.3.3 敏感信息泄漏 2
4.4 等级测评过程 2
4.4.1 测评准备活动 3
4.4.2 方案编制活动 3
4.4.3 现场测评活动 3
4.4.4 分析与报告编制活动 3
5 测评准备活动 3
5.1 测评准备活动的工作流程 3
5.2 测评准备活动的主要任务 3
5.2.1 项目启动 3
5.2.2 信息收集和分析 4
5.2.3 工具和表单准备 4
5.3 测评准备活动的输出文档 5
5.4 测评准备活动中双方的职责 5
6 方案编制活动 5
6.1 方案编制活动的工作流程 5
6.2 方案编制活动的主要任务 6
6.2.1 测评对象确定 6
6.2.2 测评指标确定 7
6.2.3 测试工具接入点确定 8
6.2.4 测评内容确定 9
6.2.5 测评指导书开发 9
6.2.6 测评方案编制 10

6.3 方案编制活动的输出文档.....11
6.4 方案编制活动中双方的职责.....11
7 现场测评活动.....11
7.1 现场测评活动的工作流程.....11
7.2 现场测评活动的主要任务.....12
7.2.1 现场测评准备.....12
7.2.2 现场测评和结果记录.....12
7.2.3 结果确认和资料归还.....14
7.3 现场测评活动的输出文档.....15
7.4 现场测评活动中双方的职责.....15
8 分析与报告编制活动.....16
8.1 分析与报告编制活动的工作流程.....16
8.2 分析与报告编制活动的主要任务.....16
8.2.1 单项测评结果判定.....16
8.2.2 单元测评结果判定.....17
8.2.3 整体测评.....18
8.2.4 风险分析.....18
8.2.5 等级测评结论形成.....19
8.2.6 测评报告编制.....19
8.3 分析与报告编制活动的输出文档.....20
8.4 分析与报告编制活动中双方的职责.....20
附录A.....22
附录B.....24
B.1 测评对象确定原则和方法.....24
B.2 具体确定方法说明.....24
B.2.1 第一级信息系统.....24
B.2.2 第二级信息系统.....25
B.2.3 第三级信息系统.....25
B.2.4 第四级信息系统.....26
附录C.....27
C.1 依据标准，遵循原则.....27
C.2 恰当选取，保证强度.....27
C.3 规范行为，规避风险.....27
附录D.....27
D.1 测评方案编制示例.....27

D.1.1 被测系统描述.....27
D.1.2 测评对象.....28
D.1.3 测评指标.....30
D.1.4 测评工具和接入点.....31
D.1.5 测评内容.....32
D.1.6 测评指导书.....35
D.2 测评报告编制示例.....38
D.2.1 整体测评.....38
D.2.2 整改建议.....40
参考文献.....42

前　言

（略）

引 言

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）、《关于信息安全等级保护工作的实施意见》（公通字[2004]66号）和《信息安全等级保护管理办法》（公通字[2007]43号），制定本标准。

本标准是信息安全等级保护相关系列标准之一。

与本标准相关的系列标准包括：

——GB/T 22240-2008 信息安全技术 信息系统安全等级保护定级指南；

——GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求；

——GB/T CCCC-CCCC 信息安全技术 信息系统安全等级保护实施指南；

——GB/T DDDD-DDDD 信息安全技术 信息系统安全等级保护测评要求。

信息安全技术
信息系统安全等级保护测评过程指南

1 范围

本标准规定了信息系统安全等级保护测评（以下简称等级测评）工作的测评过程，既适用于测评机构、信息系统的主管部门及运营使用单位对信息系统安全等级保护状况进行的安全测试评价，也适用于信息系统的运营使用单位在信息系统定级工作完成之后，对信息系统的安全保护现状进行的测试评价，获取信息系统的全面保护需求。

2 规范性引用文件

下列文件中的条款通过在本标准中的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否使用这些文件的最新版本。凡是不注明日期的引用文件，其最新版本适用于本标准。

GB/T 5271.8 信息技术 词汇 第8部分：安全

GB 17859-1999 计算机信息系统安全保护等级划分准则

GB/T 22240-2008 信息安全技术 信息系统安全等级保护定级指南

GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求

GB/T CCCC-CCCC 信息安全技术 信息系统安全等级保护实施指南

GB/T DDDD-DDDD 信息安全技术 信息系统安全等级保护测评要求

《信息安全等级保护管理办法》（公通字[2007]43号）

3 术语和定义

GB/T 5271.8、GB 17859-1999、GB/T CCCC-CCCC和GB/T DDDD-DDDD确立的以及下列的术语和定义适用于本标准。

3.1

优势证据 superior evidence

对单一测评项实施等级测评过程中获得的多个测评结果之间存在矛盾，且都没有足够的证据否定与之矛盾的测评结果的，则测评结果的证明力明显大于其他测评结果的证明力的那个（些）测评结果即为优势证据。

4 等级测评概述

4.1 等级测评的作用

依据《信息安全等级保护管理办法》（公通字[2007]43号），信息系统运营、使用单位在进行信息系统备案后，都应当选择测评机构进行等级测评。等级测评是测评机构依据《信息系统安全等级保护测评要求》等管理规范和技术标准，检测评估信息系统安全等级保护状况是否达到相应等级基本要求的过程，是落实信息安全等级保护制度的重要环节。

在信息系统建设、整改时，信息系统运营、使用单位通过等级测评进行现状分析，确定系统的安全保护现状和存在的安全问题，并在此基础上确定系统的整改安全需求。

在信息系统运维过程中，信息系统运营、使用单位定期委托测评机构开展等级测评，对信息系统安全等级保护状况进行安全测试，对信息安全管控能力进行考察和评价，从而判定信息系统是否具备GB/T 22239-2008中相应等级安全保护能力。而且，等级测评报告是信息系统开展整改加固的重要指导性文件，也是信息系统备案的重要附件材料。等级测评结论为信息系统未达到相应等级的基本安全保护能力的，运营、使用单位应当根据等级测评报告，制定方案进行整改，尽快达到相应等级的安全保护能力。

4.2 等级测评执行主体

可以为三级及以上等级信息系统实施等级测评的等级测评执行主体应具备如下条件：在中华人民共和国境内注册成立（港澳台地区除外）；由中国公民投资、中国法人投资或者国家投资的企事业单位（港澳台地区除外）；从事相关检测评估工作两年以上，无违法记录；工作人员仅限于中国公民；法人及主要业务、技术人员无犯罪记录；使用的技术装备、设施应当符合《信息安全等级保护管理办法》（公通字[2007]43号）对信息安全产品的要求；具有完备的保密管理、项目管理、质量管理、人员管理和培训教育等安全管理制度；对国家安全、社会秩序、公共利益不构成威胁。（摘自《信息安全等级保护管理办法》（公通字[2007]43号））

等级测评执行主体应履行如下义务：遵守国家有关法律法规和技术标准，提供安全、客观、公正的检测评估服务，保证测评的质量和效果；保守在测评活动中知悉的国家秘密、商业秘密和个人隐私，防范测评风险；对测评人员进行安全保密教育，与其签订安全保密责任书，规定应当履行的安全保密义务和承担的法律责任，并负责检查落实。

4.3 等级测评风险

等级测评实施过程中，被测系统可能面临以下风险。

4.3.1 验证测试影响系统正常运行

在现场测评时，需要对设备和系统进行一定的验证测试工作，部分测试内容需要上机查看一些信息，这就可能对系统的运行造成一定的影响，甚至存在误操作的可能。

4.3.2 工具测试影响系统正常运行

在现场测评时，会使用一些技术测试工具进行漏洞扫描测试、性能测试甚至抗渗透能力测试。测试可能会对系统的负载造成一定的影响，漏洞扫描测试和渗透测试可能对服务器和网络通讯造成一定影响甚至伤害。

4.3.3 敏感信息泄漏

泄漏被测系统状态信息，如网络拓扑、IP地址、业务流程、安全机制、安全隐患和有关文档信息。

4.4 等级测评过程

本标准中的测评工作过程及任务基于受委托测评机构对信息系统的初次等级测评给出。运营、使用单位的自查或受委托测评机构对已经实施过一次（或以上）等级测评的被测系统的等级测评，测评机构和测评人员可以根据实际情况调整部分工作任务，具体原则见附录A。

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

4.4.1 测评准备活动

本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。测评准备工作是否充分直接关系到后续工作能否顺利开展。本活动的主要任务是掌握被测系统的详细情况，准备测试工具，为编制测评方案做好准备。

4.4.2 方案编制活动

本活动是开展等级测评工作的关键活动，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确定与被测信息系统相适应的测评对象、测评指标及测评内容等，并根据需要重用或开发测评指导书测评指导书，形成测评方案。

4.4.3 现场测评活动

本活动是开展等级测评工作的核心活动。本活动的主要任务是按照测评方案的总体要求，严格执行测评指导书测评指导书，分步实施所有测评项目，包括单元测评和整体测评两个方面，以了解系统的真实保护情况，获取足够证据，发现系统存在的安全问题。

4.4.4 分析与报告编制活动

本活动是给出等级测评工作结果的活动，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GB/T DDDD-DDDD的有关要求，通过单项测评结果判定、单元测评结果判定、整体测评和风险分析等方法，找出整个系统的安全保护现状与相应等级的保护要求之间的差距，并分析这些差距导致被测系统面临的风险，从而给出等级测评结论，形成测评报告文本。

5 测评准备活动

5.1 测评准备活动的工作流程

测评准备活动的目标是顺利启动测评项目，准备测评所需的相关资料，为顺利编制测评方案打下良好的基础。

测评准备活动包括项目启动、信息收集和分析、工具和表单准备三项主要任务。这三项任务的基本工作流程见图1：

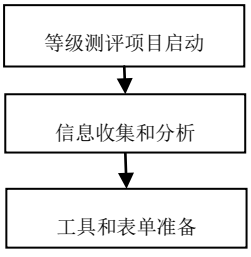

图 1 测评准备活动的基本工作流程

5.2 测评准备活动的主要任务

5.2.1 项目启动

在项目启动任务中，测评机构组建等级测评项目组，获取测评委托单位及被测系统的基本情况，从基本资料、人员、计划安排等方面为整个等级测评项目的实施做基本准备。

输入：委托测评协议书。

任务描述：

a) 根据测评双方签订的委托测评协议书和系统规模，测评机构组建测评项目组，从人员方面做好准备，并编制项目计划书。项目计划书应包含项目概述、工作依据、技术思路、工作内容和项目组织等。

b) 测评机构要求测评委托单位提供基本资料，包括：被测系统总体描述文件，详细描述文件，安全保护等级定级报告，系统验收报告，安全需求分析报告，安全总体方案，自查或上次等级测评报告（如果有），测评委托单位的信息化建设状况与发展以及联络方式等。

输出/产品：项目计划书。

5.2.2 信息收集和分析

测评机构通过查阅被测系统已有资料或使用调查表格的方式，了解整个系统的构成和保护情况，为编写测评方案和开展现场测评工作奠定基础。

输入：调查表格，被测系统总体描述文件，详细描述文件，安全保护等级定级报告，系统验收报告，安全需求分析报告，安全总体方案，自查或上次等级测评报告（如果有）。

任务描述：

a) 测评机构收集等级测评需要的各种资料，包括测评委托单位的各种方针文件、规章制度及相关过程管理记录、被测系统总体描述文件、详细描述文件、安全保护等级定级报告、安全需求分析报告、安全总体方案、安全现状评价报告、安全详细设计方案、用户指南、运行步骤、网络图表、配置管理文档等。

b) 测评机构将调查表格提交给测评委托单位，督促 被测系统相关人员准确填写调查表格。

c) 测评机构收回填写完成的调查表格，并分析调查结果，了解和熟悉被测系统的实际情况。分析的内容包括被测系统的基本信息、物理位置、行业特征、管理框架、管理策略、网络及设备部署、软硬件重要性及部署情况、范围及边界、业务种类及重要性、业务流程、业务数据及重要性、业务安全保护等级、用户范围、用户类型、被测系统所处的运行环境及面临的威胁等。这些信息可以重用自查或上次等级测评报告中的可信结果。

d) 如果调查表格填写不准确或不完善或存在相互矛盾的地方较多，测评机构应安排现场调查，与被测系统相关人员进行面对面的沟通和了解。

输出/产品：填好的调查表格。

5.2.3 工具和表单准备

测评项目组成员在进行现场测评之前，应熟悉与被测系统相关的各种组件、调试测评工具、准备各种表单等。

输入：各种与被测系统相关的技术资料。

任务描述：

a) 测评人员调试本次测评过程中将用到的测评工具，包括漏洞扫描工具、渗透性测试工具、性能测试工具和协议分析工具等。

b) 测评人员模拟被测系统搭建测评环境。

c) 准备和打印表单，主要包括：现场测评授权书、文档交接单、会议记录表单、会议

签到表单等。

输出/产品：选用的测评工具清单，打印的各类表单。

5.3 测评准备活动的输出文档

测评准备活动的输出文档及其内容如表1所示：

表 1 测评准备活动的输出文档及其内容

任务	输出文档	文档内容
项目启动	项目计划书	项目概述、工作依据、技术思路、工作内容和项目组织等
信息收集和分析	填好的调查表格	被测系统的安全保护等级、业务情况、数据情况、软硬件情况、管理模式和相关部门及角色等。
工具和表单准备	选用的测评工具清单 打印的各类表单：现场测评授权书、文档交接单、会议记录表单、会议签到表单。	现场测评授权、交接的文档名称、会议记录项目、会议签到项目。

5.4 测评准备活动中双方的职责

测评机构职责：

a) 组建等级测评项目组。

b) 指出测评委托单位应提供的基本资料。

c) 准备被测系统基本情况调查表格，并提交给测评委托单位。

d) 向测评委托单位介绍安全测评工作流程和方法。

e) 向测评委托单位说明测评工作可能带来的风险和规避方法。

f) 了解测评委托单位的信息化建设状况与发展，以及被测系统的基本情况。

g) 初步分析系统的安全情况。

h) 准备测评工具和文档。

测评委托单位职责：

a) 向测评机构介绍本单位的信息化建设状况与发展情况。

b) 准备测评机构需要的资料。

c) 为测评人员的信息收集提供支持和协调。

d) 准确填写调查表格。

e) 根据被测系统的具体情况，如业务运行高峰期、网络布置情况等，为测评时间安排提供适宜的建议。

f) 制定应急预案。

6 方案编制活动

6.1 方案编制活动的工作流程

方案编制活动的目标是整理测评准备活动中获取的信息系统相关资料，为现场测评活动提供最基本的文档和指导方案。

方案编制活动包括测评对象确定、测评指标确定、测试工具接入点确定、测评内容确定、测评指导书测评指导书开发及测评方案编制六项主要任务。这六项任务的基本工作流程见图2：

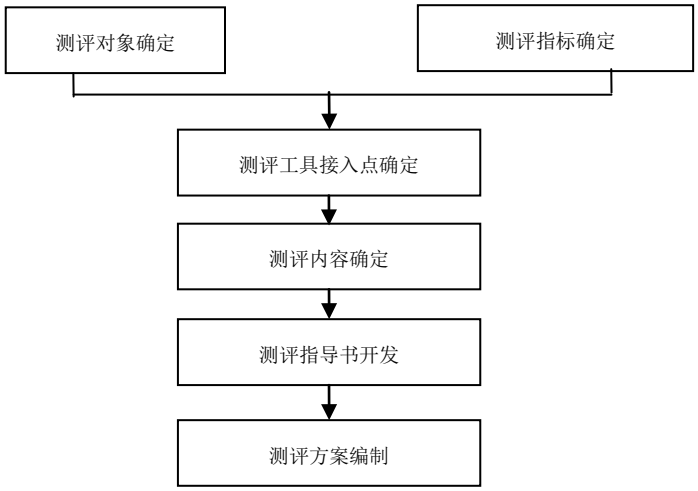

图 2 方案编制活动的基本工作流程

6.2 方案编制活动的主要任务

6.2.1 测评对象确定

根据已经了解到的被测系统信息，分析整个被测系统及其涉及的业务应用系统，确定出本次测评的测评对象。

输入：填好的调查表格。

任务描述：

a) 识别并描述被测系统的整体结构

根据调查表格获得的被测系统基本情况，识别出被测系统的整体结构并加以描述。描述内容应包括被测系统的标识（名称），物理环境，网络拓扑结构和外部边界连接情况等，并给出网络拓扑图。

b) 识别并描述被测系统的边界

根据填好的调查表格，识别出被测系统边界并加以描述。描述内容应包括被测系统与其他网络进行外部连接的边界连接方式，如采用光纤、无线和专线等；描述各边界主要设备，如防火墙、路由器或服务器等。如果在被测系统边界连接处有共用设备，一般可以把该设备划到等级较高的那个信息系统中。

c) 识别并描述被测系统的网络区域

一般信息系统都会根据业务类型及其重要程度将信息系统划分为不同的区域。对于没有进行区域划分的系统，应首先根据被测系统实际情况进行大致划分并加以描述。描述内容主要包括区域划分、每个区域内的主要业务应用、业务流程、区域的边界以及它们之间的连接情况等。

d) 识别并描述被测系统的重要节点

描述系统节点时可以以区域为线索，具体描述各个区域内包括的计算机硬件设备（包括服务器设备、客户端设备、打印机及存储器等外围设备）、网络硬件设备（包括交换机、路

由器、各种适配器等）等，并说明各个节点之间的主要连接情况和节点上安装的应用系统软件情况等。

e） 描述被测系统

对上述描述内容进行整理，确定被测系统并加以描述。描述被测系统时，一般以被测系统的网络拓扑结构为基础，采用总分式的描述方法，先说明整体结构，然后描述外部边界连接情况和边界主要设备，最后介绍被测系统的网络区域组成、主要业务功能及相关的设备节点等。

f） 确定测评对象

分析各个作为定级对象的信息系统，包括信息系统的重要程度及其相关设备、组件，在此基础上，确定出各测评对象。

g） 描述测评对象

描述测评对象时，一般针对每个定级对象分门别类加以描述，包括机房、业务应用软件、主机操作系统、数据库管理系统、网络互联设备及其操作系统、安全设备及其操作系统、访谈人员及其安全管理文档等。在对每类测评对象进行描述时则一般采用列表的方式，包括测评对象所属区域、设备名称、用途、设备信息等内容。

输出/产品：测评方案的测评对象部分。

6.2.2 测评指标确定

根据已经了解到的被测系统定级结果，确定出本次测评的测评指标。

输入：填好的调查表格，GB/T 22239-2008。

任务描述：

a） 根据被测系统调查表格，得出被测系统的定级结果，包括业务信息安全保护等级和系统服务安全保护等级，从而得出被测系统应采取的安全保护措施 ASG 组合情况。

b） 从 GB/T 22239-2008 中选择相应等级的安全要求作为测评指标，包括对 ASG 三类安全要求的选择。举例来说，假设某信息系统的定级结果为：安全保护等级为 3 级，业务信息安全保护等级为 2 级，系统服务安全保护等级为 3 级；则该系统的测评指标将包括 GB/T 22239-2008“技术要求”中的 3 级通用安全保护类要求（G3），2 级业务信息安全类要求（S2），3 级系统服务保证类要求（A3），以及第 3 级“管理要求”中的所有要求。

c） 对于由多个不同等级的信息系统组成的被测系统，应分别确定各个定级对象的测评指标。如果多个定级对象共用物理环境或管理体系，而且测评指标不能分开，则不能分开的这些测评指标应采用就高原则。

d） 分别针对每个定级对象加以描述，包括系统的定级结果、指标选择两部分。其中，指标选择可以列表的形式给出。例如，一个安全保护等级和系统服务安全保护等级均为三级、业务信息安全保护等级为 2 级的定级对象，测评指标可以列出下表：

表 2 测评指标

测评指标					
技术/管理	层面	数量			
		S 类 (2 级)	A 类 (3 级)	G 类 (3 级)	小计
安全技术	物理安全	1	1	8	10
	网络安全	1	0	6	7
	主机安全	2	1	3	6
	应用安全	4	2	2	8
	数据安全	2	1	0	3
安全管理	安全管理制度	0	0	3	3
	安全管理机构	0	0	5	5
	人员安全管理	0	0	5	5
	系统建设管理	0	0	11	11
	系统运维管理	0	0	13	13
合 计					71（类）

输出/产品：测评方案的测评指标部分。

6.2.3 测试工具接入点确定

在等级测评中，对二级和二级以上的信息系统应进行工具测试，工具测试可能用到漏洞扫描器、渗透测试工具集、协议分析仪等测试工具。

输入：填好的调查表格，GB/T DDDD-DDDD。

任务描述：

a) 确定需要进行工具测试的测评对象。

b) 选择测试路径。一般来说，测试工具的接入采取从外到内，从其他网络到本地网段的逐步逐点接入，即：测试工具从被测系统边界外接入、在被测系统内部与测评对象不同网段及同一网段内接入等几种方式。

c) 根据测试路径，确定测试工具的接入点。

从被测系统边界外接入时，测试工具一般接在系统边界设备（通常为交换设备）上。在该点接入漏洞扫描器，扫描探测被测系统的主机、网络设备对外暴露的安全漏洞情况。在该接入点接入协议分析仪，可以捕获应用程序的网络数据包，查看其安全加密和完整性保护情况。在该接入点使用渗透测试工具集，试图利用被测试系统的主机或网络设备的安全漏洞，跨过系统边界，侵入被测系统主机或网络设备。

从系统内部与测评对象不同网段接入时，测试工具一般接在与被测对象不在同一网段的内部核心交换设备上。在该点接入扫描器，可以直接扫描测试内部各主机和网络设备对本单位其他不同网络所暴露的安全漏洞情况。在该接入点接入网络拓扑发现工具，可以探测信息系统的网络拓扑情况。

在系统内部与测评对象同一网段内接入时，测试工具一般接在与被测对象在同一网段的交换设备上。在该点接入扫描器，可以在本地直接测试各被测主机、网络设备对本地网络暴

露的安全漏洞情况。一般来说，该点扫描探测出的漏洞数应该是最多的，它说明主机、网络设备在没有网络安全保护措施下的安全状况。如果该接入点所在网段有大量用户终端设备，则可以在该接入点接入非法外联检测设备，测试各终端设备是否出现过非法外联情况。

d) 结合网络拓扑图，采用图示的方式描述测试工具的接入点、测试目的、测试途径和测试对象等相关内容。

输出/产品：测评方案的测评内容中关于测评工具接入点部分。

6.2.4 测评内容确定

本部分确定现场测评的具体实施内容，即单元测评内容。

输入：填好的调查表格，测评方案的测评对象、测评指标及测评工具接入点部分。

任务描述：

a) 确定单元测评内容

依据GB/T DDDD-DDDD，将前面已经得到的测评指标和测评对象结合起来，然后再将测评对象与具体的测评方法结合起来，这也是编制测评指导书测评指导书的第一步。

具体做法就是把各层面上的测评指标结合到具体测评对象上，并说明具体的测评方法，如此构成一个个可以具体实施测评的单元。参照GB/T DDDD-DDDD，结合已选定的测评指标和测评对象，概要说明现场单元测评实施的工作内容；涉及到工具测试部分，应根据确定的测试工具接入点，编制相应的测试内容。

在测评方案中，现场单元测评实施内容通常以表格的形式给出，表格包括测评指标、测评内容描述等内容。现场测评实施内容是项目组每个成员开发测评指导书测评指导书的基础。

现场单元测评实施内容表格描述的基本格式之一为：

表 3 ××××（如物理安全）单元测评实施内容

序号	测评指标	测评内容描述
1	测评指标 1	测评对象、测评方法、测评实施概述
2	测评指标 2	
3	测评指标 3	
……	……	

输出/产品：测评方案的单元测评实施部分。

6.2.5 测评指导书开发

测评指导书是具体指导测评人员如何进行测评活动的文件，是现场测评的工具、方法和操作步骤等的详细描述，是保证测评活动可以重现的根本。因此，测评指导书应当尽可能详尽、充分。

输入：测评方案的测试工具接入点、单元测评实施部分。

任务描述：

a) 描述单个测评对象，包括测评对象的名称、IP 地址、用途、管理人员等信息。

b) 根据 GB/T DDDD-DDDD 的单元测评实施确定测评活动，包括测评项、测评方法、

操作步骤和预期结果等四部分。

测评项是指GB/T 22239-2008中对该测评对象在该用例中的要求，在GB/T DDDD-DDDD中对应每个测评单元中的“测评指标”的具体要求项。测评方法是指访谈、检查和测试三种方法，具体到测评对象上可细化为文档审查、配置检查、工具测试和实地察看等多种方法，每个测评项可能对应多个测评方法。操作步骤是指在现场测评活动中应执行的命令或步骤，是按照GB/TDDDD-DDDD中的每个“测评实施”项目开发的操作步骤，涉及到工具测试时，应描述工具测试路径及接入点等；预期结果是指按照操作步骤在正常的情况下应得到的结果和获取的证据。

c） 单元测评一般以表格形式设计和描述测评项、测评方法、操作步骤和预期结果等内容。整体测评则一般以文字描述的方式表述，可以以测评用例的方式进行组织。

单元测评的测评指导书描述的基本格式为：

表 4 ×××（测评对象，如核心交换机）单元测评指导书

序号	测评指标		操作步骤	预期结果
1	测评指标 1	测评项 a）	1．…… 2．……	1．…… 2．……
2		测评项 b）	……	……
3		测评项 c）	……	……
4		……	……	……
5	测评指标 2	测评项 a）	……	……
6		……	……	……
7	……	……	……	……

输出/产品：测评指导书，测评结果记录表格。

6.2.6 测评方案编制

测评方案是等级测评工作实施的基础，指导等级测评工作的现场实施活动。测评方案应包括但不局限于以下内容：项目概述、测评对象、测评指标、测评工具的接入点以及单元测评实施等。

输入：委托测评协议书，填好的调研表格，GB/T 22239-2008中相应等级的基本要求，测评方案的测评对象、测评指标、测试工具接入点、测评内容部分。

任务描述：

a） 根据委托测评协议书和填好的调研表格，提取项目来源、测评委托单位整体信息化建设情况及被测系统与单位其他系统之间的连接情况等。

b） 根据等级保护过程中的等级测评实施要求，将测评活动所依据的标准罗列出来。

c） 依据委托测评协议书和被测系统情况，估算现场测评工作量。工作量可以根据配置检查的节点数量和工具测试的接入点及测试内容等情况进行估算。

d） 根据测评项目组成员安排，编制工作安排情况。

e) 根据以往测评经验以及被测系统规模，编制具体测评计划，包括现场工作人员的分工和时间安排。在进行时间计划安排时，应尽量避开被测系统的业务高峰期，避免给被测系统带来影响。同时，在测评计划中应将具体测评所需条件以及测评需要的配合人员也一并给出，便于测评实施之前双方沟通协调、合理安排。

f) 汇总上述内容及方案编制活动的其他任务获取的内容形成测评方案文稿。

g) 评审和提交测评方案。测评方案初稿应通过测评项目组全体成员评审，修改完成后形成提交稿。然后，测评机构将测评方案提交给测评委托单位签字认可。

输出/产品：经过评审和确认的测评方案文本。

6.3 方案编制活动的输出文档

方案编制活动的输出文档及其内容如表5所示：

表5 方案编制活动的输出文档及其内容

任务	输出文档	文档内容
测评对象确定	测评方案的测评对象部分	被测系统的整体结构、边界、网络区域、重要节点、测评对象等
测评指标确定	测评方案的测评指标部分	被测系统定级结果、测评指标
测试工具接入点确定	测评方案的测试工具接入点部分	测试工具接入点及测试方法
测评内容确定	测评方案的单元测评实施部分	单元测评实施内容
测评指导书开发	测评指导书	各测评对象的测评内容及方法
测评方案编制	测评方案文本	项目概述、测评对象、测评指标、测试工具接入点、单元测评实施内容等

6.4 方案编制活动中双方的职责

测评机构职责：

a) 详细分析被测系统的整体结构、边界、网络区域、重要节点等。

b) 初步判断被测系统的安全薄弱点。

c) 分析确定测评对象、测评指标和测试工具接入点，确定测评内容及方法。

d) 编制测评方案文本，并对其内部评审，并提交被测机构签字确认。

测评委托单位职责：

a) 对测评方案进行认可，并签字确认。

7 现场测评活动

7.1 现场测评活动的工作流程

现场测评活动通过与测评委托单位进行沟通和协调，为现场测评的顺利开展打下良好基础，然后依据测评方案实施现场测评工作，将测评方案和测评工具等具体落实到现场测评活动中。现场测评工作应取得分析与报告编制活动所需的、足够的证据和资料。

现场测评活动包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项主要任务。这三项任务的基本工作流程见图3：

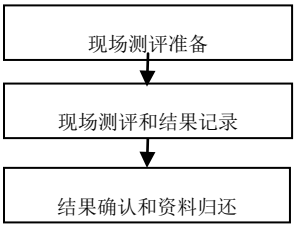

图 3 现场测评活动的基本工作流程

7.2 现场测评活动的主要任务

7.2.1 现场测评准备

本任务启动现场测评，是保证测评机构能够顺利实施测评的前提。

输入：现场测评授权书，测评方案。

任务描述：

a) 测评委托单位签署现场测评授权书。

b) 召开测评现场首次会，测评机构介绍测评工作，交流测评信息，进一步明确测评计划和方案中的内容，说明测评过程中具体的实施工作内容，测评时间安排等，以便于后面的测评工作开展。

c) 测评双方确认现场测评需要的各种资源，包括测评委托单位的配合人员和需要提供的测评条件等，确认被测系统已备份过系统及数据。

d) 测评人员根据会议沟通结果，对测评结果记录表单和测评程序进行必要的更新。

输出/产品：会议记录，更新后的测评计划和测评程序，确认的测评授权书等。

7.2.2 现场测评和结果记录

现场测评一般包括访谈、文档审查、配置检查、工具测试和实地察看五个方面。

7.2.2.1 访谈

输入：测评指导书，技术安全和管理安全测评的测评结果记录表格。

任务描述：

a) 测评人员与被测系统有关人员（个人/群体）进行交流、讨论等活动，获取相关证据，了解有关信息。在访谈范围上，不同等级信息系统在测评时有不同的要求，一般应基本覆盖所有的安全相关人员类型，在数量上可以抽样。具体可参照 GB/T DDDD-DDDD 中的各级要求。

输出/产品：技术安全和管理安全测评的测评结果记录或录音。

7.2.2.2 文档审查

输入：安全方针文件，安全管理制度，安全管理的执行过程文档，系统设计方案，网络设备的技术资料，系统和产品的实际配置说明，系统的各种运行记录文档，机房建设相关资料，机房出入记录等过程记录文档，测评指导书，管理安全测评的测评结果记录表格。

任务描述：

a) 检查 GB/T 22239-2008 中规定的必须具有的制度、策略、操作规程等文档是否齐备。

b) 检查是否有完整的制度执行情况记录，如机房出入登记记录、电子记录、高等级系统的关键设备的使用登记记录等。

c) 对上述文档进行审核与分析，检查他们的完整性和这些文件之间的内部一致性。

下面列出对不同等级信息系统在测评实施时的不同强度要求。

一级：满足GB/T 22239-2008中的一级要求。

二级：满足GB/T 22239-2008中的二级要求，并且所有文档之间应保持一致性，要求有执行过程记录的，过程记录文档的记录内容应与相应的管理制度和文档保持一致，与实际情况保持一致。

三级：满足GB/T 22239-2008中的三级要求，所有文档应具备且完整，并且所有文档之间应保持一致性，要求有执行过程记录的，过程记录文档的记录内容应与相应的管理制度和文档保持一致，与实际情况保持一致，安全管理过程应与系统设计方案保持一致且能够有效管理系统。

四级：满足GB/T 22239-2008中的四级要求，所有文档应具备且完整，并且所有文档之间应保持一致性，要求有执行过程记录的，过程记录文档的记录内容应与相应的管理制度和文档保持一致，与实际情况保持一致，安全管理过程应与系统设计方案保持一致且能够有效管理系统。

输出/产品：管理安全测评的测评结果记录。

7.2.2.3 配置检查

输入：测评指导书，技术安全测评的网络、主机、应用测评结果记录表格。

任务描述：

a) 根据测评结果记录表格内容，利用上机验证的方式检查应用系统、主机系统、数据库系统以及网络设备的配置是否正确，是否与文档、相关设备和部件保持一致，对文档审核的内容进行核实（包括日志审计等）。

b) 如果系统在输入无效命令时不能完成其功能，将要对其进行错误测试。

c) 针对网络连接，应对连接规则进行验证。

下面列出对不同等级信息系统在测评实施时的不同强度要求。

一级：满足GB/T 22239-2008中的一级要求。

二级：满足GB/T 22239-2008中的二级要求，测评其实施的正确性和有效性，检查配置的完整性，测试网络连接规则的一致性。

三级：满足GB/T 22239-2008中的三级要求，测评其实施的正确性和有效性，检查配置的完整性，测试网络连接规则的一致性，测试系统是否达到可用性和可靠性的要求。

四级：满足GB/T 22239-2008中的四级要求，测评其实施的正确性和有效性，检查配置的完整性，测试网络连接规则的一致性，测试系统是否达到可用性和可靠性的要求。

输出/产品：技术安全测评的网络、主机、应用测评结果记录。

7.2.2.4 工具测试

输入：测评指导书，技术安全测评的网络、主机、应用测评结果记录表格。

任务描述：

a) 根据测评指导书，利用技术工具对系统进行测试，包括基于网络探测和基于主机审计的漏洞扫描、渗透性测试、性能测试、入侵检测和协议分析等。

b) 备份测试结果。

下面列出对不同等级信息系统在测评实施时的不同强度要求。

一级：满足GB/T 22239-2008中的一级要求。

二级：满足GB/T 22239-2008中的二级要求，针对主机、服务器、关键网络设备、安全设备等设备进行漏洞扫描等。

三级：满足GB/T 22239-2008中的三级要求，针对主机、服务器、网络设备、安全设备等设备进行漏洞扫描，针对应用系统完整性和保密性要求进行协议分析，渗透测试应包括基于一般脆弱性的内部和外部渗透攻击。

四级：满足GB/T 22239-2008中的四级要求，针对主机、服务器、网络设备、安全设备等设备进行漏洞扫描，针对应用系统完整性和保密性要求进行协议分析，渗透测试应包括基于一般脆弱性的内部和外部渗透攻击。

输出/产品：技术安全测评的网络、主机、应用测评结果记录，工具测试完成后的电子输出记录，备份的测试结果文件。

7.2.2.5 实地察看

输入：测评指导书，技术安全测评的物理安全和管理安全测评结果记录表格。

任务描述：

a) 根据被测系统的实际情况，测评人员到系统运行现场通过实地的观察人员行为、技术设施和物理环境状况判断人员的安全意识、业务操作、管理程序和系统物理环境等方面的安全情况，测评其是否达到了相应等级的安全要求。

下面列出对不同等级信息系统在测评实施时的不同强度要求。

一级：满足GB/T 22239-2008中的一级要求。

二级：满足GB/T 22239-2008中的二级要求。

三级：满足GB/T 22239-2008中的三级要求，判断实地观察到的情况与制度和文档中说明的情况是否一致，检查相关设备、设施的有效性和位置的正确性，与系统设计方案的一致性。

四级：满足GB/T 22239-2008中的四级要求，判断实地观察到的情况与制度和文档中说明的情况是否一致，检查相关设备、设施的有效性和位置的正确性，与系统设计方案的一致性。

输出/产品：技术安全测评的物理安全和管理安全测评结果记录。

7.2.3 结果确认和资料归还

输入：测评结果记录，工具测试完成后的电子输出记录。

任务描述：

a) 测评人员在现场测评完成之后，应首先汇总现场测评的测评记录，对漏掉和需要进一步验证的内容实施补充测评。

b) 召开测评现场结束会，测评双方对测评过程中发现的问题进行现场确认。

c) 测评机构归还测评过程中借阅的所有文档资料，并由 测评委托单位文档资料提供者签字确认。

输出/产品：现场测评中发现的问题汇总，证据和证据源记录，测评委托单位的书面认可文件。

7.3 现场测评活动的输出文档

现场测评活动的输出文档及其内容如表6所示：

表 6 现场测评活动的输出文档及其内容

任务	输出文档	文档内容
现场测评准备	会议记录、确认的测评授权书、更新后的测评计划和测评程序	工作计划和内容安排，双方人员的协调，测评委托单位应提供的配合
访谈	技术安全和管理安全测评的测评结果记录或录音	访谈记录
文档审查	管理安全测评的测评结果记录	管理制度和管理执行过程文档的记录
配置检查	技术安全测评的网络、主机、应用测评结果记录	检查内容的记录
工具测试	技术安全测评的网络、主机、应用测评结果记录，工具测试完成后的电子输出记录，备份的测试结果文件	漏洞扫描、渗透性测试、性能测试、入侵检测和协议分析等内容的技术测试结果
实地察看	技术安全测评的物理安全和管理安全测评结果记录	检查内容的记录
测评结果确认	现场核查中发现的问题汇总、证据和证据源记录、测评委托单位的书面认可文件	测评活动中发现的问题、问题的证据和证据源、每项检查活动中测评委托单位配合人员的书面认可

7.4 现场测评活动中双方的职责

测评机构职责：

a) 利用访谈、文档审查、配置检查、工具测试和实地察看的方法测评被测系统的保护措施情况，并获取相关证据。

测评委托单位职责：

a) 测评前备份系统和数据，并确认被测设备状态完好。
b) 协调被测系统内部相关人员的关系，配合测评工作的开展。
c) 签署现场测评授权书。
d) 相关人员回答测评人员的问询，对某些需要验证的内容上机进行操作。
e) 相关人员确认测试前协助测评人员实施工具测试并提供有效建议，降低安全测评对系统运行的影响。
f) 相关人员协助测评人员完成业务相关内容的问询、验证和测试。
g) 相关人员对测评结果进行确认。
h) 相关人员确认测试后被测设备状态完好。

8 分析与报告编制活动

8.1 分析与报告编制活动的工作流程

在现场测评工作结束后，测评机构应对现场测评获得的测评结果（或称测评证据）进行汇总分析，形成等级测评结论，并编制测评报告。

测评人员在初步判定单元测评结果后，还需进行整体测评，经过整体测评后，有的单元测评结果可能会有所变化，需进一步修订单元测评结果，而后进行风险分析和评价，形成等级测评结论。分析与报告编制活动包括单项测评结果判定、单元测评结果判定、整体测评、风险分析、等级测评结论形成及测评报告编制六项主要任务。这六项任务的基本工作流程见图4：

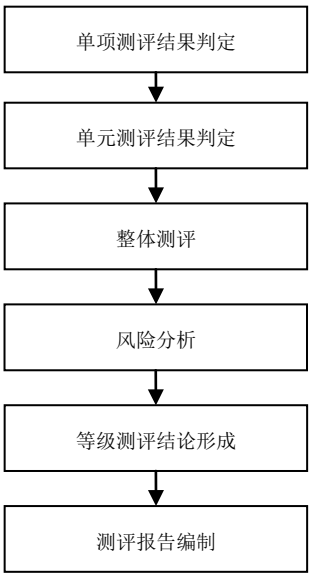

图 4 分析与报告编制活动的基本工作流程

8.2 分析与报告编制活动的主要任务

8.2.1 单项测评结果判定

本任务主要是针对测评指标中的单个测评项，结合具体测评对象，客观、准确地分析测评证据，形成初步单项测评结果，单项测评结果是形成等级测评结论的基础。

输入：技术安全和管理安全的单项测评结果记录，测评指导书。

任务描述：

a) 针对每个测评项，分析该测评项所对抗的威胁在被测系统中是否存在，如果不存在，则该测评项应标为不适用项。对于适用项，则

b) 分析单个测评项是否有多方面的要求内容，针对每一方面的要求内容，从一个或多个测评证据中选择出“优势证据”，并将“优势证据”与要求内容的预期测评结果相比较。

c) 如果测评证据表明所有要求内容与预期测评结果一致，则判定该测评项的单项测评结果为符合；如果测评证据表明所有要求内容与预期测评结果不一致，判定该测评项的单项测评结果为不符合；否则判定该测评项的单项测评结果为部分符合。

根据“优势证据”的定义，具体从测评方式上来看，针对物理安全测评，实地察看证据相比文档审查证据为优势证据，文档审查证据相比访谈证据为优势证据；针对技术安全的其他方面测评，工具测试证据相比配置检查证据为优势证据，配置检查证据相比访谈证据为优势证据；针对管理安全测评，优势证据不确定，需根据实际情况分析确定优势证据。

输出/产品：测评报告的单元测评的结果记录部分。

8.2.2 单元测评结果判定

本任务主要是将单项测评结果进行汇总，分别统计不同测评对象的单项测评结果，从而判定单元测评结果，并以表格的形式逐一列出。

输入：测评报告的单元测评的结果记录部分。

任务描述：

a) 按层面分别汇总不同测评对象对应测评指标的单项测评结果情况，包括测评多少项，符合要求的多少项等内容，一般以表格形式列出。

汇总统计分析的基本表格形式可以如下：

表 7 ××安全单元测评结果汇总表

序号	测评对象	测评指标			
		测评指标 1	测评指标 2	测评指标 3	……
1	对象 1	✓（或×或△或 N/A） 符合项数/在对象 1 上测评的测评指标 1 包含的测评项总数			
2	对象 2				
3	对象 3				
……	……				
	小 计	符合项数/在上述对象上测评的测评指标 1 包含的测评项总数			
注 “✓”表示“符合”，“△”表示部分符合，“×”表示“不符合”，“N/A”表示“不适用”。					

上表中的符号即为测评对象对应的单元测评结果。测评对象在某个测评指标的单元测评结果判别原则如下：

1. 测评指标包含的所有适用测评项的单项测评结果均为符合，则该测评对象对应该测评指标的单元测评结果为符合；
2. 测评指标包含的所有适用测评项的单项测评结果均为不符合，则该测评对象对应该测评指标的单元测评结果为不符合；
3. 测评指标包含的所有测评项均为不适用项，则该测评对象对应该测评指标的单元测评结果为不适用；
4. 测评指标包含的所有适用测评项的单项测评结果不全为符合或不符合，则该测评对象对应该测评指标的单元测评结果为部分符合。

输出/产品：测评报告的单元测评的结果汇总部分。

8.2.3 整体测评

针对单项测评结果的不符合项，采取逐条判定的方法，从安全控制间、层面间和区域间出发考虑，给出整体测评的具体结果，并对系统结构进行整体安全测评。

输入：测评报告的单元测评的结果汇总部分。

任务描述：

a) 针对测评对象“部分符合”及“不符合”要求的单个测评项，分析与该测评项相关的其他测评项能否和它发生关联关系，发生什么样的关联关系，这些关联关系产生的作用是否可以“弥补”该测评项的不足，以及该测评项的不足是否会影响与其有关联关系的其他测评项的测评结果。

b) 针对测评对象“部分符合”及“不符合”要求的单个测评项，分析与该测评项相关的其他层面的测评对象能否和它发生关联关系，发生什么样的关联关系，这些关联关系产生的作用是否可以“弥补”该测评项的不足，以及该测评项的不足是否会影响与其有关联关系的其他测评项的测评结果。

c) 针对测评对象“部分符合”及“不符合”要求的单个测评项，分析与该测评项相关的其他区域的测评对象能否和它发生关联关系，发生什么样的关联关系，这些关联关系产生的作用是否可以“弥补”该测评项的不足，以及该测评项的不足是否会影响与其有关联关系的其他测评项的测评结果。

d) 从安全角度分析被测系统整体结构的安全性，从系统角度分析被测系统整体安全防范的合理性。

e) 汇总上述分析结论，形成表格。

表格基本形式如下：

表 8 ××整体测评结果

序号	安全控制	测评对象	单项判定 不符合项	能否进行关 联互补	说明
1	测评指标 1	对象 1			
		对象 2			
		……			
2	测评指标 1	对象 1			
		……			
……	……	……			
项 目 小 计					

输出/产品：测评报告的整体测评部分。

8.2.4 风险分析

测评人员依据等级保护的相关规范和标准，采用风险分析的方法分析等级测评结果中存在的安全问题可能对被测系统安全造成的影响。

输入：填好的调查表格，测评报告的单元测评的结果汇总及整体测评部分。

任务描述：

a) 结合单元测评的结果汇总和整体测评结果，将物理安全、网络安全、主机安全、应用安全等层面中各个测评对象的测评结果再次汇总分析，统计符合情况。一般可以表格的形式描述。

表格的基本形式可以如下：

表 9 ××系统测评结果汇总

序号	层面（类）	测评指标	符合情况			
1	网络安全	测评指标 1	符合	部分符合	不符合	不适用
……		……				
……	……	……				
统计						

b) 判断测评结果汇总中部分符合项或不符合项所产生的安全问题被威胁利用的可能性，可能性的取值范围为高、中和低。

c) 判断测评结果汇总中部分符合项或不符合项所产生的安全问题被威胁利用后，对被测系统的业务信息安全和系统服务安全造成的影响程度，影响程度取值范围为高、中和低。

d) 综合 b）和 c）的结果，对被测系统面临的安全风险进行赋值，风险值的取值范围为高、中和低。

e) 结合被测系统的安全保护等级对风险分析结果进行评价，即对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益造成的风险。

输出：测评报告的测评结果汇总及风险分析和评价部分。

8.2.5 等级测评结论形成

测评人员在测评结果汇总的基础上，找出系统保护现状与等级保护基本要求之间的差距，并形成等级测评结论。

输入：测评报告的测评结果汇总部分。

任务描述：

a) 根据表 9 测评结果汇总表格，如果部分符合和不符合项的统计结果不全为 0，则该信息系统未达到相应等级的基本安全保护能力；如果部分符合和不符合项的统计结果全为 0，则该信息系统达到了相应等级的基本安全保护能力。

输出/产品：测评报告的等级测评结论部分。

8.2.6 测评报告编制

测评报告应包括但不局限于以下内容：概述、被测系统描述、测评对象说明、测评指标说明、测评内容和方法说明、单元测评、整体测评、测评结果汇总、风险分析和评价、等级测评结论、整改建议等。

其中，概述部分描述被测系统的总体情况、本次测评的主要测评目的和依据；被测系统描述、测评对象、测评指标、测评内容和方法等部分内容编制时可以参考测评方案相关部分内容，有改动的地方应根据实际测评情况进行修改。

输入：测评方案，单元测评的结果记录和结果汇总部分，整体测评部分，风险分析和评价部分、等级测评结论部分。

任务描述：

a) 测评人员整理前面几项任务的输出/产品，编制测评报告相应部分。一个测评委托单位应形成一份测评报告，如果一个测评委托单位内有多个被测系统，报告中应分别描述每一个被测系统的等级测评情况。

b) 针对被测系统存在的安全隐患，从系统安全角度提出相应的改进建议，编制测评报告的安全建设整改建议部分。

c) 列表给出现场测评的文档清单和单项测评记录，以及对各个测评项的单项测评结果判定情况，编制测评报告的单元测评的结果记录和问题分析部分。

d) 测评报告编制完成后，测评机构应根据测评协议书、测评委托单位提交的相关文档、测评原始记录和其他辅助信息，对测评报告进行评审。

e) 评审通过后，由项目负责人签字确认并提交给测评委托单位。

输出/产品：经过评审和确认的被测系统等级测评报告。

8.3 分析与报告编制活动的输出文档

分析与报告编制活动的输出文档及其内容如表10所示：

表 10 分析与报告编制活动的输出文档及其内容

任务	输出文档	文档内容
单项测评结果判定	等级测评报告的单元测评的结果记录部分	分析被测系统的安全现状（各个层面的基本安全状况）与标准中相应等级的基本要求的符合情况，给出单项测评结果。
单项测评结果汇总分析	等级测评报告的单元测评的结果汇总部分	汇总统计单项测评结果，给出针对每个对象的单元测评结果。
整体测评	等级测评报告的整体测评部分	分析被测系统整体安全状况及对单项测评结果的修订情况。
风险分析	等级测评报告的风险分析和评价部分	分析被测系统存在的风险情况。
等级测评结论形成	等级测评报告的等级测评结论部分	对测评结果进行分析，形成等级测评结论。
测评报告编制	等级测评报告	单项测评记录和结果，单项测评结果汇总，整体测评过程及结果，风险分析过程及结果，等级测评结论，安全建设整改建议等。

8.4 分析与报告编制活动中双方的职责

测评机构职责：

a) 分析并判定单项测评结果和整体测评结果。

b) 分析评价被测系统存在的风险情况。

c) 根据测评结果形成等级测评结论。

d) 编制等级测评报告，说明系统存在的安全隐患和缺陷，并给出改进建议。

e) 评审等级测评报告，并将评审过的等级测评报告按照分发范围进行分发。

f) 将生成的过程文档归档保存，并将测评过程中生成的电子文档清除。

测评委托单位职责：

a) 签收测评报告。

附录 A

（资料性附录）

等级测评工作流程

受委托测评机构实施的等级测评工作活动及流程与运营、使用单位的自查活动及流程会有所差异，初次等级测评和再次等级测评的工作活动及流程也不完全相同，而且针对不同等级信息系统实施的等级测评工作活动及流程也不相同。

受委托测评机构对信息系统的初次等级测评可以分为四项活动：测评准备活动、方案编制活动、现场测评活动、分析与报告编制活动。具体如图5所示：

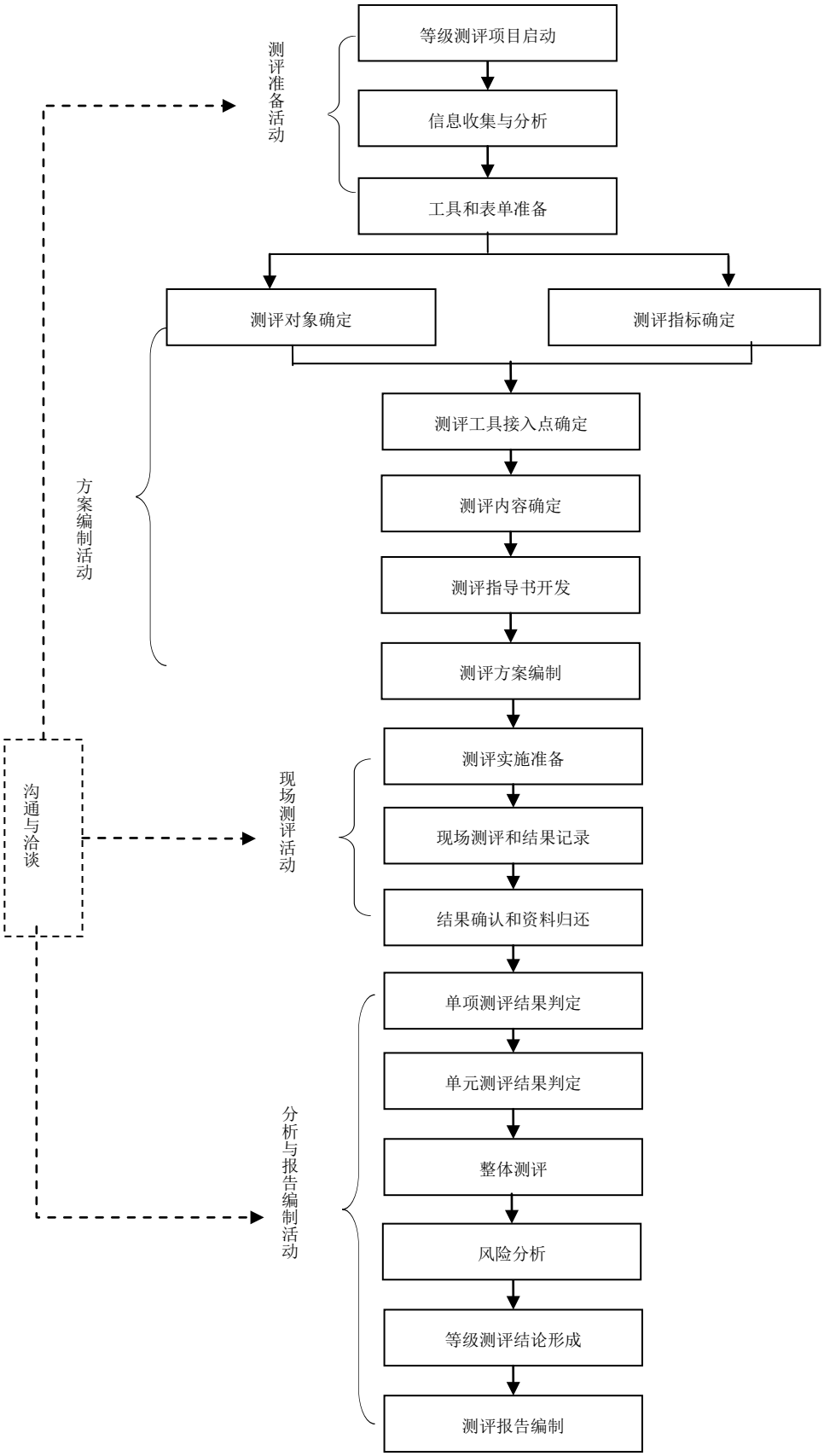

图 5　等级测评基本工作流程

上图是对受委托测评机构对信息系统实施初次等级测评的基本工作流程。如果被测系统已经实施过一次（或多次）等级测评，上图中的四个活动保持不变，但是具体任务内容会有所变化。测评机构和测评人员可以根据上一次等级测评中存在的问题和被测系统的实际情况调整部分工作任务内容。例如，信息收集和分析任务中，可以只收集那些自上次等级测评后有所变更的信息，其他信息可以重用上次等级测评结果；测评对象尽量选择上次等级测评中未测过或存在问题的作为测评对象；测评内容也应关注上次等级测评中发现的问题。

不同等级信息系统的等级测评的基本工作活动与图5中信息系统的等级测评活动应完全一致，即：测评准备、方案编制、现场测评、分析与报告编制四项活动。由于图5给出的是较为全面的工作流程和任务，因此，较低等级信息系统的等级测评的各个活动的具体工作任务应在图5基础上删除或简化部分内容。如针对二级信息系统的等级测评，测评人员在分析与报告编制活动中可以不进行单项测评结果汇总分析，仅进行简单的汇总等。相反，较高等级信息系统的等级测评的工作任务则可以在此基础上增加或细化部分内容。如针对四级信息系统的等级测评，在测评对象确定任务中，不但需要确定出测评对象，还需给出选择这些测评对象的过程及理由等；整体测评需设计具体的整体测评实例等。

附录 B

（资料性附录）

测评对象确定方法

B.1 测评对象确定原则和方法

测评对象是等级测评的直接工作对象，也是在被测系统中实现特定测评指标所对应的安全功能的具体系统组件，因此，选择测评对象是编制测评方案的必要步骤，也是整个测评工作的重要环节。恰当选择测评对象的种类和数量是整个等级测评工作能够获取足够证据、了解到被测系统的真实安全保护状况的重要保证。

测评对象的确定一般采用抽查的方法，即：抽查信息系统中具有代表性的组件作为测评对象。并且，在测评对象确定任务中应兼顾工作投入与结果产出两者的平衡关系。

在确定测评对象时，需遵循以下原则：

1. 恰当性，选择的设备、软件系统等应能满足相应等级的测评强度要求；
2. 重要性，应抽查对被测系统来说重要的服务器、数据库和网络设备等；
3. 安全性，应抽查对外暴露的网络边界；
4. 共享性，应抽查共享设备和数据交换平台/设备；
5. 代表性，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类型。

B.2 具体确定方法说明

B.2.1 第一级信息系统

第一级信息系统的等级测评，测评对象的种类和数量比较少，重点抽查关键的设备、设施、人员和文档等。可以抽查的测评对象种类主要考虑以下几个方面：

1. 主机房（包括其环境、设备和设施等），如果某一辅机房中放置了服务于整个信息系统或对信息系统的安全性起决定作用的设备、设施，那么也应该作为测评对象；

2. 整个系统的网络拓扑结构；
3. 安全设备，包括防火墙、入侵检测设备、防病毒网关等；
4. 边界网络设备（可能会包含安全设备），包括路由器、防火墙和认证网关等；
5. 对整个信息系统的安全性起决定作用的网络互联设备，如核心交换机、路由器等；
6. 承载最能够代表被测系统使命的业务或数据的核心服务器（包括其操作系统和数据库）；
7. 最能够代表被测系统使命的重要业务应用系统；
8. 信息安全主管人员；
9. 涉及到信息系统安全的主要管理制度和记录，包括进出机房的登记记录、信息系统相关设计验收文档等。

在本级信息系统测评时，信息系统中配置相同的安全设备、边界网络设备、网络互联设备以及服务器应至少抽查一台作为测评对象。

B.2.2 第二级信息系统

第二级信息系统的等级测评，测评对象的种类和数量都较多，重点抽查重要的设备、设施、人员和文档等。可以抽查的测评对象种类主要考虑以下几个方面：

1. 主机房（包括其环境、设备和设施等），如果某一辅机房中放置了服务于整个信息系统或对信息系统的安全性起决定作用的设备、设施，那么也应该作为测评对象；
2. **存储被测系统重要数据的介质的存放环境；**
3. 整个系统的网络拓扑结构；
4. 安全设备，包括防火墙、入侵检测设备、防病毒网关等；
5. 边界网络设备（可能会包含安全设备），包括路由器、防火墙和认证网关等；
6. 对整个信息系统**或其局部的安全性**起决定作用的网络互联设备，如核心交换机、**汇聚层交换机**、核心路由器等；
7. 承载被测系统核心**或重要业务、数据**的服务器（包括其操作系统和数据库）；
8. **重要管理终端**；
9. 能够代表被测系统**主要使命**的业务应用系统；
10. 信息安全主管人员、**各方面的负责人员**；
11. 涉及到信息系统安全的**所有**管理制度和记录。

在本级信息系统测评时，信息系统中配置相同的安全设备、边界网络设备、网络互联设备以及服务器应至少抽查**两台**作为测评对象。

B.2.3 第三级信息系统

第三级信息系统的等级测评，测评对象种类上基本覆盖、数量进行抽样，重点抽查主要的设备、设施、人员和文档等。可以抽查的测评对象种类主要考虑以下几个方面：

1. 主机房（包括其环境、设备和设施等）和**部分辅机房，应将放置了服务于信息系统的局部（包括整体）或对信息系统的局部（包括整体）安全性**起重要作用的设备、设施的辅机房选取作为测评对象；
2. 存储被测系统重要数据的介质的存放环境；
3. **办公场地**；

4. 整个系统的网络拓扑结构；
5. 安全设备，包括防火墙、入侵检测设备和防病毒网关等；
6. 边界网络设备（可能会包含安全设备），包括路由器、防火墙、认证网关和边界接入设备（如楼层交换机）等；
7. 对整个信息系统或其局部的安全性起作用的网络互联设备，如核心交换机、汇聚层交换机、路由器等；
8. 承载被测系统**主要业务或数据的服务器**（包括其操作系统和数据库）；
9. **管理终端和主要业务应用系统终端**；
10. 能够完成被测系统**不同业务使命的业务应用系统**；
11. **业务备份系统**；
12. 信息安全主管人员、各方面的负责人员、**具体负责安全管理的当事人、业务负责人；**
13. 涉及到信息系统安全的所有管理制度和记录。

在本级信息系统测评时，信息系统中配置相同的安全设备、边界网络设备、网络互联设备、服务器、终端以及备份设备，每类应至少抽查两台作为测评对象。

B.2.4 **第四级信息系统**

第四级信息系统的等级测评，测评对象种类上完全覆盖、数量进行抽样，重点抽查不同种类的设备、设施、人员和文档等。可以抽查的测评对象种类主要考虑以下几个方面：

1. 主机房和**全部**辅机房（包括其环境、设备和设施等）；
2. **介质的存放环境**；
3. 办公场地；
4. 整个系统的网络拓扑结构；
5. 安全设备，包括防火墙、入侵检测设备和防病毒网关等；
6. 边界网络设备（可能会包含安全设备），包括路由器、防火墙、认证网关和边界接入设备（如楼层交换机）等；
7. **主要**网络互联设备，包括核心和汇聚层交换机；
8. **主要**服务器（包括其操作系统和数据库）；
9. 管理终端和主要业务应用系统终端；
10. **全部**应用系统；
11. 业务备份系统；
12. 信息安全主管人员、各方面的负责人员、具体负责安全管理的当事人、业务负责人；
13. 涉及到信息系统安全的所有管理制度和记录。

在本级信息系统测评时，信息系统中配置相同的安全设备、边界网络设备、网络互联设备、服务器、终端以及备份设备，每类应至少抽查**三台**作为测评对象。

附录 C

（资料性附录）

等级测评工作要求

C.1 依据标准，遵循原则

等级测评实施应依据等级保护的相关技术标准进行。相关技术标准主要包括GB/T 22239-2008和GB/T DDDD-DDDD，其中等级测评目标和内容应依据GB/T 22239-2008，对具体测评项的测评实施方法则依据GB/T DDDD-DDDD。

在等级测评实施活动中，应遵循GB/T DDDD-DDDD中规定的测评原则，保证测评工作公正、科学、合理和完善。

C.2 恰当选取，保证强度

恰当选取是指对具体测评对象的选择要恰当，既要避免重要的对象、可能存在安全隐患的对象没有被选择，也要避免过多选择，使得工作量增大。

保证强度是指对被测系统应实施与其等级相适应的测评强度。

C.3 规范行为，规避风险

测评机构实施等级测评的过程应规范，包括：制定内部保密制度；制定过程控制制度；规定相关文档评审流程；指定专人负责保管等级测评的归档文件等。

测评人员的行为应规范，包括：测评人员进入现场佩戴工作牌；使用测评专用的电脑和工具；严格按照测评指导书使用规范的测评技术进行测评；准确记录测评证据；不擅自评价测评结果；不将测评结果复制给非测评人员等。

规避风险，是指要充分估计测评可能给被测系统带来的影响，向被测系统运营/使用单位揭示风险，要求其提前采取预防措施进行规避。同时，测评机构也应采取与测评委托单位签署委托测评协议、保密协议、现场测评授权书、要求测评委托单位进行系统备份、规范测评活动、及时与测评委托单位沟通等措施规避风险，尽量避免给被测系统和单位带来影响。

附录 D

（资料性附录）

测评方案与报告编制示例

某公司（简称“AAA”）用电信息系统承载着该公司的电力营销业务，由数据存储、业务处理、接入、对外服务和外联等五个功能区域组成，是一个安全等级为三级的信息系统。

现场测评时间为X年X月X日至X年X月X日，现场测评小组分为管理组（2人）和技术组（4人）两组，分别完成安全管理和安全技术方面的测评。

D.1 测评方案编制示例

针对AAA用电信息系统的实际情况，下面从被测系统描述、测评对象、测评指标、测评工具和接入点、测评内容以及配套的测评指导书等方面说明测评方案的编制方法。

D.1.1 被测系统描述

被测系统为承载着AAA公司电力营销业务，是AAA公司的重要信息系统，其安全等级定为三级（S3A2G3）。

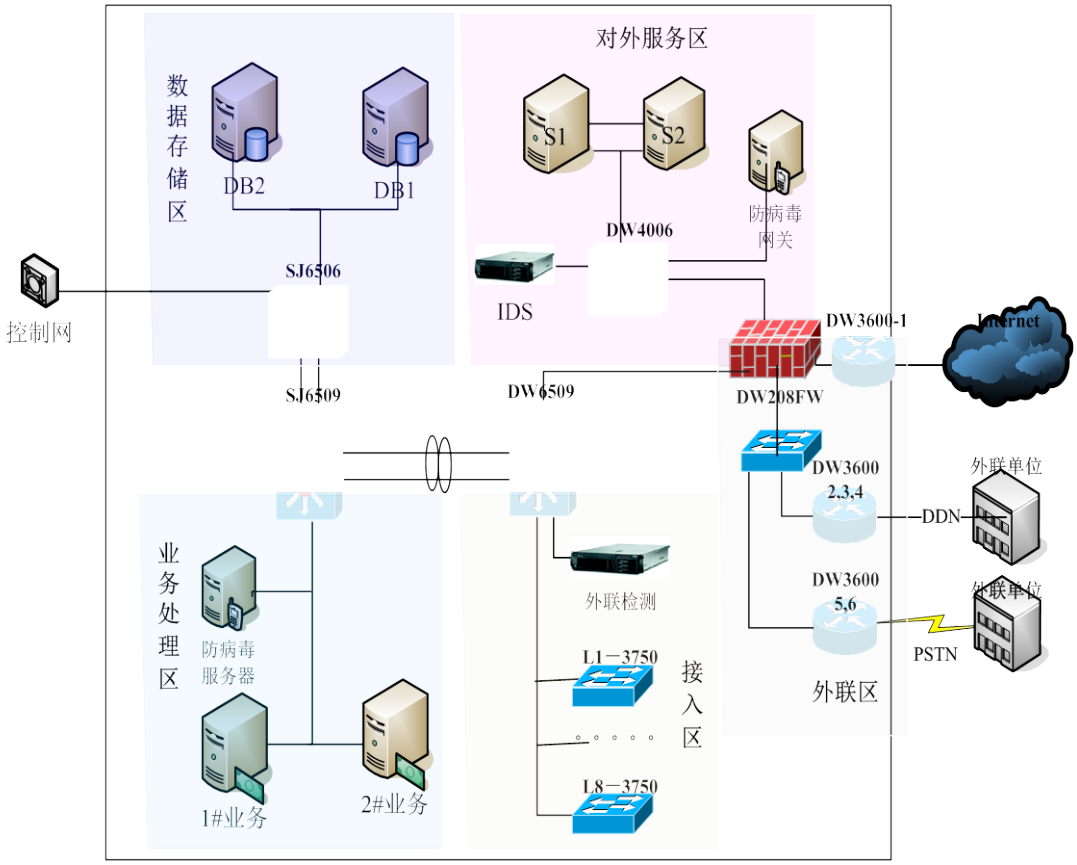

图 6 被测系统网络拓扑结构示意图

被测系统由数据存储、业务处理、接入、对外服务和外联等五个功能区域组成，对内有业务扩充管理、电量计量管理、电费结算、收费、统计分析等业务功能模块；对外有可以为Internet网、大客户单位、拨号用户等提供电费数据查询、交纳、业务扩充、投诉等服务的功能模块。数据存储功能区位于屏蔽机房，其它功能区域位于中心机房。

与被测系统相连的外部连接有Internet、外联单位（包括DDN单位和PSTN用户）和控制网三处。在Internet、外联单位的边界连接处设置了防火墙；与控制网连接是通过交换机SJ6506以共用服务器方式进行的。整个网络拓扑结构示意图如图6所示。

D.1.2 测评对象

根据用电信息系统的实际情况，分别确定物理安全、网络安全、主机安全、应用安全等各层面的测评对象。

a) 物理方面主要是测评屏蔽机房和主机房。

b) 网络方面主要测评的设备有：路由器、交换机、防火墙、IDS、外联检测、防病毒等，如表 11 所示。

表 11 网络设备测评列表

序号	功能区域	设备名称	用 途	设备信息	抽查说明
1	外联区	DW3600（Internet）	外部接入路由器（Internet）	型号：CISCO 3600 IP:	查 1 台
2		DW3600 2,3,4（DDN）	外部接入路由器（DDN）	型号：CISCO 3600 IP:	查 1 台
3		DW3600 5,6（PSTN）	外部接入路由器（PSTN 拨号接入）	型号：CISCO 3600 IP:	查 1 台
4	对外服务区	DW208DW	DW208FW 防火墙，系统内外隔离	型号：NetScreen 208 IP:192.168.32-33/24	查 1 台
5		DW4006	对外服务区交换机	型号：CISCO 4006 IP:	查 1 台
6		IDS	入侵检查设备	型号：启明星辰 IP:	查 1 台
7		防病毒网关	邮件防病毒网关	型号：瑞星 IP:	查 1 台
8	接 入区	DW6509	核心交换机	型号：CISCO 6509 IP:192.168.100.24-25/24	查 1 台
9		L1-3750 到 L8－3750	接入交换机	型号：CISCO 3750 IP:	查 2 台
10		外联检测	非法外联监测设备	型号： IP:	查 1 台
11	业务处理区	SJ6509	核心交换机	型号：CISCO 6509 IP:192.168.100.1-3/24	
12	数据存储区	SJ6506	接入交换机	型号：CISCO 6506 IP: 192.168.100.7-8/24	查 1 台

c） 主机方面主要测评的主机服务器（包括数据库服务器）如表 12 所示。

表 12 主机测评列表（示例）

序号	设备名称	用 途	设备信息	抽查说明
1	S1	对外服务业务逻辑处理	型号：IBM PC 服务器 OS: WIN2003 IP:	查 1 台
2	S2	对外服务网站	型号：IBM PC 服务器 OS: WIN2003 IP:	查 1 台
3	1#业务	用电业务处理中间件	型号：IBM PC 服务器 OS:Linux IP:192.168.1.70	查 1 台
4	DB1（数据库服务器 1）	用电数据存储服务器	型号：IBM 小型机 OS: AIX DB:Sybase IP: IP:192.168.1.10	查 1 台
5	用电业务客户机	运行用电业务客户端程序	型号：DELL PC OS: Win 2000 IP: IP:192.168.10.10	查 2 台
6	……	……	……	

d） 应用方面主要测评的应用系统如表 13 所示。

表 13 应用系统测评列表（示例）

序号	系统名称	系统描述	抽查说明
1	用电应用系统	主要完成的功能包括业务扩充、电量计量、电费计算、查询、统计等业务。涉及到的业务信息包括用户登录权限认证信息、用电业务数据等与电力公司服务业务相关的信息。	抽查
2	对外服务网站系统	……	
……	……	……	

e） 安全管理，主要测评对象为与信息安全管理有关的策略、制度、操作规程、运行记录、管理人员、技术人员和相关设备设施等。

D.1.3 测评指标

被测系统的定级结果为：安全保护等级为3级，业务信息安全等级为S3，系统服务安全等级为A2；则该系统的测评指标应包括GB/T 22239-2008“技术要求”中的3级通用指标类（G3），3级业务信息安全指标类（S3），2级系统服务安全指标类（A2），以及第3级“管理要求”中的所有指标类。本次测评的测评指标情况具体如表14所示。

表 14 测评指标

测评指标					
技术/管理	层面	类数量			
		S 类 (3 级)	A 类 (2 级)	G 类 (3 级)	小计
安全技术	物理安全	1	1	8	10
	网络安全	1	0	6	7
	主机安全	3	1	3	7
	应用安全	5	2	2	9
	数据安全	2	1	0	3
安全管理	安全管理机构	0	0	3	3
	安全管理制度	0	0	5	5
	人员安全管理	0	0	5	5
	系统建设管理	0	0	11	11
	系统运维管理	0	0	13	13
合　　计					73（类）

D.1.4　测评工具和接入点

本次测评的信息系统为3级信息系统，根据3级信息系统的测评强度要求，在测试的广度上，应基本覆盖不同类型的机制，在数量、范围上可以抽样；在测试的深度上，应执行功能测试和渗透测试，功能测试可能涉及机制的功能规范、高级设计和操作规程等文档，渗透测试可能涉及机制的所有可用文档，并试图智取进入信息系统等。因此，对其进行测评，应涉及到漏洞扫描工具、渗透测评工具集等多种测试工具。

针对被测系统的网络边界和测评设备、主机和业务应用系统的情况，需要在被测系统及其互联网络中设置6个测试工具接入点－－接入点JA到JF，如图7所示，“接入点”标注表示进行工具测试时，需要从该接入点接入，对应的箭头路线表示工具测试数据的主要流向示意。

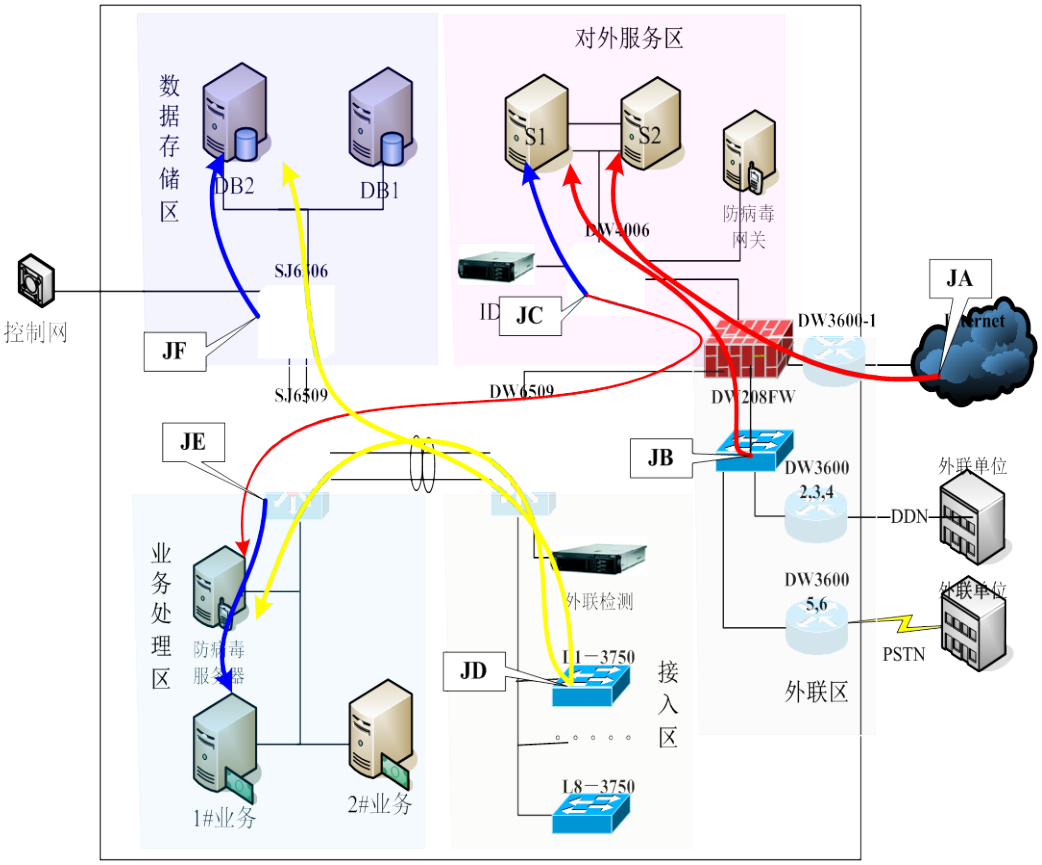

图 7 工具接入示意图

a) 在接入点 JA 接入扫描器，模拟 Internet 用户，探测对外服务功能区上各服务器对 Internet 暴露的安全漏洞情况。并根据漏洞扫描的结果接入渗透测试工具集，试图利用服务器的安全漏洞入侵服务器。

b) 在接入点 JB 接入扫描器，模拟外联单位，探测对外服务功能区上各服务器对外联单位暴露的安全漏洞情况。并根据漏洞扫描的结果接入渗透测试工具集，试图利用服务器的安全漏洞入侵服务器。

c) 在接入点 JC 接入扫描器，直接测试对外服务功能区上各服务器对网络暴露的安全漏洞情况。同时，试图穿过防火墙，探测业务处理功能区上各服务器对外暴露的安全漏洞情况。并根据漏洞扫描的结果接入渗透测试工具集，试图利用业务处理功能区上各服务器的安全漏洞入侵服务器。

d) ……

D.1.5 测评内容

本次测评的单项测评从技术上的物理安全、网络安全、主机系统安全、应用安全和数据安全五个层面和管理上的安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等五个方面分别进行。

a) 物理安全

物理安全测评将通过访谈、文档审查和实地察看的方式测评信息系统的物理安全保障情况。主要涉及对象为屏蔽机房和主机房。

在内容上，物理安全层面测评实施过程涉及10个测评单元，具体如表15所示：

表 15 物理安全单元测评实施内容（示例）

序号	测评指标	测评内容描述
1	物理位置的选择	通过访谈物理安全负责人，检查屏蔽机房和主机房等过程，测评屏蔽机房和主机房等信息系统物理场所在位置上是否具有防震、防风和防雨等多方面的安全防范能力。
2	物理访问控制	通过访谈物理安全负责人，检查屏蔽机房和主机房出入口、机房分区域情况等过程，测评信息系统在物理访问控制方面的安全防范能力。
……	……	……

b） 网络安全

网络安全测评将通过访谈、配置检查和工具测试的方式测评信息系统的网络安全保障情况。主要涉及对象为网络互联设备、网络安全设备和网络拓扑结构等三大类对象。

在内容上，网络安全层面测评实施过程涉及7个测评单元，具体如表16所示：

表 16 网络安全单元测评实施内容（示例）

序号	测评指标	测评内容描述
1	网络结构安全与网段划分	通过访谈网络管理员，检查网络拓扑情况、测评核心交换机 DW6509、接入路由器 DW3600 等网络互联设备，测试系统访问路径和网络带宽分配情况等过程，测评分析网络架构与网段划分、隔离等情况的合理性和有效性。
2	网络访问控制	通过访谈安全员，检查防火墙 DW208DW、接入路由器 DW3600、核心交换机 DW6509、SJ6509 等访问控制设备，测试系统对外暴露安全漏洞情况等过程，测评分析信息系统对网络区域边界相关的网络隔离与访问控制能力。
……	……	……

c） 主机系统安全

主机系统安全测评将通过访谈、配置检查和工具测试的方式测评信息系统的主机安全保障情况。本次重点测评的操作系统包括各网站服务器、应用服务器和数据库服务器等的操作系统，数据库管理系统为数据库服务器Sybase。

在内容上，主机系统安全层面测评实施过程涉及7个测评单元，具体如表17所示。

表 17 主机系统安全单元测评实施内容（示例）

序号	测评指标	测评内容描述
1	身份鉴别	对各主机服务器和终端设备相应操作系统或数据库的身份鉴别情况进行配置检查，测评分析被测系统主机的身份鉴别能力。
2	访问控制	检查各主机服务器和终端设备相应操作系统或数据库的访问控制设置情况，包括安全策略覆盖、控制粒度以及权限设置情况等，测评分析被测系统主机的访问控制能力。
……	……	……

d） 应用安全

应用安全测评将通过访谈、配置检查和工具测试的方式测评信息系统的应用安全保障情况，主要涉及对象为用电信息系统、对外服务网站系统和远程客户服务系统。

在内容上，应用安全层面测评实施过程涉及9个测评单元，具体如表18所示。

表 18 应用安全单元测评实施内容（示例）

序号	测评指标	测评内容描述
1	身份鉴别	检查业务应用系统的身份标识与鉴别功能设置和使用配置情况； 检查业务应用系统对用户登录各种情况的处理，如登录失败处理、登录连接超时等。
2	访问控制	检查业务应用系统的访问控制功能设置情况，如访问控制的策略、访问控制粒度、权限设置情况等。
……	……	……

e） 数据安全

数据安全测评将通过访谈、配置检查的方式测评信息系统的数据安全保障情况，主要涉及对象为信息系统的管理数据及业务数据等。

在内容上，数据安全层面测评实施过程涉及3个测评单元，具体如表19所示。

表 19 数据安全单元测评实施内容（示例）

序号	测评指标	测评内容描述
1	数据完整性	检查信息系统的数据完整性保护情况，包括传输完整性、存储完整性保护措施等；
2	数据保密性	检查信息系统的数据保密性保护情况，包括传输保密性和存储保密性保护措施等。
3	备份和恢复	数据的备份情况，包括软、硬件方面的支持情况等。

f） 安全管理部分

安全管理部分为全局性问题，涉及安全管理制度、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等五个方面。其中，安全管理制度测评实施过程涉及3个测评单元，安全管理机构测评实施过程涉及5个测评单元，人员安全管理测评实施过程涉及5个测评单元，系统建设管理测评实施过程涉及11个测评单元，系统运维管理测评实施过程涉及13个测评单元等。由于管理部分的测评内容在描述时差异不大，这里以安全管理制度部分为例说明。

安全管理制度方面的测评对象主要为安全主管人员、安全管理人员等，具体如表20所示。

表 20 安全管理制度单元测评实施内容（示例）

序号	测评指标	测评内容描述
1	管理制度	通过访谈安全主管，检查有关管理制度体系文档等过程，测评管理制度体系在内容覆盖上是否全面、完善。
2	制定与发布	通过访谈安全主管，检查有关制度制定要求文档等过程，测评管理制度的制定和发布过程是否遵循一定的流程。
3	评审和修订	通过访谈安全主管，检查管理制度评审记录等过程，测评管理制度定期评审和修订情况。

D.1.6 测评指导书

下面从被测系统的物理安全、网络安全、主机安全、应用安全等技术部分和安全管理部分分别举例说明测评指导书的格式和开发方法。

a） 物理安全

按照方案的要求，物理安全应测评物理位置选择（G3）、物理访问控制（G3）、防盗窃和防破坏（G3）、防雷击（G3）、防水和防潮（G3）、防静电（G3）、温湿度控制（G3）、电力供应（A2）和电磁防护（S3）等。在GB/T 22239-2008中找到对应等级项目的要求，然后在GB/T DDDD-DDDD中找到相应的测评方法。如：对于温湿度控制（G3），在GB/T 22239-2008中的描述为“机房应设置温、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。”，按照该要求在GB/T DDDD-DDDD的第三级中找到对应测评方法，然后按照该方法开发出对应的预期结果。

按照上述思路，对于“温湿度控制（G3）”可以开发出如下的测评指导书。

【测评项】

机房应设置温、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。

【测评实施过程】

1. 应访谈物理安全负责人，询问机房是否配备了温、湿度自动调节设施，保证温湿度能够满足计算机设备运行的要求，是否在机房管理制度中规定了温湿度控制的要求，是否有人负责此项工作；
2. 应访谈机房维护人员，询问是否定期检查和维护机房的温湿度自动调节设施，询问是否出现过温湿度影响系统运行的事件；
3. 应检查机房是否有温湿度控制设计/验收文档，是否能够满足系统运行需要，是否与当前实际情况相符合；
4. 应检查温、湿度自动调节设施是否能够正常运行，查看温湿度记录、运行记录和维护记录；查看机房温、湿度是否满足GB 2887-89《计算站场地技术条件》的要求。

【预期结果】

1. 执行步骤1)，机房配备了温、湿度自动调节设施，在机房管理制度中规定了温湿度

控制的要求，有人负责此项工作；

2. 执行步骤2)，定期检查和维护机房的温湿度自动调节设施，没有出现过温湿度影响系统运行的事件；
3. 执行步骤3)，有温湿度控制设计/验收文档，能够满足系统运行需要，与当前实际情况相符合；
4. 温、湿度自动调节设施能够正常运行，机房温、湿度满足GB 2887-89《计算站场地技术条件》的要求。

b） 网络安全

按照测评方案的要求，核心交换机SJ6509应测评网络访问控制（G3）、网络安全审计（G3）、网络设备防护（G3）等部分的内容。在GB/T 22239-2008中找到对应等级项目的要求，然后在GB/T DDDD-DDDD中找到相应的测评方法。如：对于网络设备防护（G3），在GB/T 22239-2008中的描述之一为“应对网络设备的管理员登录地址进行限制”，按照该项要求找到对应测评实施（方法），然后开发出对应的操作步骤和预期结果即可。

按照上述思路，对于“网络设备防护（G3）” 的一个测评项可以开发如下的测评指导书。

【测评项】

应对网络设备的管理员登录地址进行限制。

【测评实施过程】

1. 应检查边界和主要网络设备上的安全设置，查看是否对边界和主要网络设备的管理员登录地址进行限制；
2. 应测试边界和主要网络设备的安全设置，对网络设备的管理员登录地址进行限制（如使用任意地址登录，观察网络设备的动作等）等功能是否有效。

【操作步骤】

1. 执行命令：show ip permit，查看IP地址限定情况；
2. 在业务处理功能区中，用主机192.168.1.3（限制的IP地址）试图登录SJ6509的管理界面，查看是否成功。

【预期结果】

1. 执行步骤1)，系统对管理IP地址进行了限定；
2. 执行步骤2)，192.168.1.3登录SJ6509的管理界面失败。

c） 主机安全

按照方案的要求，DB2（数据库为Sybase）应测评身份鉴别（S3）、自主访问控制（S3）、强制访问控制（S3）、安全审计（G3）、资源控制（A2）、数据备份与恢复（A2）、数据完整性（S3）、数据保密性（S3）等部分的内容。在GB/T 22239-2008中找到对应等级项目的要求，然后在GB/T DDDD-DDDD中找到相应的测评方法。如：对于身份鉴别（S3），在测评项中的描述之一为“应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别”，按照该项要求找到对应测评实施方法，然后开发对应操作步骤和预期结果。

按照上述思路，对于“身份鉴别（S3）”的一个测评项可以开发如下的测评指导书。

【测评项】

应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。

【测评实施过程】

应检查主要数据库管理系统，查看对管理用户的身份鉴别是否采用两个及两个以上鉴别技术的组合来进行身份鉴别（如采用用户名/口令、挑战应答、动态口令、物理设备、生物识别技术和数字证书方式的身份鉴别技术中的任意两个组合）。

【操作步骤】

1. 在DB2主机上执行命令：select * from syslogins，查看是否有用户存在空口令；
2. 询问数据库管理员，除使用口令鉴别外是否采用其他的鉴别方式，如果有，则检查其是否有效。

【预期结果】

1. 执行步骤1)，数据库没有空口令用户，从而说明数据库管理系统采用口令鉴别方式；
2. 执行步骤2)，数据库管理系统还采取有其他的鉴别方式，并且有效。

d） 应用安全和数据安全

按照方案的要求，业务应用程序（用户自主开发）应测评身份鉴别（S3）、访问控制（S3）、安全审计（G3）、剩余信息保护（G3）、通信完整性（S3）、通信保密性（S3）、抗抵赖（S3）、软件容错（A3）、资源控制（A3）、数据备份与恢复（A3）、数据完整性（S3）、数据保密性（S3）等部分的内容。在GB/T 22239-2008中找到对应等级项目的要求，然后在GB/T DDDD-DDDD中找到相应的测评方法。如：对于通信保密性（S3），在测评项中的描述之一为“应对通信过程中的整个报文或会话过程进行加密。”，按照该项要求找到对应测评实施方法，然后开发出对应操作步骤和预期结果。

按照上述思路，对于“通信保密性（S3）”的一个测评项可以开发如下的测试用例。

【测评项】

应对通信过程中的整个报文或会话过程进行加密。

【测评实施过程】

1. 应访谈安全管理员，询问业务系统数据在通信过程中是否采取保密措施，具体措施有哪些；
2. 应测试主要应用系统，通过查看通信双方数据包的内容，查看系统在通信过程中，对整个报文或会话过程进行加密的功能是否有效。

【操作步骤】

1. 应访谈安全管理员，询问业务系统数据在通信过程中是否采取保密措施，具体措施有哪些；
2. 应采用协议分析工具测试应用系统，通过查看通信双方数据包的内容，查看系统在通信过程中，是否对整个报文或会话过程进行加密，加密功能是否有效。

【预期结果】

1. 执行步骤1)，业务系统采用了保密措施，且能具体说明保密措施；
2. 执行步骤2)，协议分析工具看到的数据包进行了加密，且加密方法符合国家规定，时有效的。

e） 管理安全

管理安全部分在测评时可以按照GB/T DDDD-DDDD中介绍的测评实施过程在现场直接实施使用。对于系统运维管理中的密码管理“应建立密码使用管理制度，使用符合国家密码管理规定的密码技术和产品”的要求可以编制如下的测评指导书。

【测评项】

应建立密码使用管理制度，使用符合国家密码管理规定的密码技术和产品。

【测评实施过程】

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

【预期结果】

1. 执行步骤1)，密码技术和产品的使用遵照国家密码管理规定；
2. 执行步骤2)，有密码使用管理制度。

D.2 测评报告编制示例

等级测评报告一般包括：概述、被测系统描述、测评对象说明、测评指标说明、测评内容和方法说明、单元测评的结果记录及结果汇总、整体测评、测评结果汇总、风险分析和评价、等级测评结论、整改建议等内容。下面主要举例说明整体测评和整改建议这两部分内容。

D.2.1 整体测评

a） 物理层面

1. 由于屏蔽机房位于主机房内部，其唯一出口也在主机房内，因此，对其物理层面的安全要求中的物理访问控制、防盗窃和防破坏的测评项可以通过关联互补关系得到补充。
2. ……

综合以上测评分析过程，可以得到如表21物理层面的整体测评结果（安全控制间、层面间和区域间）：

表 21 物理层面整体测评结果

序号	安全控制	测评对象	单项判定不符合项	能否进行关联互补	说明
1	物理位置的选择	屏蔽机房	－－		
		主机房	－－		
2	物理访问控制	屏蔽机房	a）b)c)	能	屏蔽机房位于主机房内部
		主机房	－－		
3	防盗窃和防破坏	屏蔽机房	a）f)g)	能	
		主机房	－－		
……	……	……	……	……	……
项 目 小 计					

b） 网络层面

1. 外联功能区拨号路由器DW3600上基本没有直接采取较好的拨号访问控制措施，只是对用户进行了固定IP地址分配。但是，由于在防火墙DW208FW上，严格限定了拨号接入IP地址的用户的访问范围，从而可以弥补这部分功能。
2. 外联功能区的6台路由器DW3600在网络设备防护的用户身份认证方面，存在口令不强、未限制管理员登录地址等方面问题，但是，由于这些设备都没有开放网络管理（TELNET/HTTP等），全部采取通过本地串口方式来管理，而其又是存放在主机房中，因此，其网络设备防护安全控制可以通过物理的相关措施（物理访问控制、防盗窃和防破坏等）得到增强。
3. 对外服务功能区的网络安全审计功能没有采取单独的设备来完成，其网络流量、用户行为等的监测、记录功能是通过网络入侵防范安全控制的IDS来协助完成的。
4. 网络安全审计设备IDS具有对部分病毒、蠕虫攻击的检测识别能力，可以部分弥补恶意代码防范功能，因为，防病毒网关只对邮件数据进行病毒过滤。
5. …….

综合以上测评分析过程，可以得到如表22的测评结果：

表 22 网络层面整体测评结果

序号	安全控制	测评对象	单项判定不符合项	能否进行关联互补	说明
1	网络结构安全与网段划分	网络拓扑图	－－		
2	网络访问控制	防火墙 208	－－		
		核心交换机 C6509	－－		
3	拨号访问控制	拨号路由器 DW3600	a）c)	能	
4	网络安全审计				
……	……	……	……	……	……
8	网络设备防护	路由器 DW3600 1,2,3,4,5,6	e)f)g)	能	
项目小计					

c） 系统结构测评分析

在信息系统整体结构的安全性方面，从被测系统的网络拓扑结构示意图来看，该网络系统虽然有多处相对独立的出口，但是这些出口除到控制网外的连线都集中到防火墙DW208FW，因此，从在网络结构上，不存在出口过多的问题；对外服务功能区上防病毒服务器a（拓扑图上未标出）使用双网卡方式工作，一边连接内部网络，一边连接对外服务功能区，通过防火墙DW208FW上网升级，这在安全上是不可取的，外部用户一旦控制防病毒服务器a，则可通过双网卡直接进入信息系统的内部网络功能区域，对信息系统的安全构成严重威胁。

从被测系统的网络拓扑结构示意图来看，内部网络划分了多个功能区域，这些功能区域之间采取了网络访问控制措施，即使是内网用户也只能访问到应用处理功能区上的服务器主机，而不能直接访问数据存储功能区的数据库服务器。这种保护方法符合纵深防御的要求，重点突出，能较好地解决一些安全问题。

D.2.2 整改建议

a) 安全建议（网络安全部分）

1. 主要问题

- 没有绘制与实际网络相一致的网络拓扑结构图。有一份与实际网络相一致的网络拓扑结构图对网络管理相当重要，可以方便工作人员掌握网络的整体情况，便于网络故障的排除，便于网络安全设备的策略配置等；
- 没有对重要网段采取网络层地址与数据链路层地址绑定措施。进行 MAC 地址和 IP 地址的绑定，有助于防止地址欺骗。

2. 立即整改

需要立即整改的安全建议如下：

- 应根据当前运行的网络拓扑情况，绘制与实际网络相一致的网络拓扑结构图，以便于工作人员掌握网络结构的整体情况；

3. 持续改进

需要持续改进的建议如下：

- 对重要网段采取网络层地址与数据链路层地址绑定措施，防止地址欺骗；
- 购置并在适当网段部署防病毒网关。

b) 安全管理方面

1. 主要问题

- 与安全管理制度相配套的总体信息安全策略还没有正式制定，且有部分管理制度没有制定，如工程实施安全管理制度等。总体性安全策略文件是整个机构开展信息安全工作的纲领，对机构近期和远期的安全规划起着重要的指导作用。没有方针性文件的指引和统一规划，机构的信息安全工作则会有工作方向不明确的问题；
- 对信息安全关键岗位的人员管理缺乏更细粒度的要求。没有明确对这些岗位的人员是否有区别于其他岗位的更严格的录用要求、日常信用审查等管理要求。关键岗位所从事的工作是信息安全工作的重中之重，加强对这些岗位人员的管理，对做好信息安全工作起到了关键的作用。

2. 改进建议

- 进一步完善安全管理文件体系，尽快制定信息安全总体政策、方针文件，并进一步补充、完善、细化各类管理制度，如工程安全实施管理制度、系统交付管理制度等，从而形成高层策略文件、各类管理制度、具体操作规程和各类操作记录等四层塔式管理文件体系；
- 加强对关键岗位人员（如系统管理员、网络管理员、安全管理员）的管理，定期对其进行信用审查，并要求其签署岗位安全协议，使其承诺在岗位上的具体安全责任、工作职责以及保密义务,从而保证对关键岗位进行关键管理。

参考文献

[1] NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems-2001.10

[2] NIST Special Publication 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems-2004.5

[3] NIST Special Publication 800-53 Revision 1 Recommended Security Controls for Federal Information Systems-2006.12

[4] NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems-2007.6

[5] Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual (DoD 8510.1-M)

[6] OCTAVE Method Implementation Guide v2.0

[7] 《信息安全等级保护管理办法》（公通字[2007]43 号）