

YDB

中 国 通 信 标 准 化 协 会 标 准

YDB 111—2012

增值电信业务系统安全防护定级和评测 实施规范 搜索系统

Implementation Specification of Classified Security Protection and Testing for
Value-added Telecommunication Service System Search System

2012 – 11 – 13 印发

中国通信标准化协会

目 次

前言	II
1 范围	1
2 规范性引用文件	1
3 术语、定义和缩略语	1
3.1 术语和定义	1
3.2 缩略语	2
4 概述	2
4.1 安全防护范围	2
4.2 安全风险分析	3
4.3 安全防护内容	5
5 定级实施规范	6
5.1 安全等级划分	6
5.2 定级要素	7
5.3 安全等级的计算方法	8
6 安全防护要求	9
6.1 第1级要求	9
6.2 第2级要求	9
6.3 第3.1级要求	21
6.4 第3.2级要求	31
6.5 第4级要求	31
6.6 第5级要求	31
7 安全防护评测实施指南	31
7.1 第1级要求	31
7.2 第2级要求	32
7.3 第3.1级要求	48
7.4 第3.2级要求	61
7.5 第4级要求	61
7.6 第5级要求	61

前 言

本实施规范是“增值电信业务系统安全防护定级和评测实施规范”系列实施规范之一，该系列实施规范包含如下实施规范：

- 增值电信业务系统安全防护定级和评测实施规范 门户综合网站系统；
- 增值电信业务系统安全防护定级和评测实施规范 即时通信系统；
- 增值电信业务系统安全防护定级和评测实施规范 网络交易系统；
- 增值电信业务系统安全防护定级和评测实施规范 信息社区服务系统；
- 增值电信业务系统安全防护定级和评测实施规范 邮件系统；
- 增值电信业务系统安全防护定级和评测实施规范 搜索系统；
- 增值电信业务系统安全防护定级和评测实施规范 互联网接入服务系统。

本实施规范按照GB/T1.1-2009给出的规则起草。

为适应信息通信业发展对通信标准文件的需要，由中国通信标准化协会组织制定“中国通信标准化协会标准”，推荐有关方面参考采用。有关对本实施规范的建议和意见，向中国通信标准化协会反映。

本实施规范由中国通信标准化协会提出并归口。

本实施规范起草单位：工业和信息化部电信研究院。

本实施规范主要起草人：何友斌、黄晨、鲁冬雪、魏薇、邓东丰、封莎。

增值电信业务系统安全防护定级和评测实施规范 搜索系统

1 范围

本实施规范规定了搜索系统开展网络安全防护有关系统定级、分等级防护和安全评测等方面的规范性要求。

本实施规范适用于增值电信企业运营的搜索系统。

2 规范性引用文件

下列文件对于本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）适用于本文件。

YD 5098-2005	通信局(站)防雷与接地工程设计规范
YD 5002	邮电建筑防火设计标准
YD/T 5026-2005	电信机房铁架安装设计标准

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本实施规范。

3.1.1

搜索系统安全等级 security classification of search system

搜索系统重要程度的表征。重要程度从搜索系统受到破坏后，对国家安全、社会秩序、经济运行、公共利益造成的损害来衡量。

3.1.2

搜索系统安全等级保护 classified security protection of search system

对搜索系统分等级实施安全保护。

3.1.3

搜索系统安全风险 security risk of search system

人为或自然的威胁可能利用搜索系统中存在的脆弱性导致安全事件的发生及造成的影响。

3.1.4

搜索系统资产 asset of search system

搜索系统中具有价值的资源，是安全防护体系保护的對象。搜索系统中的资产可能以多种形式存在，无形的、有形的、硬件、软件，包括物理布局、通信设备、物理线路、数据、软件、文档、规程、业务、人员、管理等各种类型的资源，如数据检索、展现等相关服务器。

3.1.5

YDB 111—2012

搜索系统威胁 threat of search system

可能导致对搜索系统产生危害的不希望事故潜在起因，它可能是人为的，也可能是非人为的；可能是无意失误，也可能是恶意攻击。

3.1.6

搜索系统脆弱性 vulnerability of search system

搜索系统的资产中存在的弱点、缺陷与不足，不直接对搜索系统资产造成危害，但可能被搜索系统威胁所利用从而危害搜索系统资产的安全。

3.1.7

搜索系统灾难 disaster of search system

由于各种原因，造成搜索系统故障或瘫痪，使搜索系统数据检索、展现等业务功能停顿或服务水平不可接受、达到特定的时间的突发性事件。

3.1.8

搜索系统灾后备份 backup for disaster recovery of search system

为了搜索系统灾难恢复而对相关要素进行备份的过程。

3.1.9

搜索系统灾难恢复 disaster recovery of search system

为了将搜索系统从灾难造成的故障或瘫痪状态恢复到正常运行状态或部分正常运行状态、并将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态，而设计的活动和流程。

3.1.10

搜索系统安全评测 security testing of search system

对搜索系统的安全保护能力是否达到相应安全等级的安全防护要求进行衡量。

3.2 缩略语

下列缩略语适用于本实施规范。

CVE	Common Vulnerabilities & Exposures	通用漏洞披露
CVND	China National Vulnerability Database	国家信息安全漏洞库
DDoS	Distributed Denial of Service	分布式拒绝服务
DoS	Denial of Service	拒绝服务
IP	Internet Protocol	互联网协议
ID	Identity	身份标识
TCP	Transmission Control Protocol	传输控制协议
URL	Universal Resource Locator	网页地址
UDP	User Datagram Protocol	用户数据报协议

4 概述

4.1 安全防护范围

搜索系统是指根据一定的策略，运用特定的计算机程序从互联网上搜集信息，在对信息进行组织和处理后，为用户提供信息检索服务，并将用户检索的相关信息(网页、音视频、新闻等)展示给用户的系统。

搜索系统的核心功能模块通常包括：

- a) 前端模块：为互联网用户提供前端接入和结果浏览的功能；
- b) 数据索引模块：为互联网用户提供数据索引、搜索的功能；
- c) 内容抓取模块：用于检索和抓取互联网数据；
- d) 数据存储模块：用于存储搜索系统从互联网搜索的关键词、URL 等结果索引数据；
- e) 对外能力接口模块：用于实现与第三方合作系统的认证授权及数据索引与检索功能。

搜索系统功能架构如图1所示。

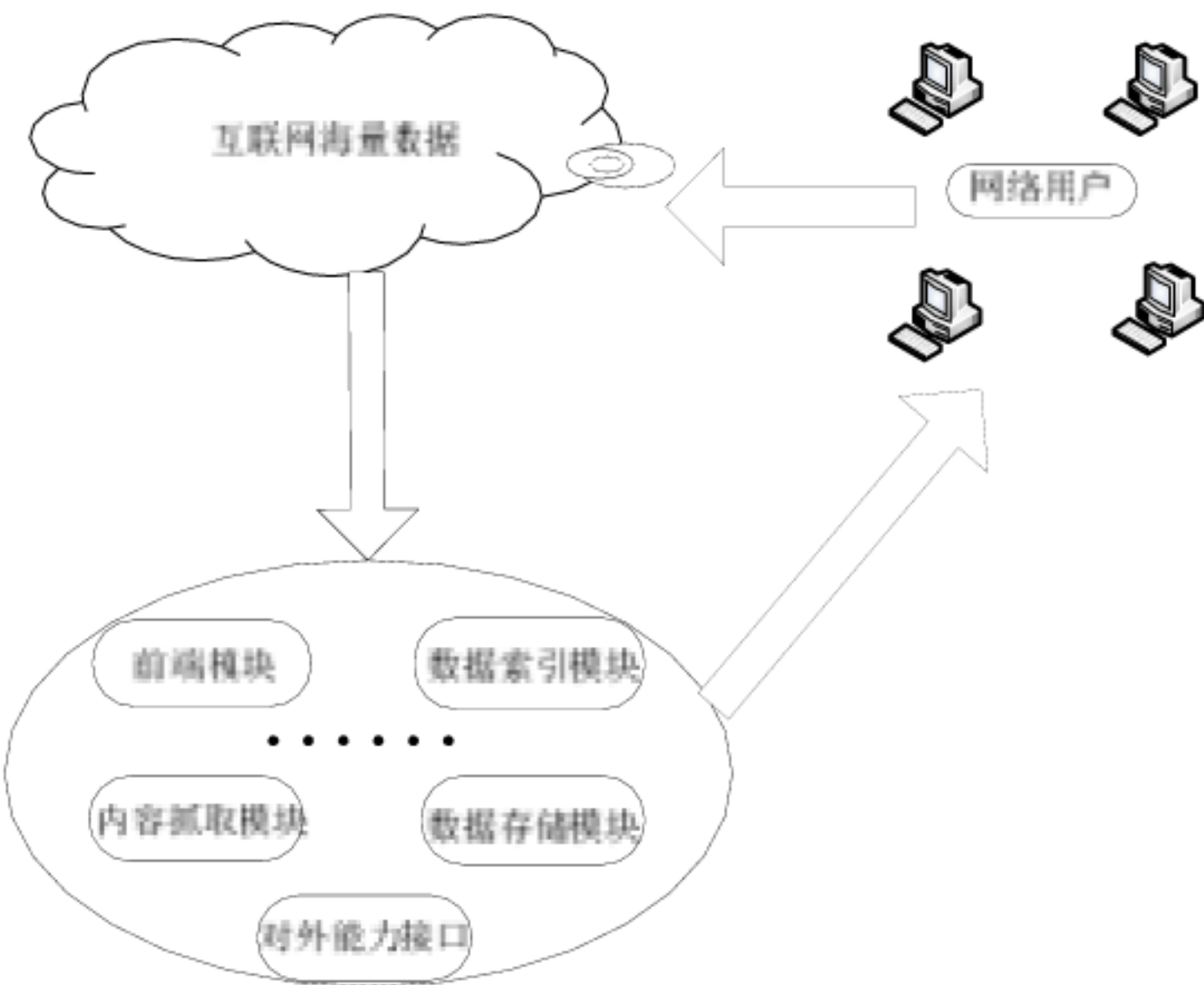


图1 搜索系统功能架构图

4.2 安全风险分析

搜索系统的重要资产至少应包括：

- a) 搜索系统及操作维护终端：如前端模块、数据索引模块、数据存储模块、内容抓取模块和对外能力接口模块涉及的服务器、数据库和操作维护终端；系统内部网络设备(如系统内部组网路由器、交换机等设备)、系统内部链路等；
- b) 搜索业务关键数据：如搜索结果页（网页标题、网页链接、文字摘要、网页缓存链接等）、搜索业务系统服务器的后台管理账户、口令等。

搜索系统相关代表性资产的类别划分如表1所示。

表1 资产类别

类别	主要资产
设备及链路	前端模块、数据索引模块、数据存储模块和内容抓取模块等涉及的操作维护终端、服务器和数据库，系统内部网络设备（如系统内部组网路由器、交换机等设备）、系统内部链路。
软件	数据库软件、中间件、业务控制和运维管理软件等。
数据和信息	搜索结果页数据（网页标题、网页链接、文字摘要、网页缓存链接等）、搜索系统服务器管理账户、口令等。
文档和资料	纸质以及保存在存储介质中的各种文件资料（如设计文档、技术要求、管理规定、工作计划、技术报告、用户手册等）。
人员	相关管理、维护、开发、数据备份人员等。
环境和设施	业务系统和设备所处的物理环境，机房、电力、防火、防水、防静电、温湿度控制等相关设施。

对于搜索系统而言，正确向用户展现搜索结果页（网页标题、网页链接、文字摘要、网页缓存链接等）尤为重要。因此，搜索系统前端模块、数据索引模块、数据存储模块、内容抓取模块和对外能力接口模块的功能实现、部署、配置、管理等环节对实现搜索功能起了直接决定性的作用。

搜索系统面临来自公众互联网和内部网络的各种安全威胁，包括黑客发起DDoS攻击服务器或者篡改、重定向搜索结果页，内部人员操作失误等。由此，搜索系统任何可能存在的安全脆弱性被利用后会产生很大的安全风险，例如：服务器安全措施不到位，可能被DoS或DDoS攻击，进而影响对用户提供服务；系统部署防入侵防攻击措施不到位，攻击者可能从外网渗透进内网系统，篡改向用户展示的搜索结果页；系统数据配置操作失误，配置审计、保护措施不到位，可导致搜索结果页被篡改；监控系统覆盖范围不够，无法及时发现和处理安全事件，或者内部人员利用提权漏洞篡改监控数据；用户信息保护措施不到位，可从外网窃取内网用户敏感信息；对可能包含恶意代码的检索结果进行监测和过滤的机制不完善，可导致恶意代码大量传播。搜索系统存在的安全脆弱性可能对搜索结果页展示、正常业务功能提供构成安全威胁，甚至进一步威胁基础网络和互联网用户终端的安全。

搜索系统的脆弱性包括技术脆弱性和管理脆弱性两个方面，脆弱性识别对象应以资产为核心。搜索系统的脆弱性分析应包括但不限于表2所列范围。

表2 脆弱性类别

类别	对象	主要脆弱性
技术脆弱性	业务及应用	相关服务器未进行合理备份，重要数据未及时进行备份； 相关业务存在漏洞，相关服务器的应用代码存在漏洞、后门； 相关服务器存在过多不必要的开放端口； 相关服务器配置不合理，访问控制策略设置不合理； 相关服务器的日志功能没有启用或日志记录不完整； 系统规划、设备部署、链路部署、资源配置、业务保护和恢复能力、安全技术措施和策略等方面的缺陷。
	设备	相关设备存在硬件隐患或质量问题； 相关设备的操作系统存在安全隐患； 相关口令设置不合理、复杂度不够或没有定期更新； 设备重要部件未进行合理冗余； 相关设备超过使用年限或核心部件老化； 相关设备发生故障后未及时告警。
	物理环境	机房场地选择不合理； 防火、供配电、防静电、接地与防雷、电磁防护、温湿度控制不符合规范； 通信线路、相关服务器、主机等设备的保护不符合规范。
管理脆弱性		安全管理机构方面：岗位设置不合理（如人员配置过少、职责不清）、授权和审批程序简化、沟通和合作未执行、审核和检查未执行等； 安全管理制度方面：管理制度不完善、制度评审和修订不及时等； 人员安全管理方面：人员录用不符合程序、人员离岗未办理安全手续、人员未进行安全培训、对于第三方人员未进行限制访问等； 建设管理方面：安全方案不完善、软件开发不符合程序、工程实施未进行安全验收或验收不严格等； 运维管理方面：物理环境管理措施简单、存储介质使用不受限、设备没有定期维护、厂家支持力度不够、关键性能指标没有定期监控、无恶意代码防范措施、无数据备份和恢复策略、访问控制不严格、操作管理不规范等，应急保障措施不到位，灾难恢复预案不完善。

搜索系统的威胁根据来源可分为技术威胁、环境威胁和人为威胁。环境威胁包括自然界不可抗的威胁和其他物理威胁。根据威胁的动机，人为威胁又可分为恶意和非恶意两种。搜索系统的威胁分析应包括但不限于表3所列范围。

表3 威胁类别

类别		主要威胁
环境威胁	物理环境	断电、静电、灰尘、潮湿、温湿度异常、电磁干扰等；意外事故或通讯线路方面的故障。
	自然灾害	鼠蚁虫害、洪灾、火灾、泥石流、山体滑坡、地震、台风、雷击。
人为威胁	恶意人员	不满的或有预谋的内部人员滥用权限进行恶意破坏；攻击者利用非法手段进入机房内部盗窃、破坏、篡改源站内容，攻击者非法物理访问相关设备、存储介质等；攻击者利用网络协议、操作系统、应用系统漏洞，越权访问相关设备的文件、数据或其他资源；攻击者利用各种工具获取相关设备身份鉴别数据，并对鉴别数据进行分析和解剖，获得鉴别信息，未授权访问应用系统，或非法使用相关文件和数据；攻击者利用应用系统扩散病毒、蠕虫，利用相关攻击工具恶意消耗应用系统资源（如发动DDoS攻击），导致系统能力下降或瘫痪、无法正常提供应用服务；攻击者截获数据，进行篡改、插入，并重发，造成数据的完整性、真实性丧失。
	非恶意人员	内部人员由于缺乏责任心或者无作为，应该执行而没有执行相应的操作、或无意地执行了错误或危险的操作导致安全事件；内部人员没有遵循规章制度和操作流程而导致故障或信息损坏；内部人员由于缺乏培训、专业技能不足、不具备岗位技能要求而导致故障或攻击；安全管理制度不完善、落实不到位造成安全管理不规范或者管理混乱导致安全事件；内部人员由于安全检查不及时不到位导致系统主机（如服务器、系统网络设备）使用时间过长或质量问题等导致硬件故障，系统链路发生故障，相关设备的操作系统软件、应用软件运行故障，相关设备数据丢失或系统运行中断，存储介质老化或质量问题等导致不可用，系统不能正常运行。

4.3 安全防护内容

搜索系统的主要功能是为公众互联网提供信息内容搜索的信息系统，因此保障其搜索数据安全，防止搜索结果页被恶意篡改至关重要。保障搜索系统基础设施安全、管理安全等也是安全防护的重要内容。

4.3.1 业务及应用安全

业务及应用安全包括身份鉴别、访问控制、安全审计、数据安全、资源控制、信息保护、web安全防护、对外能力接口、恶意代码防范等方面安全要求。

4.3.2 网络安全

网络安全包括网络结构安全、入侵防范、安全审计等方面安全要求。

4.3.3 设备及软件系统安全

YDB 111—2012

设备及软件系统安全包括网络及安全设备、通用主机操作系统、数据库、中间件等方面安全要求。

4.3.4 物理环境安全

物理环境安全包括物理机房位置、物理机房访问控制、物理机房安全防护措施等方面的安全要求。

4.3.5 管理安全

管理安全包括管理制度、机构、人员等方面的安全要求。

5 定级实施规范

5.1 安全等级划分

搜索系统进行安全等级划分的总体原则是：依据定级对象受到破坏后对国家安全、社会秩序、经济运行、公共利益以及业务运营企业的合法权益的损害程度，对搜索系统进行安全等级划分，共分为5个等级。

5.1.1 第1级

定级对象受到破坏后，会对其业务运营企业的合法权益造成轻微损害，但不损害国家安全、社会秩序、经济运行和公共利益。

本级由业务运营企业依据国家和通信行业有关标准进行保护。

5.1.2 第2级

定级对象受到破坏后，会对业务运营企业的合法权益产生严重损害，或者对社会秩序、经济运行和公共利益造成轻微损害，但不损害国家安全。

本级由业务运营企业依据国家和通信行业有关标准进行保护，主管部门对其安全等级保护工作进行指导。

5.1.3 第3级

5.1.3.1 第3.1级

定级对象受到破坏后，会对业务运营企业的合法权益产生很严重损害，或者对社会秩序、经济运行和公共利益造成较大损害，或者对国家安全造成轻微损害。

本级由业务运营企业依据国家和通信行业有关标准进行保护，主管部门对其安全等级保护工作进行监督、检查。

5.1.3.2 第3.2级

定级对象受到破坏后，会对业务运营企业的合法权益产生特别严重损害，或者对社会秩序、经济运行和公共利益造成严重损害，或者对国家安全造成较大损害。

本级由业务运营企业依据国家和通信行业有关标准进行保护，主管部门对其安全等级保护工作进行重点监督、检查。

5.1.4 第4级

定级对象受到破坏后，会对社会秩序、经济运行和公共利益造成特别严重损害，或者对国家安全造成严重损害。

本级由业务运营企业依据国家和通信行业有关标准以及业务的特殊安全要求进行保护,主管部门对其安全等级保护工作进行强制监督、检查。

5.1.5 第5级

定级对象受到破坏后,会对国家安全造成特别严重损害。

本级由业务运营企业依据国家和通信行业有关标准以及业务的特殊安全需求进行保护,主管部门对其安全等级保护工作进行专门监督、检查。

5.2 定级要素

确定定级对象的安全等级应根据如下三个相互独立的定级要素:社会影响力、规模和服务范围和所提供服务的的重要性。

5.2.1 社会影响力-I

定级对象的社会影响力表示其受到破坏后对国家安全、社会秩序、经济运行和公共利益的损害程度,对此定级要素进行赋值时,应先确定对国家安全的损害程度,再确定对社会秩序、经济运行和公共利益的损害程度。定级对象的社会影响力赋值应是对国家安全、社会秩序、经济运行和公共利益的损害程度最严重者。

搜索系统的服务对象范围广泛,数量众多,受到破坏后会对社会秩序、经济运行和公共利益造成较为严重的损害,建议社会影响力赋值为3。

5.2.2 规模和服务范围-R

定级对象的规模表示其服务的用户数多少,服务范围表示其服务的地区范围大小。各指标数值由业务运营企业提供。

搜索系统定级对象的规模和服务范围R可根据如下指标确定:市场占有率(R1表示),指该搜索引擎产生的页面浏览量占总页面(包含国外搜索引擎)浏览量的比例,即请求量份额,权重为a;用户渗透率(R2表示),指的是被调研网民一段时间内(如半年)使用某个搜索引擎的比例,即渗透率=半年内使用过该搜索引擎的用户/总体搜索引擎用户,权重为b;用户首选率(R3表示),指该搜索引擎用户中首选用户的比例。权重值a、b、c建议分别取:3、1、1。其中,R取值为三类指标加权平均:

$$R=(a\times R1 + b\times R2 + c\times R3)/(a+b+c) \dots\dots\dots (1)$$

对于R,可参考知名市场调研公司cnzz和艾瑞的数据统计、以及中国互联网网络信息中心(CNNIC)搜索引擎相关市场年度报告。

表4 规模 R1 赋值表

市场占有率	赋值
市场占有率在 10%以下	1
市场占有率在 10%以上, 20%及以下	2
市场占有率在 20%以上, 60%及以下	3
市场占有率在 60%以上, 90%及以下	4
市场占有率在 90%及以上	5

表5 规模 R2 赋值表

用户渗透率	赋值
用户渗透率在 20%以下	1
用户渗透率在 20%以上，40%及以下	2
用户渗透率在 40%以上，60%及以下	3
用户渗透率在 60%以上，90%及以下	4
用户渗透率在 90%及以上	5

表6 规模 R3 赋值表

用户首选率	赋值
用户首选率在 20%以下	1
用户首选率在 20%以上，40%及以下	2
用户首选率在 40%以上，60%及以下	3
用户首选率在 60%以上，90%及以下	4
用户首选率在 90%及以上	5

5.2.3 所提供服务的的重要性-V

定级对象所提供服务的的重要性表示其提供的服务被破坏后对业务运营企业的合法权益的影响程度，此定级要素可通过定级对象所提供的服务本身的重要性来衡量，如业务的经济价值，业务重要性，对企业自身形象的影响等方面。

搜索系统所提供服务的的重要性很高，被破坏后对业务运营企业的合法权益造成很大损害，建议提供服务的重要性赋值为3。

在确定某一个定级要素的赋值时，无需考虑其他两个定级要素。

5.3 安全等级的计算方法

在完成定级对象的社会影响力I、规模和服务范围R、所提供服务的的重要性V三个定级要素的赋值后，需采用以下公式来计算定级对象的安全等级值：

$$k = \text{Round1} \{ \text{Log}_2 \{ [\alpha \times 2^I + \beta \times 2^R + \gamma \times 2^V] \} \} \dots\dots\dots (2)$$

其中，*k*代表安全等级值，*I*代表社会影响力赋值、*R*代表规模和服务范围赋值、*V*代表所提供服务的的重要性赋值，Round1 {}表示四舍五入处理，保留1位小数，Log₂ []表示取以2为底的对数，*α*、*β*、*γ*分别表示定级对象的社会影响力、规模和服务范围、所提供服务的的重要性赋值所占的权重，*α*≥0，*β*≥0，*γ*≥0，且*α*+*β*+*γ*=1。应根据实际情况确定权重值*α*、*β*、*γ*，建议分别取：1/3、1/3、1/3，或者0.3、0.4、0.3。

计算所得定级对象的安全等级值与安全等级的映射关系如表7所示。

表7 安全等级值与安全等级的映射关系

安全等级值 <i>k</i>	安全等级
$1 \leq k < 1.5$	第 1 级
$1.5 \leq k < 2.5$	第 2 级
$2.5 \leq k < 3.3$	第 3.1 级
$3.3 \leq k \leq 4$	第 3.2 级
$4 < k < 4.5$	第 4 级
$4.5 \leq k \leq 5$	第 5 级

6 安全防护要求

6.1 第1级要求

6.1.1 业务及应用安全

不作要求。

6.1.2 网络安全

不作要求。

6.1.3 设备及软件系统安全

不作要求。

6.1.4 物理环境安全

不作要求。

6.1.5 管理安全

不作要求。

6.2 第2级要求

6.2.1 业务及应用安全

6.2.1.1 身份鉴别

身份鉴别要求如下：

- a) 对提供登录功能的搜索系统，应提供专用的登录控制模块对登录系统的业务用户进行身份标识和鉴别；
- b) 对提供登录功能的搜索系统，应提供并启用业务用户身份标识唯一检查功能，保证系统中不存在重复用户身份标识，身份鉴别信息不易被冒用。

6.2.1.2 访问控制

访问控制要求如下：

- a) 对提供登录功能的搜索系统应提供访问控制功能，依据安全策略控制业务用户、管理用户对系统文件、数据库表等客体的访问，控制粒度为单个用户；
- b) 对提供登录功能的搜索系统，应提供并启用业务用户登录认证策略，如防范暴力破解、限定失败登录次数、锁定时间等。

6.2.1.3 安全审计

安全审计要求如下：

- a) 对提供登录功能的搜索系统，应提供覆盖到系统每个业务用户帐号的安全审计功能，至少应能对业务用户关键操作、重要行为、业务资源使用情况、系统重要安全事件等进行审计；
- b) 对提供登录功能的搜索系统，应保证无法删除、修改或覆盖审计记录；
- c) 对提供登录功能的搜索系统，审计记录的内容至少应包括事件日期、时间、发起者信息、类型、描述和结果等。

6.2.1.4 数据安全性

数据安全性要求如下：

- a) 对提供登录功能的搜索系统，业务用户登录应进行会话初始验证；
- b) 对提供登录功能的搜索系统，应提供用户登录认证过程数据加密传输功能；
- c) 对提供搜索的系统，应保证向用户展示的搜索结果(如文本、图片、应用软件等)不被篡改和伪造。

6.2.1.5 资源控制

资源控制要求如下：

- a) 对提供登录功能的搜索系统，当系统通信会话中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；
- b) 对提供登录功能的搜索系统，应能够对单个业务用户的多重并发会话进行限制。

6.2.1.6 信息保护

信息保护要求如下：

- a) 搜索系统在获得用户数据信息时，应征得用户同意，并采取传输加密等措施保障相应数据的传输安全，防止传输过程中泄漏；
- b) 搜索系统发生用户信息泄漏，应依据与用户签订的合同协议对用户进行赔偿；
- c) 搜索系统应采取充分的安全保障措施保障用户数据信息的存储安全，并保障存储系统的安全，防止存储过程中泄漏；
- d) 搜索系统应妥善保存存储有用户信息数据的纸质资料、电子介质等；
- e) 搜索系统在用户申请、审核及投诉处理过程中使用用户数据信息外，不得将用户数据信息用于任何其他用途；
- f) 搜索系统应采取措施加强对接触到用户数据信息人员的管理，严格控制接触用户信息的人员范围，合理设定用户信息操作权限，防止出现人为的信息泄漏事件；
- g) 搜索系统应当明确告知用户收集和处理用户个人信息的方式、内容和用途以及信息泄漏风险，并向用户说明本系统要采取的信息保护措施，不得将用户提交的资料和信息泄露给他人，利用该信息牟利。在与用户签署的相关合同协议中，应明确规定运营企业对用户信息安全承担保护责任，写明采取的具体信息保护措施；
- h) 搜索系统应对信息安全防护工作进行定期检查或抽查，发现有违规行为时，可以依据相关协议等追究其责任。

6.2.1.7 Web 安全防护

Web安全防护要求如下：

- a) 搜索系统应对所有来源的输入进行验证，默认所有输入都可能包含恶意信息，只要其来源不在可信任的范围之内，就应对输入进行验证并尽量使用白名单验证方法；
- b) 搜索系统应设计一套统一的验证接口，向整个应用系统提供一致的验证方法，并降低开发与代码维护的工作量；
- c) 搜索系统应在服务器端进行输入验证，避免客户端输入验证被绕过；
- d) 搜索系统应对输入内容进行规范化处理后再进行验证，如文件路径、URL 地址等；
- e) 搜索系统应防止关键参数被篡改，关键参数应直接从服务器端提取，避免从客户端输入；

- f) 搜索系统应确保用户不能访问到未授权的功能和数据，未经授权的用户试图访问受限资源时，系统应予以拒绝或提示用户进行身份鉴权；
- g) 搜索系统应在服务器端实现对系统内受限资源的访问控制，避免客户端访问控制被绕过；
- h) 搜索系统应采用统一的访问控制机制，保证整体访问控制策略的一致性，同时应确保访问控制策略不被非法修改；
- i) 搜索系统应确保会话的安全创建，在用户认证成功后，应为用户创建新的会话并释放原有会话，创建的会话标识应满足随机性和长度要求，避免被攻击者猜测（如采用会话与 IP 地址绑定的方式），降低会话被盗用的风险；
- j) 搜索系统应确保会话数据的存储安全，用户登录成功后所生成的会话数据应存储在服务器端，并确保会话数据不能被非法访问，当更新会话数据时，要对数据进行严格的输入验证，以免会话数据的非法篡改；
- k) 搜索系统应确保会话数据的传输安全，防止泄露会话标识；
- l) 搜索系统应确保会话的安全终止，当用户登录成功并成功创建会话后，应在 web 应用系统的各个页面提供用户登出功能，登出时应及时删除服务器端的会话数据；当处于登录状态的用户直接关闭浏览器时，需要提示用户执行安全登出或者自动为用户完成登出过程，从而安全的终止本次会话；
- m) 搜索系统应设置合理的会话超时阈值，在合理范围内尽可能减小会话超时阈值，可以降低会话被劫持和重复攻击的风险，超过会话超时阈值后立刻销毁会话，清除会话的信息；
- n) 搜索系统应限制会话并发连接数，限制同一用户的会话并发连接数，避免恶意用户创建多个并发的会话来消耗系统资源，影响业务可用性；
- o) 搜索系统在涉及到关键业务操作的 web 页面，应为提供保障会话安全的补充机制（如以 web 页面一次性随机令牌的方式，作为主会话标识的补充）。

6.2.1.8 对外能力接口安全

对外能力接口安全要求如下：

- a) 搜索系统应提供数据有效性检验功能，保证通过接口输入或通过通信接口输入的数据格式或长度符合系统设定要求；
- b) 搜索系统接口均必须分别设置专门前置服务器，通过前置服务器的接口应用实现内外系统的交互；
- c) 搜索系统接口数据传输应尽量采用加密方式，原则上要求内外系统交互时，接口报文中的敏感信息应进行加密传输，如接口认证需要的密码等敏感数据；
- d) 搜索系统接口数据传输应进行校验，确保数据在传输过程中的完整性；
- e) 搜索系统接口认证信息必须以密文的形式单独存储在配置文件中；
- f) 搜索系统应对接口的状态和交互过程进行监控，并支持异常恢复。

6.2.1.9 恶意代码防范

恶意代码防范要求如下：

- a) 搜索系统应具备恶意代码过滤功能，应对通过该平台对外发布的公共信息使用自动程序过滤和人工检查结合的方式进行恶意代码检查、屏蔽和删除，防止恶意代码通过业务网络向公众传播；
- b) 搜索系统应将被屏蔽的含有恶意代码的搜索结果相关信息告知搜索用户。

6.2.2 网络安全

6.2.2.1 网络结构安全

网络结构安全要求如下：

- a) 搜索系统运营者应能提供与当前运行情况相符的系统拓扑结构图；
- b) 搜索系统应根据搜索系统应用和服务的特点，在满足高峰期流量需求的基础上，合理设计带宽。

6.2.2.2 入侵防范

搜索系统应在系统边界部署访问控制设备，并启用有效的访问控制策略。

6.2.2.3 安全审计

安全审计要求如下：

- a) 搜索系统应对系统中的重要设备运行状况、网络流量监测信息、系统管理及维护等进行日志记录，并且保留一定期限（至少 180 天）；
- b) 搜索系统审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

6.2.3 设备及软件系统安全

6.2.3.1 网络及安全设备

网络及安全设备要求如下：

- a) 搜索系统各类路由器、交换机等网络设备应满足相关行业标准要求，具有进网许可证；
- b) 搜索系统应对登录网络设备（例如路由器、交换机）以及安全设备（例如入侵检测设备、防火墙设备）的用户进行有效的身份标识和鉴别；
- c) 搜索系统中网络及安全设备管理用户的标识应唯一；
- d) 搜索系统中网络及安全设备管理用户口令应不小于 8 字节，口令应有复杂度要求（如使用大写字母、小写字母、数字、标点及特殊字符五种字符中至少二种的组合，且与用户名或身份标识无相关性）并定期更换（更新周期不大于 90 天）。

6.2.3.2 通用主机操作系统

6.2.3.2.1 安全检测

安全检测要求如下：

- a) 应对搜索系统中各个功能模块的计算机运维终端、服务器等设备的主机操作系统进行必要的安全检测，出具安全测试及验收报告并妥善保存，相关设备的安全应满足相应设备技术规范、设备安全要求等行业标准的相关规定；
- b) 搜索系统中各个功能模块的计算机运维终端、服务器等设备的主机操作系统应遵循最小安装的原则，仅安装和开通需要的功能组件和应用程序，并通过安全方式（如设置升级服务器）保持系统补丁及时得到更新；
- c) 搜索系统中各个功能模块的计算机运维终端、服务器等设备的主机操作系统应定期进行安全监测，发现并加固操作系统相关漏洞，避免业已发现的漏洞造成安全事件。

6.2.3.2.2 身份鉴别

身份鉴别要求如下：

- a) 应对搜索系统中各个功能模块的计算机运维终端、服务器等设备的主机操作系统的用户进行身份标识和鉴别；

- b) 应对搜索系统中各个功能模块的计算机运维终端、服务器等设备的主机操作系统的不同用户分配不同的用户名，确保用户名具有唯一性；
- c) 搜索系统中各个功能模块的计算机运维终端、服务器等设备的主机操作系统的管理用户身份标识应具有不易被冒用的特点，相关用户口令长度应不小于 8 字节，口令应有复杂度要求（使用大写字母、小写字母、数字、标点及特殊字符五种字符中至少二种的组合，且与用户名或身份标识无相关性）并定期更换（更新周期不大于 90 天）。

6.2.3.2.3 访问控制

访问控制要求如下：

- a) 搜索系统中各个功能模块的计算机运维终端、服务器等设备应启用访问控制功能，依据安全策略控制用户对资源的访问；
- b) 搜索系统中各个功能模块的计算机运维终端、服务器等设备应及时删除多余的、过期的账户，避免共享账户的存在；
- c) 搜索系统中各个功能模块的计算机运维终端、服务器等设备应实现操作系统和数据库系统特权用户的权限分离；
- d) 搜索系统中各个功能模块的计算机运维终端、服务器等设备应限制默认账户的访问权限，修改这些账户的默认口令，条件允许下，应重命名默认账户。

6.2.3.2.4 安全审计

安全审计要求如下：

- a) 搜索系统中各个功能模块的计算机运维终端、服务器等设备的审计范围应覆盖到主机/服务器上的每个操作系统用户；
- b) 搜索系统中各个功能模块的计算机运维终端、服务器等设备的审计内容应包括重要用户行为、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) 搜索系统中各个功能模块的计算机运维终端、服务器等设备的审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等。

6.2.3.2.5 恶意代码防范

恶意代码防范要求如下：

- a) 搜索系统中各个功能模块的计算机运维终端、服务器等设备应安装防范病毒、木马等恶意代码的软件，并及时更新防恶意代码软件版本和恶意代码库；
- b) 搜索系统中各个功能模块的计算机运维终端、服务器等设备应支持防恶意代码的统一管理。

6.2.3.2.6 资源控制

资源控制要求如下：

- a) 搜索系统中各个功能模块的服务器应通过设定计算机运维终端接入方式、网络地址范围等条件限制管理终端登录；
- b) 搜索系统中各个功能模块的服务器应根据安全策略设置计算机运维终端的操作超时锁定；
- c) 搜索系统中各个功能模块的服务器应限制单个用户对主机资源的最大或最小使用限度。

6.2.3.2.7 冗余备份

搜索系统中各个功能模块的服务器应具备一定的冗余备份，关键设备、重要部件应采用冗余的方式提供保护。

6.2.3.3 数据库及中间件软件

6.2.3.3.1 安全检测

安全检测要求如下：

- a) 应对搜索系统中各个功能模块的数据库及中间件软件进行必要的安全检测，出具安全测试及验收报告并妥善保存，相关设备的安全应满足相应设备技术规范、设备安全要求等行业标准的相关规定；
- b) 搜索系统中各个功能模块的数据库及中间件软件应遵循最小安装的原则，仅安装和开通需要的功能组件和应用程序，并通过安全方式（如设置升级服务器）保持系统补丁及时得到更新；
- c) 应对搜索系统中各个功能模块的数据库及中间件软件应定期进行安全监测，发现并加固操作系统相关漏洞，避免业已发现的漏洞造成安全事件。

6.2.3.3.2 身份鉴别

身份鉴别要求如下：

- a) 应对搜索系统中各个功能模块的数据库及中间件软件的用户进行身份标识和鉴别；
- b) 应对搜索系统中各个功能模块的数据库及中间件软件的不同用户分配不同的用户名，确保用户名具有唯一性；
- c) 应对搜索系统中各个功能模块的数据库及中间件软件的管理用户身份标识应具有不易被冒用的特点，相关用户口令长度应不小于 8 字节，口令应有复杂度要求（使用大写字母、小写字母、数字、标点及特殊字符五种字符中至少二种的组合，且与用户名或身份标识无相关性）并定期更换（更新周期不大于 90 天）。

6.2.3.3.3 访问控制

访问控制要求如下：

- a) 搜索系统中各个功能模块的数据库及中间件软件应启用访问控制功能，依据安全策略控制用户对资源的访问；
- b) 搜索系统中各个功能模块的数据库及中间件软件应及时删除多余的、过期的账户，避免共享账户的存在；
- c) 搜索系统中各个功能模块的数据库及中间件软件应实现数据库、中间件特权用户与操作系统的权限分离；
- d) 搜索系统中各个功能模块的数据库及中间件软件应限制默认账户的访问权限，修改这些账户的默认口令，条件允许下，应重命名默认账户。

6.2.3.3.4 安全审计

安全审计要求如下：

- a) 搜索系统中各个功能模块的数据库及中间件软件的审计范围应覆盖到主机/服务器上的每个操作系统用户；
- b) 搜索系统中各个功能模块的数据库及中间件软件的审计内容应包括重要用户行为、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) 搜索系统中各个功能模块的数据库及中间件软件的审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等。

6.2.3.3.5 资源控制

资源控制要求如下：

- a) 搜索系统中各个功能模块的数据库及中间件软件应通过设定计算机运维终端接入方式、网络地址范围等条件限制管理终端登录；
- b) 搜索系统中各个功能模块的数据库及中间件软件应根据安全策略设置计算机运维终端的操作超时锁定；
- c) 搜索系统中各个功能模块的数据库及中间件软件应限制单个用户对主机资源的最大或最小使用限度。

6.2.3.3.6 冗余备份

搜索系统中各个功能模块的数据库及中间件软件应具备一定的冗余备份，关键设备、重要部件应采用冗余的方式提供保护。

6.2.4 物理环境安全

6.2.4.1 物理位置的选择

物理位置选择要求如下：

- a) 机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内；
- b) 机房的承重能力应满足机房建筑要求。

6.2.4.2 物理访问控制

物理访问控制要求如下：

- a) 机房出入口应安排专人值守，控制、鉴别和记录进入的人员；
- b) 需进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围。

6.2.4.3 防盗窃和防破坏

防盗窃和防破坏要求如下：

- a) 应将主要设备放置在机房内；
- b) 应将设备或主要部件进行固定，并设置明显的不易除去的标记；
- c) 应将室外通信线缆敷设在隐蔽处，可铺设在地下或管道中；
- d) 应对介质分类标识，存储在介质库或档案室中；
- e) 主机房应安装必要的防盗报警设施。

6.2.4.4 防雷击

防雷击要求如下：

- a) 机房建筑应设置避雷装置；
- b) 机房应设置交流电源地线；
- c) 应满足 YD 5098-2005 中相关要求。

6.2.4.5 防火

防火要求如下：

- a) 机房应设置灭火设备和火灾自动报警系统；
- b) 应满足 YD 5002 中相关要求。

6.2.4.6 防水和防潮

防水和防潮要求如下：

- a) 水管安装，不得穿过机房屋顶和活动地板下；
- b) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
- c) 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。

6.2.4.7 防静电

关键设备应采用必要的接地防静电措施。

6.2.4.8 温湿度控制

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。

6.2.4.9 防尘

应采取必要的对机房的防尘措施，出入机房要求使用鞋套，有专人定期对机房进行除尘工作，有条件的设置防尘走廊。

6.2.4.10 电力供应

电力供应要求如下：

- a) 应在机房供电线路上配置稳压器和过电压防护设备；
- b) 应提供短期的备用电力供应，至少满足关键设备在断电情况下的正常运行要求。

6.2.4.11 电磁防护

电源线和通信线缆应隔离铺设，避免互相干扰。

6.2.5 管理安全

6.2.5.1 安全管理制度

6.2.5.1.1 管理制度

管理制度要求如下：

- a) 应制定安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等；
- b) 应对安全管理活动中重要的管理内容建立安全管理制度；
- c) 应对安全管理人员或操作人员执行的重要管理操作建立操作规程。

6.2.5.1.2 制定和发布

制定和发布要求如下：

- a) 应指定或授权专门的部门或人员负责安全管理制度的制定；
- b) 应组织相关人员对制定的安全管理制度进行论证和审定；
- c) 应将安全管理制度以某种方式发布到相关人员手中。

6.2.5.1.3 评审和修订

应定期对安全管理制度进行评审，对存在不足或需要改进的安全管理制度进行修订。

6.2.5.2 安全管理机构

6.2.5.2.1 岗位设置

岗位设置要求如下：

- a) 应设立安全主管、安全管理各个方面的负责人岗位，定义各负责人的职责；
- b) 应设立专职的网络安全技术人员岗位，定义有关工作岗位的职责。

6.2.5.2.2 人员配备

应配备一定数量的网络安全管理和技术人员，能满足网络安全工作所需。

6.2.5.2.3 授权和审批

授权和审批要求如下：

- a) 应根据各个部门和岗位的职责明确授权审批部门及批准人，对系统投入运行割接、升级和重要资源访问等关键活动进行审批；
- b) 应针对关键活动建立审批流程，并由批准人签字确认。

6.2.5.2.4 沟通和合作

沟通和合作要求如下：

- a) 应加强企业内部人员（如管理人员、技术人员）及机构（如业务部门、安全管理职能部门）之间的合作与沟通；
- b) 应加强与相关外部单位的合作与沟通。

6.2.5.2.5 审核和检查

应由安全管理人员定期进行安全检查，检查内容包括用户账号、系统漏洞、数据备份等情况。

6.2.5.3 人员安全管理

6.2.5.3.1 人员录用

人员录用要求如下：

- a) 应指定或授权专门的部门或人员负责人员录用；
- b) 应规范人员录用过程，对被录用人员的身份、背景和专业资格等进行审查，对其所具有的技术技能进行考核；
- c) 应与从事关键岗位的人员签署保密协议。

6.2.5.3.2 人员离岗

人员离岗要求如下：

- a) 应规范人员离岗过程，及时终止离岗员工的所有访问权限；
- b) 对于离岗人员，应取回各种身份证件、钥匙等以及企业提供的软硬件设备；
- c) 对于离岗人员，应办理严格的调离手续。

6.2.5.3.3 人员考核

应定期对各个岗位的人员进行安全技能及安全认知的考核。

6.2.5.3.4 人员和技术支持能力

相关网络安全管理和技术人员应通过技能培训和考核。

6.2.5.3.5 安全意识教育和培训

安全意识教育和培训要求如下：

- a) 应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训；
- b) 应告知人员相关的安全责任和惩戒措施，并对违反违背安全策略和规定的人员进行惩戒；
- c) 应制定安全教育和培训计划，对网络安全基础知识、岗位操作规程等进行培训。

6.2.5.3.6 外部人员访问管理

应确保在外部人员访问受控区域前得到授权或审批，批准后由专人全程陪同或监督，并登记备案。

6.2.5.4 安全建设管理

6.2.5.4.1 定级

定级要求如下：

- a) 应明确网络的边界和安全保护等级；
- b) 应以书面的形式说明定级对象确定为某个安全等级的方法和理由；
- c) 应指定专门的人员或部门负责管理定级相关材料，并按主管部门要求及时上报、审批、备案。

6.2.5.4.2 安全方案设计

安全方案设计要求如下：

- a) 应根据网络的安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；
- b) 应以书面形式描述对网络的安全保护要求、策略和措施等内容，形成网络的安全方案；
- c) 应对安全方案进行细化，形成能指导安全系统建设、安全产品采购和使用的详细设计方案；
- d) 应组织相关部门和有关安全技术专家对安全设计方案的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施。

6.2.5.4.3 产品采购和使用

产品采购和使用要求如下：

- a) 应确保安全产品采购和使用符合国家的有关规定；
- b) 应确保密码产品采购和使用符合国家密码主管部门的要求；
- c) 应指定或授权专门的部门负责产品的采购。

6.2.5.4.4 自行软件开发

自行软件开发要求如下：

- a) 应确保开发环境与实际运行环境物理分开；
- b) 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；
- c) 应确保提供软件设计的相关文档和使用指南，并由专人负责保管。

6.2.5.4.5 外包软件开发

外包软件开发要求如下：

- a) 应根据开发需求检测软件质量；
- b) 应要求开发单位提供软件设计的相关文档和使用指南；
- c) 应在软件安装之前检测软件包中可能存在的恶意代码。

6.2.5.4.6 工程实施

工程实施要求如下：

- a) 应指定或授权专门的部门或人员负责工程实施过程的管理；
- b) 应制定详细的工程实施方案，控制工程实施过程。

6.2.5.4.7 测试验收

测试验收要求如下：

- a) 应对系统进行安全性测试验收；
- b) 在测试验收前应根据设计方案或合同要求等制订覆盖网络安全要求的测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告。

6.2.5.4.8 交付

交付要求如下：

- a) 应制定网络交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；
- b) 应对负责网络运行维护的技术人员进行相应的技能培训。

6.2.5.4.9 安全服务商的选择

安全服务商的选择要求如下：

- a) 应确保安全服务商的选择符合国家的有关规定；
- b) 应与选定的安全服务商签订与安全相关的协议，明确约定相关责任；
- c) 应确保选定的安全服务商提供技术支持和服务承诺，必要时与其签订服务合同。

6.2.5.5 安全运维管理

6.2.5.5.1 运行维护管理能力要求

运行维护管理能力要求如下：

- a) 应具有完善运行维护管理制度，管理制度应涵盖业务管理和控制、系统运行、设备操作和维护等方面；
- b) 应按照统一的运行维护要求，对业务及应用系统进行规范化的维护。
- c) 应有业务及应用系统相关介质存取、验证和转储的管理制度，确保有关备份数据、信息的授权访问；
- d) 应保持与其他部门、外部单位间良好的联络和协作能力。

6.2.5.5.2 环境管理

环境管理要求如下：

- a) 应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设备设施进行维护管理；
- b) 应配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理；
- c) 应建立机房安全管理制度，对有关机房物理区域访问，物品带进、带出机房和机房环境安全等方面的管理做出规定；
- d) 应加强对办公环境的保密性管理，包括工作人员调离办公室应立即交还该办公室钥匙和不在办公区接待来访人员等内容。

6.2.5.5.3 资产管理

资产管理要求如下：

- a) 应编制与网络相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；
- b) 应建立资产安全管理制度，规定资产管理的责任人员或责任部门，并规范资产管理和使用的行为。

6.2.5.5.4 介质管理

介质管理要求如下：

- a) 应确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理；
- b) 应对介质归档和查询等过程进行记录，并根据存档介质的目录清单定期盘点；
- c) 应对需要送出维修或销毁的介质，首先清除其中的敏感数据，防止信息的非法泄漏；
- d) 应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。

6.2.5.5.5 设备管理

设备管理要求如下：

- a) 应对网络相关的各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；
- b) 应建立基于申报、审批和专人负责的设备安全管理制度，对各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理；
- c) 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现关键设备（包括备份和冗余设备）的启动/停止、加电/断电等操作；
- d) 应确保信息处理设备必须经过审批才能带离机房或办公地点。

6.2.5.5.6 网络安全管理

网络安全管理要求如下：

- a) 应指定人员对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作；
- b) 应建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定。

6.2.5.5.7 恶意代码防范管理

恶意代码防范管理要求如下：

- a) 应提高所有人员的恶意代码防范意识，明确移动存储介质使用、从外部网络接收文件、外来设备接入等环节的恶意代码安全检测要求；
- b) 应指定专人对网络和主机进行恶意代码检测并保存检测记录；
- c) 应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定。

6.2.5.5.8 密码管理

应使用符合国家密码管理规定的密码技术和产品。

6.2.5.5.9 变更管理

变更管理要求如下：

- a) 应确认网络中要发生重要变更的行为，并制定相应的变更方案；
- b) 网络发生重要变更前，应向主管领导申请，审批后方可实施变更，并在实施后向相关人员通告。

6.2.5.5.10 备份与恢复管理

备份与恢复管理要求如下：

- a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等；
- b) 应规定备份信息的备份方式（如增量备份或全备份等）、备份频度（如每日或每周等）、存储介质、保存期等；
- c) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略应指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法。

6.2.5.5.11 安全事件处置

安全事件处置要求如下：

- a) 应报告所发现的安全弱点和可疑事件，但任何情况下均不应尝试验证弱点；
- b) 应制定安全事件报告和处置管理制度，明确安全事件类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责；
- c) 应根据安全事件对本网络产生的影响，对本网络安全事件进行等级划分；
- d) 应记录并保存所有发现的安全弱点和可疑事件，分析事件原因，监督事态发展，采取措施避免安全事件发生。

6.2.5.5.12 应急预案管理

应急预案管理要求如下：

- a) 应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容；
- b) 应对相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次。

6.3 第3.1级要求

6.3.1 业务及应用安全

6.3.1.1 身份鉴别

除满足第2级的要求之外，还应满足：

- a) 对提供登录功能的搜索系统，应提供并启用用户身份标识唯一检查功能，保证系统中不存在重复用户身份标识；
- b) 对提供登录功能的搜索系统，应提供并启用用户登录认证口令复杂度强度功能，保证业务用户的口令长度应不小于8字节，口令应有复杂度要求（如使用大写字母、小写字母、数字、标点及特殊字符等类字符中至少二种的组合，且与用户名或身份标识无相关性）并定期更换（更新周期不大于90天）；

6.3.1.2 访问控制

除满足第2级的要求之外，还对提供登录功能的搜索系统，应严格设置业务用户解锁策略，按安全策略要求，被锁定的业务用户需通过注册时的标志信息进行密码重新设定或者凭有效证件进行设定。

6.3.1.3 安全审计

除满足第2级的要求之外，还对提供登录功能的搜索系统，应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

6.3.1.4 数据安全

除满足第2级的要求之外，还应满足：

- a) 对提供登录功能的搜索系统，应保证采用足够强壮的加密算法保证用户登录认证过程数据不被非授权利用和篡改。
- b) 对提供登录功能的搜索系统，应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据符合系统设定要求，确保非常规数据被过滤。

6.3.1.5 资源控制

除满足第2级的要求之外，搜索系统还应对通过该平台对外发布的公共信息使用自动程序过滤和人工检查结合的方式进行恶意代码检查、屏蔽和删除，防止恶意代码通过业务网络向公众传播。

6.3.1.6 信息保护

除满足第2级的要求之外，还对提供登录功能的搜索系统，应保护系统服务相关信息的安全，避免有关数据被篡改和破坏；

6.3.1.7 Web 安全防护

除满足第2级的要求之外，还应满足：

- a) web 程序上线前或升级后应进行代码审计，形成报告，并对审计出的问题进行代码升级完善；
- b) 应避免使用含有已公开漏洞的开源第三方应用组件及代码（漏洞库可参考 CVE、CNVD 等）。

6.3.1.8 对外能力接口安全

同第2级要求。

6.3.1.9 恶意代码防范

除满足第2级的要求之外，还对提供登录功能的搜索系统，应禁止不必要的内嵌网络服务，应禁止在用户端自动安装恶意软件和插件。

6.3.2 网络安全

6.3.2.1 网络结构安全

除满足第2级的要求之外，还应满足：

- a) 搜索系统应根据系统内部网络结构特点，按照统一的管理和控制原则划分不同的子网或网段，设备依照功能划分及其重要性等因素分区部署；
- b) 不考虑主动宕机维护的情况，搜索系统年宕机时间不超过 4.38 小时，可靠性应达到 99.95% 以上；
- c) 搜索系统应具备必要的流量负荷分担设计。

6.3.2.2 入侵防范

除满足第2级的要求之外，搜索系统还应在系统边界处对发生的网络入侵行为（包括但不限于端口扫描、强力攻击、木马后门攻击、DoS/DDoS攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击）提供有效的检测能力，当检测到入侵行为时应能记录攻击源IP、攻击类型、攻击目的、攻击时间。

6.3.2.3 安全审计

除满足第2级的要求之外，还应满足：

- a) 搜索系统应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。
- b) 搜索系统应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，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；
- c) 搜索系统应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段；
- d) 搜索系统应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。

6.3.3 设备及软件系统安全

6.3.3.1 网络及安全设备

除满足第2级的要求之外，还应满足：

- a) 搜索系统网络及安全设备应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；
- b) 搜索系统网络及安全设备应通过设定终端接入方式、网络地址范围等条件限制管理终端登录；
- c) 搜索系统网络及安全设备进行远程管理时，应采取必要措施防止身份鉴别信息在网络传输过程中被窃取。

6.3.3.2 操作系统

6.3.3.2.1 安全检测

同第2级要求。

6.3.3.2.2 身份鉴别

除满足第2级的要求之外，还应满足：

- a) 搜索系统中各个功能模块的计算机运维终端、服务器等设备的主机操作系统应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；
- b) 搜索系统中各个功能模块的计算机运维终端、服务器等设备进行远程管理时，应采取必要措施，防止鉴别信息在传输过程中被窃听。

6.3.3.2.3 访问控制

同第2级要求。

6.3.3.2.4 安全审计

除满足第2级的要求之外，搜索系统中各个功能模块的计算机运维终端、服务器等设备的审计记录，避免其受到未预期的删除、修改或覆盖等，保留一定期限（至少180天）。

6.3.3.2.5 恶意代码防范

同第2级要求。

6.3.3.2.6 资源控制

除满足第2级的要求之外，还应满足：

- a) 搜索系统应对能够对各模块的服务器进行性能和服务水平监控，监控方式可基于监听、SNMP等网管技术和协议；并设定阈值，在监测到服务水平降低到阈值时进行报警；
- b) 搜索系统中各个功能模块的服务器应保持时间上的同步。

6.3.3.2.7 冗余备份

除满足第2级的要求之外，还应满足：

- a) 搜索系统中各个功能模块的服务器应建立对操作系统关键数据（如操作系统配置数据、管理员操作维护记录、用户信息等）和重要信息进行备份和恢复的管理和控制机制；
- b) 搜索系统中相关主机数据备份范围和时间间隔、数据恢复能力应满足行业管理、业务运营企业应急预案相关要求。

6.3.3.3 数据库及中间件

6.3.3.3.1 安全检测

同第2级要求。

6.3.3.3.2 身份鉴别

除满足第2级的要求之外，还应满足：

- a) 应对搜索系统中各个功能模块的数据库及中间件软件应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；
- b) 应对搜索系统中各个功能模块的数据库及中间件软件进行远程管理时，应采取必要措施，防止身份鉴别信息在传输过程中被窃取。

6.3.3.3.3 访问控制

同第2级要求。

6.3.3.3.4 安全审计

除满足第2级的要求之外，搜索系统中各个功能模块的数据库及中间件软件的审计记录，避免其受到未预期的删除、修改或覆盖等，保留一定期限（至少180天）。

6.3.3.3.5 资源控制

除满足第2级的要求之外，还应满足：

- a) 搜索系统中各个功能模块的数据库及中间件软件行性能和服务水平监控，监控方式可基于监听、SNMP等网管技术和协议；并设定阈值，在监测到服务水平降低到阈值时进行报警；
- b) 搜索系统中各个功能模块的数据库及中间件软件应保持时间上的同步。

6.3.3.3.6 冗余备份

除满足第2级的要求之外，还应满足：

- a) 搜索系统中各个功能模块的数据库及中间件软件应建立对关键数据（如配置数据、管理员操作维护记录、用户信息等）和重要信息进行备份和恢复的管理和控制机制；
- b) 搜索系统中各个功能模块的数据库及中间件软件中相关数据备份范围和时间间隔、数据恢复能力应满足行业管理、业务运营企业应急预案相关要求。

6.3.4 物理环境安全要求

6.3.4.1 物理位置的选择

除满足第2级的要求之外，还应满足：

- a) 机房场地应避免设在建筑物的顶层或地下室，以及用水设备的下层或隔壁；
- b) 如果机房有铁架，机房铁架安装应满足 YD/T 5026-2005 要求。

6.3.4.2 物理访问控制

除满足第2级的要求之外，还应满足：

- a) 应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域；
- b) 重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。

6.3.4.3 防盗窃和防破坏

除满足第2级的要求之外，还应满足：

- a) 应利用光、电等技术设置机房防盗报警系统；
- b) 应对机房设置监控报警系统。

6.3.4.4 防雷击

除满足第2级的要求之外，还应设置防雷保安器，防止感应雷。

6.3.4.5 防火

除满足第2级的要求之外，还应满足：

- a) 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；
- b) 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；
- c) 机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。

6.3.4.6 防水和防潮

除满足第2级的要求之外，还应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。

6.3.4.7 防静电

除满足第2级的要求之外，还应满足：

- a) 主要设备应采用必要的接地防静电措施；
- b) 机房应采用防静电地板。

6.3.4.8 温湿度控制

同第2级要求。

6.3.4.9 防尘

同第2级要求。

6.3.4.10 电力供应

除满足第2级的要求之外，还应满足：

- a) 应设置冗余或并行的电力电缆线路为系统供电；

- b) 应建立备用供电系统。

6.3.4.11 电磁防护

除满足第2级的要求之外，还应采用接地方式防止外界电磁干扰和设备寄生耦合干扰。

6.3.4.12 防鼠

信息服务业务系统所处机房应具备防虫防鼠等相关措施，以有效防范鼠虫蚁害。

6.3.5 管理安全要求

6.3.5.1 安全管理制度

6.3.5.1.1 管理制度

除满足第2级的要求之外，还应满足：

- a) 应对安全管理活动中的各类管理内容建立安全管理制度，以规范安全管理活动；
- b) 应形成由安全策略、管理制度、操作规程等构成的全面的安全管理制度体系。

6.3.5.1.2 制定和发布

除满足第2级的要求之外，还应满足：

- a) 安全管理制度应有统一的格式，并进行版本控制；
- b) 安全管理制度应通过正式、有效的方式发布；
- c) 安全管理制度应注明发布范围，并对收发文进行登记。

6.3.5.1.3 评审和修订

除满足第2级的要求之外，还应满足：

- a) 安全领导小组应负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定；
- b) 应定期或不定期对安全管理制度进行检查和审定。

6.3.5.2 安全管理机构

6.3.5.2.1 岗位设置

除满足第2级的要求之外，还应满足：

- a) 应设立安全管理工作的职能部门；
- b) 应成立指导和管理安全工作的委员会或领导小组，其最高领导应由单位主管领导委任或授权；
- c) 应制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。

6.3.5.2.2 人员配备

除满足第2级的要求之外，还应满足：

- a) 应配备专职安全管理员，不可兼任；
- b) 关键事务岗位应配备多人共同管理。

6.3.5.2.3 授权和审批

除满足第2级的要求之外，还应满足：

- a) 应根据各个部门和岗位的职责明确授权审批事项；
- b) 应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；
- c) 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息；
- d) 应记录审批过程并保存审批文档。

6.3.5.2.4 沟通和合作

除满足第2级的要求之外，还应满足：

- a) 各类管理人员之间、组织内部机构之间以及网络安全职能部门内部定期或不定期召开协调会议，共同协作处理网络安全问题；
- b) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息；
- c) 应聘请网络安全专家作为常年的安全顾问，指导网络安全建设，参与安全规划和安全评审等。

6.3.5.2.5 审核和检查

除满足第2级的要求之外，还应满足：

- a) 应由内部人员或上级单位定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；
- b) 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报；
- c) 应制定安全审核和安全检查制度，规范安全审核和安全检查工作，定期按照程序进行安全审核和安全检查活动。

6.3.5.3 人员安全管理

6.3.5.3.1 人员录用

除满足第2级的要求之外，还应满足：

- a) 应严格规范人员录用过程，对被录用人的资质等进行审查；
- b) 应签署保密协议；
- c) 应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。

6.3.5.3.2 人员离岗

除满足第2级的要求之外，关键岗位人员离岗须承诺调离后的保密义务后方可离开。

6.3.5.3.3 人员考核

除满足第2级的要求之外，还应满足：

- a) 应对关键岗位的人员进行全面、严格的安全审查和技能考核；
- b) 应对考核结果进行记录并保存。

6.3.5.3.4 人员和技术支持能力

同第2级要求。

6.3.5.3.5 安全意识教育和培训

除满足第2级的要求之外，还应满足：

- a) 应对安全责任和惩戒措施进行书面规定；
- b) 应对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划；
- c) 应对安全教育和培训的情况和结果进行记录并归档保存。

6.3.5.3.6 外部人员访问管理

除满足第2级的要求之外，还应满足：

- a) 应确保在外部人员访问受控区域前先提出书面申请；
- b) 对外部人员允许访问的区域、网络、设备、信息等内容应进行书面的规定，并按照规定执行。

6.3.5.4 安全管理

6.3.5.4.1 定级

除满足第2级的要求之外，还应满足：

- a) 应组织相关部门和有关安全技术专家对网络定级结果的合理性和正确性进行论证和审定；
- b) 应将网络的定级结果分级上报至全国或地区的主管部门，主管部门对定级结果审批。

6.3.5.4.2 安全方案设计

除满足第2级的要求之外，还应满足：应指定和授权专门的部门对网络的安全建设进行总体规划，制定近期和远期的安全建设工作计划；

- a) 应根据网络的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件；
- b) 应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施；
- c) 应根据等级评测、安全评估的结果定期调整和修订总体安全策略、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。

6.3.5.4.3 产品采购和使用

除满足第2级的要求之外，还应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。

6.3.5.4.4 自行软件开发

除满足第2级的要求之外，还应满足：

- a) 应确保开发人员和测试人员分离，测试数据和测试结果受到控制；
- b) 应制定代码编写安全规范，要求开发人员参照规范编写代码；
- c) 应确保对程序资源库的修改、更新、发布进行授权和批准。

6.3.5.4.5 外包软件开发

同第2级要求。

6.3.5.4.6 工程实施

除满足第2级的要求之外，还应满足：

- a) 要求工程实施单位能正确地执行安全工程过程；

- b) 应制定工程实施方面的管理制度，明确说明实施过程的控制方法和人员行为准则。

6.3.5.4.7 测试验收

除满足第2级的要求之外，还应满足：

- a) 应对系统测试验收的控制方法和人员行为准则进行书面规定；
- b) 应指定或授权专门的部门负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作。

6.3.5.4.8 交付

除满足第2级的要求之外，还应满足：

- a) 应对网络交付的控制方法和人员行为准则进行书面规定；
- b) 应指定或授权专门的部门负责网络交付的管理工作，并按照管理规定的要求完成交付工作；
- c) 在网络正式投入使用前，应根据实际情况进行试运行，试运行期间应提供相关应急预防措施；
- d) 在网络正式投入使用后，应对开发、建设过程中涉及安全要求的配置、口令等内容重新修改、设定。

6.3.5.4.9 安全服务商的选择

同第2级要求。

6.3.5.4.10 等级评测

等级评测要求如下：

- a) 在网络运行过程中，应至少每年对网络进行一次等级评测，发现不符合相应等级保护标准要求的及时整改；
- b) 应在网络发生变更时及时对网络进行等级评测，发现级别发生变化的及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的及时整改；
- c) 应选择具有国家相关技术资质和安全资质的评测单位进行等级评测；
- d) 应指定或授权专门的部门或人员负责等级评测的管理。

6.3.5.5 安全运维管理

6.3.5.5.1 环境管理

除满足第2级的要求之外，还应满足：

- a) 应有指定的部门负责机房安全，并配置电子门禁系统，对机房来访人员实行登记记录和电子记录双重备案管理。
- b) 工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感数据的纸档文件。

6.3.5.5.2 资产管理

除满足第2级的要求之外，还应满足：

- a) 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；
- b) 应对信息分类与标识方法做出规定，并对信息的使用、传输和存储等进行规范化管理。

6.3.5.5.3 介质管理

除满足第2级的要求之外，还应满足：

- a) 应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面做出规定；
- b) 应对介质的物理传输过程中人员选择、打包、交付等情况进行控制；
- c) 应对存储介质的使用过程进行严格的管理，对带出工作环境的存储介质进行内容加密和监控管理，对保密性较高的存储介质未经批准不得自行销毁；
- d) 应根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同；
- e) 应对重要介质中的数据和软件采取加密存储。

6.3.5.5.4 设备管理

除满足第2级的要求之外，还应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等。

6.3.5.5.5 监控管理

监控管理要求如下：

- a) 应对通信线路、主机、网络设备和应用程序的运行状况、网络流量、用户行为等进行监测和报警，形成记录并妥善保存；
- b) 应组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施；
- c) 应建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理。

6.3.5.5.6 网络安全管理

除满足第2级的要求之外，还应满足：

- a) 应实现设备的最小服务配置，并对配置文件进行定期离线备份；
- b) 应依据安全策略允许或者拒绝便携式和移动式设备的网络接入；
- c) 应定期检查是否存在违反规定拨号上网或其他违反网络安全策略的行为。

6.3.5.5.7 恶意代码防范管理

除满足第2级的要求之外，还应定期检查网络内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报。

6.3.5.5.8 密码管理

除满足第2级的要求之外，还应建立密码使用管理制度。

6.3.5.5.9 变更管理

除满足第2级的要求之外，还应满足：

- a) 应建立变更管理制度，变更和变更方案需有评审过程；
- b) 应建立变更申报和变更审批文件化程序，对变更影响进行分析并文档化，记录变更实施过程，并妥善保存所有文档和记录；
- c) 应建立中止变更并从失败变更中恢复的文件化程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。

6.3.5.5.10 备份与恢复管理

除满足第2级的要求之外，还应满足：

- a) 应建立备份与恢复管理相关的安全管理制度；
- b) 应建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存；
- c) 应定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。

6.3.5.5.11 安全事件处置

除满足第2级的要求之外，还应满足：

- a) 应制定安全事件报告和响应处理程序，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等；
- b) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存；
- c) 对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序。

6.3.5.5.12 应急预案管理

除满足第2级的要求之外，还应满足：

- a) 应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障；
- b) 应定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期；
- c) 应规定应急预案需要定期审查和根据实际情况更新等内容，并按照执行。

6.4 第3.2级要求

同第3.1级要求。

6.5 第4级要求

同第3.2级要求。

6.6 第5级要求

待补充。

7 安全防护评测实施指南

7.1 第1级要求

7.1.1 业务及应用安全

不作要求。

7.1.2 网络安全

不作要求。

7.1.3 设备及软件系统安全

不作要求。

7.1.4 物理环境安全

不作要求。

7.1.5 管理安全

不作要求。

7.2 第2级要求

7.2.1 业务及应用安全检测要求

7.2.1.1 身份鉴别

身份鉴别要求如下：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查对提供登录功能的搜索系统，是否提供专用的登录控制模块对登录系统的业务用户进行身份标识和鉴别；
- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查对提供登录功能的搜索系统，是否提供并启用业务用户身份标识唯一检查功能，保证系统中不存在重复用户身份标识，身份鉴别信息不易被冒用。

7.2.1.2 访问控制

访问控制要求如下：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查对提供登录功能的搜索系统应提供访问控制功能，是否依据安全策略控制业务用户、管理用户对系统文件、数据库表等客体的访问，控制粒度为单个用户；
- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查对提供登录功能的搜索系统，是否提供并启用业务用户登录认证策略，如防范暴力破解、限定失败登录次数、锁定时间等。

7.2.1.3 安全审计

安全审计要求如下：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查对提供登录功能的搜索系统，是否提供覆盖到系统每个业务用户帐号的安全审计功能，至少应对业务用户关键操作、重要行为、业务资源使用情况、系统重要安全事件等进行审计；
- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查对提供登录功能的搜索系统，是否保证无法删除、修改或覆盖审计记录；
- c) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查对提供登录功能的搜索系统，审计记录的内容是否至少应包括事件日期、时间、发起者信息、类型、描述和结果等。

7.2.1.4 数据安全性

数据安全性要求如下：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查对提供登录功能的搜索系统，业务用户登录是否进行会话初始验证；

- b) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查对提供登录功能的搜索系统, 是否提供用户登录认证过程数据加密传输功能;
- c) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查对提供搜索的系统, 是否保证向用户展示的搜索结果(如文本、图片、应用软件等)不被篡改。

7.2.1.5 资源控制

资源控制要求如下:

- a) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查对提供登录功能的搜索系统, 当系统通信的会话中的一方在一段时间内未作任何响应, 另一方是否能够自动结束会话;
- b) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查对提供登录功能的搜索系统, 是否能够对单个业务用户的多重并发会话进行限制。

7.2.1.6 信息保护

信息保护要求如下:

- a) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查搜索系统是否在获得用户数据信息时征得用户同意, 并采取传输加密等措施保障相应数据的传输安全, 防止传输过程中泄漏;
- b) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查若搜索系统发生用户信息泄漏是否依据与用户签订的合同协议对用户进行赔偿;
- c) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查搜索系统是否采取充分的安全保障措施保障用户数据信息的存储安全, 并保障存储系统的安全, 防止存储过程中泄漏;
- d) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查搜索系统是否妥善保存存储有用户信息数据的纸质资料、电子介质等;
- e) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查搜索系统是否在用户申请、审核及投诉处理过程中使用用户数据信息外, 不得将用户数据信息用于任何其他用途;
- f) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查搜索系统是否采取措施加强对接触到用户数据信息人员的管理, 严格控制接触用户信息的人员范围, 合理设定用户信息操作权限, 防止出现人为的信息泄漏事件;
- g) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查搜索系统是否当明确告知用户收集和处理用户个人信息的方式、内容和用途以及信息泄漏风险, 并向用户说明本系统要采取的信息保护措施, 不得将用户提交的资料和信息泄露给他人, 利用该信息牟利。在与用户签署的相关合同中, 应明确规定运营企业对用户信息安全承担保护责任, 写明采取的具体信息保护措施;
- h) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查搜索系统是否对信息安全防护工作进行定期检查或抽查, 发现有违规行为时, 可以依据相关协议等追究其责任。

7.2.1.7 Web 安全防护

Web安全防护要求如下:

- a) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查搜索系统是否对所有来源的输入进行验证并使用白名单验证方法;
- b) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查搜索系统是否具备统一的验证接口, 向整个应用系统提供一致的验证方法, 并降低开发与代码维护的工作量;
- c) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查搜索系统是否在服务器端进行输入验证, 避免客户端输入验证被绕过;
- d) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查搜索系统是否对输入内容进行规范化处理后再进行验证, 如文件路径、URL 地址等;
- e) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查搜索系统是否采用有效手段防止关键参数被篡改, 关键参数应直接从服务器端提取, 避免从客户端输入;
- f) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查搜索系统是否确保用户不能访问到未授权的功能和数据, 并使用未经授权的用户访问受限资源, 验证系统是否予以拒绝或提示用户进行身份鉴权;
- g) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查搜索系统是否在服务器端实现对系统内受限资源的访问控制, 避免客户端访问控制被绕过;
- h) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查搜索系统是否采用统一的访问控制机制, 访问控制策略是否不可被非法修改;
- i) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查系统是否确保会话的安全创建, 在用户认证成功后, 是否为用户创建新的会话并释放原有会话, 创建的会话标识是否满足随机性和长度要求, 避免被攻击者猜测 (如采用会话与 IP 地址绑定的方式), 降低会话被盗用的风险;
- j) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查搜索系统是否确保会话数据的存储安全, 用户登录成功后所生成的会话数据是否存储在服务器端, 会话数据是否不能被非法访问, 当更新会话数据时, 是否对数据进行严格的输入验证, 以免会话数据的非法篡改;
- k) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查搜索系统是否确保会话数据的传输安全, 防止泄露会话标识;
- l) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查搜索系统是否确保会话的安全终止, 当用户登录成功并成功创建会话后, 是否在 web 应用系统的各个页面提供用户登出功能, 登出时是否及时删除服务器端的会话数据; 当处于登录状态的用户直接关闭浏览器时, 是否提示用户执行安全登出或者自动为用户完成登出过程, 从而安全的终止本次会话;
- m) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查搜索系统是否设置合理的会话超时阈值, 超过会话超时阈值后, 是否立刻销毁会话, 清除会话的信息;
- n) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查搜索系统是否限制会话并发连接数, 是否限制同一用户的会话并发连接数;
- o) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查搜索系统在涉及到关键业务操作的 web 页面, 是否为用户提供保障会话安全的补充机制 (如以 web 页面一次性随机令牌的方式, 作为主会话标识的补充)。

7.2.1.8 对外能力接口安全

对外能力接口安全要求如下：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统是否提供数据有效性检验功能，通过接口输入或通过通信接口输入的数据格式或长度是否符合系统设定要求；
- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统是否为各个接口分别设置专门前置服务器，是否通过前置服务器的接口应用实现内外系统的交互；
- c) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统接口数据传输是否采用加密方式，并通过协议分析工具对数据加密情况进行分析验证；
- d) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统接口数据传输是否进行校验，并通过协议分析工具对传输过程中数据的完整性进行分析验证；
- e) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统接口认证信息是否以密文的形式单独存储在配置文件中；
- f) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统是否对接口的状态和交互过程进行监控，是否支持异常恢复。

7.2.1.9 恶意代码防范

恶意代码防范要求如下：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统是否具备恶意代码过滤功能，是否对通过该平台对外发布的公共信息使用自动程序过滤和人工检查结合的方式进行恶意代码检查、屏蔽和删除，防止恶意代码通过业务网络向公众传播；
- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统是否将被屏蔽的含有恶意代码的搜索结果相关信息告知搜索用户。

7.2.2 网络安全检测要求

7.2.2.1 网络结构安全

网络结构安全要求如下：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统是否绘制与当前运行情况相符的系统拓扑结构图；
- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统是否根据搜索系统应用和服务的特点，在满足高峰期流量需求的基础上，合理设计带宽。

7.2.2.2 入侵防范

应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统是否在系统边界部署访问控制设备，并启用有效的访问控制策略。

7.2.2.3 安全审计

安全审计要求如下：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统是否对系统中的重要设备运行状况、网络流量监测信息、系统管理及维护等进行日志记录，并且保留一定期限（至少 180 天）；
- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统审计记录是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

7.2.3 设备及软件系统安全检测要求

7.2.3.1 网络及安全设备

网络及安全设备要求如下：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统各类路由器、交换机等网络设备是否满足相关行业标准要求，具有进网许可证；
- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统是否对登录网络设备（例如路由器、交换机）以及安全设备（例如入侵检测设备、防火墙设备）的用户进行有效的身份标识和鉴别；
- c) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中网络及安全设备管理用户的标识是否唯一；
- d) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中网络及安全设备管理用户口令是否不小于 8 字节，口令应有复杂度要求（如使用大写字母、小写字母、数字、标点及特殊字符五种字符中至少二种的组合，且与用户名或身份标识无相关性）并定期更换（更新周期不大于 90 天）。

7.2.3.2 通用主机操作系统

7.2.3.2.1 安全检测

安全检测要求如下：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的计算机运维终端、服务器等设备的主机操作系统，出具安全测试及验收报告并妥善保存，相关设备的安全应满足相应设备技术规范、设备安全要求等行业标准的相关规定；
- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的计算机运维终端、服务器等设备的主机操作系统是否遵循最小安装的原则，仅安装和开通需要的功能组件和应用程序，并通过安全方式（如设置升级服务器）保持系统补丁及时得到更新；
- c) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的计算机运维终端、服务器等设备的主机操作系统是否定期进行安全监测，发现并加固操作系统相关漏洞，避免业已发现的漏洞造成安全事件。

7.2.3.2.2 身份鉴别

身份鉴别要求如下：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查是否搜索系统中各个功能模块的计算机运维终端、服务器等设备的主机操作系统的用户进行身份标识和鉴别；
- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查是否搜索系统中各个功能模块的计算机运维终端、服务器等设备的主机操作系统的不同用户分配不同的用户名，确保用户名具有唯一性；
- c) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的计算机运维终端、服务器等设备的主机操作系统的管理用户身份标识是否具有不易被冒用的特点，相关用户口令长度应不小于 8 字节，口令应有复杂度要求（使用大写字母、小写字母、数字、标点及特殊字符五种字符中至少二种的组合，且与用户名或身份标识无相关性）并定期更换（更新周期不大于 90 天）。

7.2.3.2.3 访问控制

访问控制要求如下：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的计算机运维终端、服务器等设备是否启用访问控制功能，依据安全策略控制用户对资源的访问；
- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的计算机运维终端、服务器等设备是否及时删除多余的、过期的账户，避免共享账户的存在；
- c) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的计算机运维终端、服务器等设备是否实现操作系统和数据库系统特权用户的权限分离；
- d) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的计算机运维终端、服务器等设备是否限制默认账户的访问权限，修改这些账户的默认口令，条件允许下，应重命名默认账户。

7.2.3.2.4 安全审计

安全审计要求如下：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的计算机运维终端、服务器等设备的审计范围是否覆盖到主机/服务器上的每个操作系统用户；
- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的计算机运维终端、服务器等设备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) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的计算机运维终端、服务器等设备的审计记录是否包括事件的日期、时间、类型、主体标识、客体标识和结果等。

7.2.3.2.5 恶意代码防范

恶意代码防范要求如下：

- a) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查搜索系统中各个功能模块的计算机运维终端、服务器等设备是否安装防范病毒、木马等恶意代码的软件, 并及时更新防恶意代码软件版本和恶意代码库;
- b) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查搜索系统中各个功能模块的计算机运维终端、服务器等设备是否支持防恶意代码的统一管理。

7.2.3.2.6 资源控制

资源控制要求如下:

- a) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查搜索系统中各个功能模块的服务器是否通过设定计算机运维终端接入方式、网络地址范围等条件限制管理终端登录;
- b) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查搜索系统中各个功能模块的服务器是否根据安全策略设置计算机运维终端的操作超时锁定;
- c) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查搜索系统中各个功能模块的服务器是否限制单个用户对主机资源的最大或最小使用限度。

7.2.3.2.7 冗余备份

应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查搜索系统中各个功能模块的服务器是否具备一定的冗余备份, 关键设备、重要部件应采用冗余的方式提供保护。

7.2.3.3 数据库及中间件软件

7.2.3.3.1 安全检测

安全检测要求如下:

- a) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查是否应对搜索系统中各个功能模块的数据库及中间件软件进行必要的安全检测, 出具安全测试及验收报告并妥善保存, 相关设备的安全应满足相应设备技术规范、设备安全要求等行业标准的相关规定;
- b) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查搜索系统中各个功能模块的数据库及中间件软件是否遵循最小安装的原则, 仅安装和开通需要的功能组件和应用程序, 并通过安全方式(如设置升级服务器)保持系统补丁及时得到更新;
- c) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查是否对搜索系统中各个功能模块的数据库及中间件软件应定期进行安全监测, 发现并加固操作系统相关漏洞, 避免业已发现的漏洞造成安全事件。

7.2.3.3.2 身份鉴别

身份鉴别要求如下:

- a) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查是否应搜索系统中各个功能模块的数据库及中间件软件的用户进行身份标识和鉴别;
- b) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查是否搜索系统中各个功能模块的数据库及中间件软件的不同用户分配不同的用户名, 确保用户名具有唯一性;

- c) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查是否对搜索系统中各个功能模块的数据库及中间件软件的管理用户身份标识应具有不易被冒用的特点，相关用户口令长度应不小于 8 字节，口令应有复杂度要求（使用大写字母、小写字母、数字、标点及特殊字符五种字符中至少二种的组合，且与用户名或身份标识无相关性）并定期更换（更新周期不大于 90 天）。

7.2.3.3.3 访问控制

访问控制要求如下：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的数据库及中间件软件是否启用访问控制功能，依据安全策略控制用户对资源的访问；
- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的数据库及中间件软件是否及时删除多余的、过期的账户，避免共享账户的存在；
- c) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的数据库及中间件软件是否实现数据库、中间件特权用户与操作系统的权限分离；
- d) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的数据库及中间件软件是否限制默认账户的访问权限，修改这些账户的默认口令，条件允许下，应重命名默认账户。

7.2.3.3.4 安全审计

安全审计要求如下：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的数据库及中间件软件的审计范围是否覆盖到主机/服务器上的每个操作系统用户；
- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的数据库及中间件软件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) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的数据库及中间件软件的审计记录是否包括事件的日期、时间、类型、主体标识、客体标识和结果等。

7.2.3.3.5 资源控制

资源控制要求如下：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的数据库及中间件软件是否通过设定计算机运维终端接入方式、网络地址范围等条件限制管理终端登录；
- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的数据库及中间件软件是否根据安全策略设置计算机运维终端的操作超时锁定；

- c) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的数据库及中间件软件是否限制单个用户对主机资源的最大或最小使用限度。

7.2.3.3.6 冗余备份

应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的数据库及中间件软件是否具备一定的冗余备份，关键设备、重要部件应采用冗余的方式提供保护。

7.2.4 物理环境安全检测要求

7.2.4.1 物理位置的选择

物理位置选择要求如下：

- a) 应访谈物理安全负责人，询问现有机房和办公场地是否具有基本的防震、防风 and 防雨等能力，是否出现过由于防震、防风、防雨能力不足造成的安全事件，有没有及时采取补救措施；检查机房和办公场地的设计/验收文档，查看是否有机房和办公场地所在地建筑能够具有防震、防风 and 防雨等能力的说明；应检查机房和办公场地是否在具有防震、防风 and 防雨等能力的建筑内；
- b) 应查看机房设计文档，检查机房承重是否满足承重要求。

7.2.4.2 物理访问控制

物理访问控制要求如下：

- a) 检查机房是否指定了专人在机房出入口值守；进入机房的人员身份鉴别措施（如戴有可见的身份标识）；查看是否有来访人员进入机房的审批记录；
- b) 询问机房管理人员，来访人员是否须经批准审核，在来访过程中限制和监控其活动范围；查看是否具有来访人员审批表，检查限制和监控人员活动范围的措施等是否到位。

7.2.4.3 防盗窃和防破坏

防盗窃和防破坏要求如下：

- a) 应访谈机房维护人员，询问并现场查看主要设备是否放置在机房内；
- b) 应检查设备或设备的主要部件的固定情况，是否不易被移动或被搬走，是否设置明显的无法除去的标记；
- c) 应检查室外通信线缆敷设是否在隐蔽处：铺设在地下或管道中；
- d) 应访谈资产管理员，在介质管理中，是否进行了分类标识，是否存放在介质库或档案室中，且进行分类存放（满足磁介质、纸介质等的存放要求）；
- e) 应访谈机房维护人员，询问并现场查看主机房是否安装了必要的防盗报警设施。

7.2.4.4 防雷击

防雷击要求如下：

- a) 应访谈物理安全负责人，询问机房建筑是否设置了避雷装置，是否通过验收或国家有关部门的技术检测；应访谈机房维护人员，询问机房建筑避雷装置是否有人定期进行检查和维护；应检查是否具有机房建筑避雷装置定期检查和维护记录；
- b) 应检查机房是否设置了交流电源地线；应检查机房是否有建筑防雷设计/验收文档，机房接地设计/验收文档，是否有地线连接要求的描述，与实际情况是否一致；

- c) 应检查机房是否有建筑防雷设计/验收文档，机房接地设计/验收文档，查看是否满足 YD 5098-2005 中相关要求。

7.2.4.5 防火

防火要求如下：

- a) 应检查机房是否设置了灭火装置（灭火器），摆放位置是否合理，有效期是否合格；应检查机房是否设置了火灾自动报警系统，该系统是否正常工作，查看运行记录、报警记录、定期检查和维修记录；
- b) 应检查是否有机房防火设计/验收文档，文档是否与现有消防配置状况一致，是否满足 YD 5002 中相关要求。

7.2.4.6 防水和防潮

防水和防潮要求如下：

- a) 应访谈物理安全负责人，机房内是否有上下水管安装，现场检查机房的实际情况是否满足水管安装不得穿过机房屋顶和活动地板下的要求；
- b) 应访谈物理安全负责人，询问是否采取了防止雨水通过机房窗户、屋顶和墙壁渗透的措施，并现场进行检查机房是否不存在窗户、屋顶和墙壁等出现过漏水、渗透和返潮现象；
- c) 应访谈机房维护人员，询问机房是否采取了避免水蒸气结露和地下积水的转移与渗透的防范措施；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，与机房湿度记录情况是否一致。

7.2.4.7 防静电

应访谈物理安全负责人，询问机房内的关键设备是否采用了必要的接地等防静电措施，是否有控制机房湿度的措施；应检查机房内关键设备是否有安全接地，查看机房的相对湿度的记录，查看机房是否存在明显的静电现象。

7.2.4.8 温湿度控制

应访谈物理安全负责人，询问机房是否配备了恒温恒湿系统，保证温湿度能够满足设备运行的要求，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；应检查恒温恒湿系统是否能够正常运行，查看是否有温湿度记录、运行记录和维护记录。

7.2.4.9 防尘

应访谈物理安全负责人，询问机房是否防尘措施；应检查出入机房是否使用鞋套，是否有专人定期对机房进行除尘工作，是否有防尘走廊；应检查是否有防尘记录、运行记录和维护记录。

7.2.4.10 电力供应

电力供应要求如下：

- a) 应访谈物理安全负责人，询问机房供电线路上是否设置了稳压器和过电压防护设备；应检查机房，查看机房供电线路上的稳压器、过电压防护设备是否正常运行，查看供电电压是否正常；
- b) 应访谈物理安全负责人，询问是否设置了短期备用电源设备（如 UPS），供电时间是否满足系统最低电力供应需求；应检查短期备用电源设备等电源设备的检查和维护记录，应定期对备用电源设备进行充放电检查。

7.2.4.11 电磁防护

应访谈机房维护人员，询问是否做到电源线和通信线缆隔离；应检查机房布线，查看是否做到电源线和通信线缆隔离。

7.2.5 管理安全检测要求

7.2.5.1 安全管理制度

7.2.5.1.1 管理制度

管理制度要求如下：

- a) 检查网络安全工作的总体方针、政策性文件和安全策略文件，查看文件是否明确机构安全工作的总体目标、范围、方针、原则、责任等；
- b) 检查安全管理制度，查看文件是否明确安全管理活动中重要的管理内容；
- c) 检查是否有日常管理操作的操作规程，如网络维护手册和用户操作规程等，是否规定了管理人员或操作人员执行的重要管理操作。

7.2.5.1.2 制定和发布

制定和发布要求如下：

- a) 访谈安全主管，是否指定或授权专门的部门或人员负责安全管理制度的制定；检查安全管理制度文档；
- b) 访谈安全主管，询问安全管理制度的制定程序，是否对制定的安全管理制度进行论证和评审，论证和评审方式如何（如召开评审会、函审、内部审核等）；检查管理制度评审记录，查看是否有相关人员的评审意见；
- c) 访谈安全主管，安全管理制度以何种方式发布，是否能正确地发布到相关人员手中。

7.2.5.1.3 评审和修订

访谈安全主管，询问是否定期对安全管理制度体系的合理性和适用性进行评审，评审周期多长；发现存在不足或需要改进时是否进行修订，检查是否有相关记录。

7.2.5.2 安全管理机构

7.2.5.2.1 岗位设置

岗位设置要求如下：

- a) 访谈相关负责人员，询问是否设立安全主管以及安全管理各个方面的负责人岗位，是否明确各个岗位的职责分工；
- b) 访谈安全主管，询问设置了哪些工作岗位，是否包含专职的网络安全技术员等重要岗位，检查岗位职责文件，是否明确各个岗位的职责分工。

7.2.5.2.2 人员配备

访谈安全主管，询问各个安全管理和技术岗位人员（按照岗位职责文件询问，包括系统安全管理员、技术员等重要岗位人员）配备情况，数量是否充足；检查人员配备要求管理文档，查看是否明确应配备哪些安全管理和技术人员等重要岗位人员。

7.2.5.2.3 授权和审批

授权和审批要求如下：

- a) 访谈安全主管，对系统投入运行、割接、升级和重要资源的访问等关键活动是否有相应的审批部门及批准人；检查授权审批管理文件，查看文件是否明确审批事项、审批部门、审批人等；
- b) 访谈安全主管，询问针对关键活动是否建立审批流程，是否由批准人签字确认；检查关键活动的审批记录。

7.2.5.2.4 沟通和合作

沟通和合作要求如下：

- a) 访谈安全主管，询问各类内部人员、机构之间沟通、合作机制；访谈安全主管，询问是否召开过部门间协调会议，组织其它部门人员共同协助处理网络安全有关问题；检查部门间协调会议以及网络安全职能部门内部会议文件或会议记录，查看是否有会议内容、会议时间、参加人员和结果等的描述；
- b) 访谈安全主管，询问是否经常与相关外部单位联系，联系方式有哪些；检查外联单位说明文档，查看说明文档是否包含全部经常联系的外部单位，是否说明外联单位的联系人和联系方式等内容。

7.2.5.2.5 审核和检查

访谈安全管理人员，询问是否组织人员定期对网络进行安全检查，检查周期多长，检查人员有哪些；安全检查包含哪些内容，是否包括用户帐号情况、系统漏洞情况、数据备份情况等。

7.2.5.3 人员安全管理

7.2.5.3.1 人员录用

人员录用要求如下：

- a) 访谈人事负责人，是否指定或授权专门的部门或人员负责人员录用；
- b) 访谈人事工作人员，询问在人员录用时是否对被录用人的身份、背景、专业资格进行审查；检查是否具有人员录用时对被录用人身份、背景、专业资格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；是否对技术人员的技术技能进行考核，检查技能考核文档或记录，查看是否记录考核内容和考核结果等；
- c) 访谈人事工作人员，询问是否与从事关键岗位的人员签署保密协议，查看保密协议。

7.2.5.3.2 人员离岗

人员离岗要求如下：

- a) 检查人员离岗的管理文档，查看是否规定了调离手续和离岗要求等，是否要求及时终止离岗员工的所有访问权限；
- b) 访谈安全主管，询问人员离岗时是否取回各种身份证件、钥匙等以及工作配备的软硬件设备等；
- c) 访谈安全主管，询问人员离岗是否办理了严格的离岗手续，检查人员离岗记录。

7.2.5.3.3 人员考核

访谈安全主管，询问是否定期对各个岗位人员进行安全技能及安全知识的考核；检查考核记录，查看记录的考核人员是否包括各个岗位的人员，考核内容是否包含安全知识、安全技能等；查看记录日期与考核周期是否一致。

7.2.5.3.4 人员和技术支持能力

应访谈安全负责人、其他相关人员，并检查人员任职信息、责任岗位规章、人员管理制度、培训考核记录，检查验证相关网络安全管理和技术人员是否接受并通过技术培训和考核。

7.2.5.3.5 安全意识教育和培训

安全意识教育和培训要求如下：

- a) 访谈安全主管，询问是否制定安全教育和培训计划并按计划对各个岗位人员进行安全意识教育、岗位技能培训和相关安全技术培训；检查是否具有安全教育和各类培训记录，查看记录是否有培训人员、培训内容、培训结果等的描述；查看记录与培训计划是否一致；
- b) 访谈安全主管，询问对违反违背安全策略和规定的人员是否有相应的惩戒措施；访谈各类人员，考查其对安全责任和惩戒措施等的理解程度；
- c) 访谈安全主管，是否制定了安全教育和培训计划，是否对网络安全基础知识、岗位操作规程等进行培训；检查安全教育和培训计划相关文档。

7.2.5.3.6 外部人员访问管理

访谈安全管理人员，询问对外部人员访问受控区域（如访问主机房、重要服务器或设备、保密文档等）前是否得到授权或审批，批准后是否由专人全程陪同或监督，并登记备案；检查外部人员访问受控区域的授权或审批记录，查看记录是否描述了外部人员访问受控区域的进入时间、离开时间、访问区域、访问设备或信息及陪同人等信息。

7.2.5.4 安全建设管理

7.2.5.4.1 定级

定级要求如下：

- a) 检查定级文档，查看是否明确网络边界和定级；
- b) 检查定级文档，查看是否明确描述网络边界划分的方法和确定安全保护等级的理由；
- c) 访谈安全主管，询问定级结果是否按主管部门要求及时上报、审批、备案。

7.2.5.4.2 安全方案设计

安全方案设计要求如下：

- a) 访谈网络建设负责人，询问是否根据网络的安全等级保护级别选择基本安全措施，是否依据风险评估的结果补充和调整安全措施，做过哪些调整；
- b) 检查网络安全方案文档，是否包括对网络的安全保护要求、策略和措施等内容；
- c) 检查网络详细设计方案文档，是否应对安全方案进行细化，形成能指导安全系统建设、安全产品采购和使用的具体设计方法；
- d) 访谈网络建设负责人，是否组织相关部门和有关安全技术专家对安全设计方案的合理性和正确性进行论证和审定，相关的安全方案在实施前是否经过批准后；检查专家论证和审定文档，检查安全方案实施的批准记录。

7.2.5.4.3 产品采购

产品采购要求如下：

- a) 访谈系统建设负责人，询问是否采用了安全产品，安全产品的采购和使用是否符合国家有关规定；

- b) 访谈系统建设负责人, 询问是否采用了密码产品, 密码产品的使用是否符合国家密码主管部门的要求;
- c) 访谈系统建设负责人, 询问是否有专门的部门负责产品的采购, 由何部门负责。

7.2.5.4.4 自行软件开发

自行软件开发要求如下:

- a) 访谈系统建设负责人, 询问是否自行开发软件, 开发环境与实际运行环境是否物理分开;
- b) 检查是否具备制定软件开发管理制度, 查看其是否说明开发过程的控制方法和人员行为准则;
- c) 访谈系统建设负责人, 询问是否提供软件设计的相关文档和使用指南, 是否由专人负责保管; 检查是否具有软件设计文档和软件使用指南。

7.2.5.4.5 外包软件开发

外包软件开发要求如下:

- a) 访谈网络建设负责人, 询问软件交付前是否依据开发需求对软件功能和性能等进行验收检测;
- b) 访谈网络建设负责人, 开发单位是否提供软件设计的相关文档和使用指南, 检查软件设计的相关文档和使用指南;
- c) 访谈网络建设负责人, 应在软件安装之前检测软件包中可能存在的恶意代码, 查看检测记录。

7.2.5.4.6 工程实施

工程实施要求如下:

- a) 访谈网络建设负责人, 是否指定或授权专门的部门或人员负责工程实施过程的管理;
- b) 访谈网络建设负责人, 是否制定详细的工程实施方案, 控制工程实施过程; 检查工程实施方案, 查看其是否覆盖工程时间限制、进度控制和质量控制等方面内容。

7.2.5.4.7 测试验收

测试验收要求如下:

- a) 访谈网络建设负责人, 询问在网络正式运行前, 是否至少每年一次委托公正的第三方测试单位对定级网络单元进行安全性测试, 并出具安全性测试报告;
- b) 访谈网络建设负责人, 在测试验收前是否根据设计方案或合同要求等制订测试验收方案, 在测试验收过程中是否详细记录测试验收结果, 并形成测试验收报告; 检查测试验收方案、测试验收结果记录和测试验收报告, 验证相关测试覆盖网络安全相关内容。

7.2.5.4.8 交付

交付要求如下:

- a) 访谈网络建设负责人, 询问交接手续是什么, 是否有交付清单, 是否根据交付清单对所交接的设备、文档、软件等进行清点;
- b) 访谈网络建设负责人, 询问目前的运维技术人员是否进行过技能培训, 检查培训记录;

7.2.5.4.9 安全服务商的选择

安全服务商选择要求如下:

- a) 访谈安全主管, 是否使用安全服务商提供的安全服务器, 是否按国家有关规定选择安全服务商;
- b) 检查与安全服务商签订的安全相关协议查看, 查看其中是否明确约定相关责任;
- c) 访谈安全主管, 是否要求安全服务商提供技术支持和服务承诺, 是否与其签订服务合同。

7.2.5.5 安全运维制度

7.2.5.5.1 运行维护能力

运行维护能力要求如下：

- a) 应访谈安全管理人员、各相关管理、技术、运维人员，询问是否有机房管理制度，询问机房管理制度覆盖的范围，检查验证是否具有完整的运行维护管理制度，管理制度是否涵盖业务管理和控制、系统运行、设备操作和维护等方面；
- b) 应访谈安全管理人员、各相关管理、技术、运维人员，询问是否有机房管理制度，询问机房管理制度覆盖的范围，检查验证是否按照统一的运行维护要求，对业务及应用系统进行规范化的维护；
- c) 应访谈安全管理人员、各相关管理、技术、运维人员，检查机房管理制度覆盖的范围，验证是否有业务及应用系统相关介质存取、验证和转储的管理制度，检查或测试验证是否能确保有关备份数据、信息的授权访问；
- d) 应访谈安全管理人员、各相关管理、技术、运维人员，检查验证是否建立和保持与其他部门、外部单位间良好的联络和协作机制，是否具有正常对外联络和协作能力。

7.2.5.5.2 环境管理

环境管理要求如下：

- a) 访谈系统管理员，询问是否指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理；检查维护管理文档；
- b) 访谈系统管理员，询问是否配备机房安全管理人员，是否对机房的出入、服务器的开机或关机等工作进行管理；检查机房出入记录、服务器开关机记录；
- c) 访谈系统管理员，询问是否建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定；检查机房安全管理制度文档；
- d) 访谈安全管理人员，询问是否加强对办公环境的保密性管理，工作人员调离办公室是否立即交还该办公室钥匙，是否不在办公区接待来访人员等。

7.2.5.5.3 资产管理

资产管理要求如下：

- a) 访谈资产管理员，是否编制与网络相关的资产清单；检查资产清单，是否包括资产责任部门、重要程度和所处位置等内容；
- b) 访谈资产管理员，是否建立资产安全管理制度；检查资产安全管理制度文档，是否规定资产管理的责任人员或责任部门，并规范资产管理和使用的行为。

7.2.5.5.4 介质管理

介质管理要求如下：

- a) 访谈资产管理员，询问介质是否存放在安全的环境中，是否对各类介质进行控制和保护，并实行存储环境专人管理，查看介质存放地点，是否符合相关要求；
- b) 访谈资产管理员，询问是否对介质归档和查询等过程进行记录，并根据存档介质的目录清单定期盘点；检查介质管理记录，查看其是否记录介质的归档、查询等情况；
- c) 访谈资产管理员，询问是否对需要送出维修或销毁的介质，清除其中的敏感数据；
- d) 访谈资产管理员，询问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；检查介质，查看是否对其进行了分类，并具有不同标识。

7.2.5.5.5 设备管理

设备管理要求如下：

- a) 访谈资产管理，询问网络相关的各种设备（包括备份和冗余设备）、线路等是否指定专门的部门或人员定期进行维护管理，由何部门/何人维护，维护周期多长；检查设备、线路维护文档。
- b) 访谈资产管理，询问是否建立基于申报、审批和专人负责的设备安全管理制度，是否对设备选用的各个环节（选型、采购、发放、领用等）进行规范化管理；检查设备审批、发放管理文档，查看其内容是否对设备选型、采购、发放和领用等环节的申报和审批作出规定；
- c) 访谈系统管理员，询问是否对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现关键设备（包括备份和冗余设备）的启动/停止、加电/断电等操作；检查服务器操作规程，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；
- d) 应访谈系统管理员，询问信息处理设备是否经过审批才能带离机房或办公地点；检查相关审批记录。

7.2.5.5.6 网络安全管理

网络安全管理要求如下：

- a) 访谈安全主管，询问是否指定人员负责网络运行日志、网络监控记录的日常维护和报警信息分析和处理工作；
- b) 访谈安全管理人员，询问是否建立网络安全管理制度，检查网络安全管理制度文档，查看其是否包含网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面的规定。

7.2.5.5.7 恶意代码防范管理

恶意代码防范管理要求如下：

- a) 访谈网络运维负责人，询问是否对员工进行基本恶意代码、病毒防范意识教育，如告知应及时升级防病毒软件，在读取移动存储设备上的数据以及网络上接收文件或邮件之前先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查；
- b) 访谈网络运维负责人，询问是否指定专人对恶意代码、病毒进行检测，并保存记录；检查是否具有恶意代码检测记录；
- c) 检查恶意代码、病毒防范管理制度，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。

7.2.5.5.8 密码管理

访谈安全主管，如采用了密码技术和产品，是否符合国家密码管理规定。

7.2.5.5.9 变更管理

变更管理要求如下：

- a) 访谈网络运维负责人，询问是否制定变更方案指导网络执行变更；检查系统变更方案，查看其是否对变更类型、变更原因、变更过程、变更前评估等方面进行说明；
- b) 访谈网络运维负责人，询问重要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；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；检查重要系统的变更申请书，查看其是否有主管领导的签字批准。

7.2.5.5.10 备份与恢复管理

备份与恢复管理要求如下：

- a) 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重要业务信息、系统数据及软件系统；
- b) 检查备份管理文档，是否规定备份信息的备份方式（如增量备份或全备份等）、备份频度（如每日或每周等）、存储介质、保存期；
- c) 检查数据的备份策略和恢复策略文档，是否考虑了数据的重要性和数据对系统运行的影响，是否指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法。

7.2.5.5.11 安全事件处置

安全事件处置要求如下：

- a) 访谈系统管理人员、网络管理人员、安全管理人员，询问是否被告知在发现安全脆弱性和可疑事件时应及时报告；
- b) 访谈安全管理人员，询问是否制定安全事件报告和处置管理制度；检查安全事件报告和处置管理制度，是否明确安全事件类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责；
- c) 访谈安全管理人员，询问是否对根据安全事件对本网络产生的影响，对本网络安全事件进行等级划分；检查安全事件定级文档，查看其内容是否明确安全事件的定义、安全事件等级划分的原则、等级描述等方面内容；
- d) 访谈安全管理人员，询问是否记录并保存所有发现的安全弱点和可疑事件，分析事件原因，监督事态发展，采取措施避免安全事件发生；检查安全事件报告和处理程序文档。

7.2.5.5.12 应急预案管理

应急预案管理要求如下：

- a) 访谈网络运维负责人，询问是否制定不同事件的应急预案；检查应急预案；
- b) 访谈网络运维负责人，询问是否对网络相关人员进行应急预案培训，应急预案培训是否至少一年一次；检查应急预案培训记录。

7.3 第3.1级要求

7.3.1 业务及应用安全检测要求

7.3.1.1 身份鉴别

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查对提供登录功能的搜索系统，是否提供并启用用户身份标识唯一检查功能，保证系统中不存在重复用户身份标识；
- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查对提供登录功能的搜索系统，是否提供并启用用户登录认证口令复杂度强度功能，保证业务用户的口令长度应不小于8字节，口令应有复杂度要求（使用大写字母、小写字母、数字、标点及特殊字符等类字符中至少二种的组合，且与用户名或身份标识无相关性）并定期更换（更新周期不大于90天）；

7.3.1.2 访问控制

除按照第2级的要求进行检测之外，还应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查对提供登录功能的搜索系统，是否严格设置业务用户解锁策略，按安全策略要求，被锁定的业务用户需通过注册时的标志信息进行密码重新设定或者凭有效证件进行设定。

7.3.1.3 安全审计

除按照第2级的要求进行检测之外，还应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查对提供登录功能的搜索系统，是否提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

7.3.1.4 数据安全性

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查对提供登录功能的搜索系统，是否保证采用足够强壮的加密算法保证用户登录认证过程数据不被非授权利用和篡改。
- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查是否提供登录功能的搜索系统，应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据符合系统设定要求，确保非常规数据被过滤。

7.3.1.5 资源控制

除按照第2级的要求进行检测之外，还应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统是否对通过该平台对外发布的公共信息使用自动程序过滤和人工检查结合的方式进行恶意代码检查、屏蔽和删除，防止含恶意代码页面通过业务网络向公众传播。

7.3.1.6 信息保护

除按照第2级的要求进行检测之外，还应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查对提供登录功能的搜索系统，是否保护系统服务相关信息的安全，避免有关数据被篡改和破坏。

7.3.1.7 Web 安全防护

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查web程序上线前或升级后是否进行代码审计，形成报告，并对审计出的问题进行代码升级完善；
- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查是否避免使用含有已公开漏洞的开源第三方应用组件及代码（漏洞库可参考 CVE、CNVD 等）。

7.3.1.8 对外能力接口安全

同第2级要求。

7.3.1.9 恶意代码防范

除按照第2级的要求进行检测之外，还应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查对提供登录功能的搜索系统，是否禁止不必要的内嵌网络服务，应禁止在用户端自动安装恶意软件和插件。

7.3.2 网络安全检测要求

7.3.2.1 网络结构安全

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统是否根据系统内部网络结构特点，按照统一的管理和控制原则划分不同的子网或网段，设备依照功能划分及其重要性等因素分区部署；
- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查不考虑主动宕机维护的情况，搜索系统是否年宕机时间不超过 4.38 小时，可靠性是否达到 99.95% 以上；
- c) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统是否具备必要的流量负荷分担设计。

7.3.2.2 入侵防范

除按照第2级的要求进行检测之外，还应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统是否在系统边界处对发生的网络入侵行为（包括但不限于端口扫描、强力攻击、木马后门攻击、DoS/DDoS攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击）提供有效的检测能力，当检测到入侵行为时应能记录攻击源IP、攻击类型、攻击目的、攻击时间。

7.3.2.3 安全审计

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统是否提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。
- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统是否根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，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；
- c) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统是否避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段；
- d) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统是否按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。

7.3.3 设备及软件操作系统安全检测要求

7.3.3.1 网络及安全设备

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统网络及安全设备是否启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统网络及安全设备是否通过设定终端接入方式、网络地址范围等条件限制管理终端登录；
- c) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统网络及安全设备进行远程管理时，是否采取必要措施防止鉴别信息在网络传输过程中被窃听。

7.3.3.2 通用主机操作系统

7.3.3.2.1 安全检测

同第2级要求。

7.3.3.2.2 身份鉴别

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的计算机运维终端、服务器等设备的主机操作系统是否启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；
- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的计算机运维终端、服务器等设备进行远程管理时，是否采取必要措施，防止鉴别信息在传输过程中被窃听。

7.3.3.2.3 访问控制

同第2级要求。

7.3.3.2.4 安全审计

除按照第2级的要求进行检测之外，还应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的计算机运维终端、服务器等设备的审计记录，是否避免其受到未预期的删除、修改或覆盖等，保留一定期限（至少180天）。

7.3.3.2.5 恶意代码防范

同第2级要求。

7.3.3.2.6 资源控制

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统是否对能够对各个模块的服务器进行性能和服务水平监控，监控方式可基于监听、SNMP 等网管技术和协议；并设定阈值，在监测到服务水平降低到阈值时进行报警；
- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的服务器是否保持时间上的同步。

7.3.3.2.7 冗余备份

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的服务器是否建立对操作系统关键数据（如操作系统配置数据、管理员操作维护记录、用户信息等）和重要信息进行备份和恢复的管理和控制机制；
- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中相关主机数据备份范围和时间间隔、数据恢复能力是否满足行业管理、业务运营企业应急预案相关要求。

7.3.3.3 数据库及中间件软件

7.3.3.3.1 安全检测

同第2级要求。

7.3.3.3.2 身份鉴别

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查是否搜索系统中各个功能模块的数据库及中间件软件应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；
- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查是否对搜索系统中各个功能模块的数据库及中间件软件进行远程管理时，应采取必要措施，防止鉴别信息在传输过程中被窃听。

7.3.3.3.3 访问控制

同第2级要求。

7.3.3.3.4 安全审计

除按照第2级的要求进行检测之外，还应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的数据库及中间件软件的审计记录是否，避免其受到未预期的删除、修改或覆盖等，保留一定期限（至少180天）。

7.3.3.3.5 资源控制

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中是否对各个功能模块的数据库及中间件软件行性能和服务水平监控，监控方式可基于监听、SNMP等网管技术和协议；并设定阈值，在监测到服务水平降低到阈值时进行报警；
- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的数据库及中间件软件是否保持时间上的同步。

7.3.3.3.6 冗余备份

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的数据库及中间件软件是否建立对关键数据（如配置数据、管理员操作维护记录、用户信息等）和重要信息进行备份和恢复的管理和控制机制；

- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查搜索系统中各个功能模块的数据库及中间件软件中相关数据备份范围和时间间隔、数据恢复能力是否满足行业管理、业务运营企业应急预案相关要求。

7.3.4 物理环境安全检测要求

7.3.4.1 物理位置的选择

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 应访谈物理安全负责人，询问现有机房的物理位置是否在建筑物的顶层或地下室，是否在用水设备的下层或隔壁；
- b) 对于有铁架安装的机房，应检查设计/验收文档，并实地检查机房铁架安装是否满足 YD/T 5026-2005 要求。

7.3.4.2 物理访问控制

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 应访谈物理安全负责人，是否对机房进行了划分区域管理，区域和区域之间是否设置了物理隔离装置；应检查机房区域划分是否合理，是否在机房重要区域前设置交付或安装等过渡区域；是否对不同的区域设置不同的物理机房，或者同一机房的区域之间是否设置有效的物理隔离装置（如隔墙等）；
- b) 应检查机房是否有电子门禁系统管理，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）；查看电子门禁系统运行、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的人员身份。

7.3.4.3 防盗窃和防破坏

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 应检查机房是否安装了利用光、电等技术的防盗报警系统；应访谈机房维护人员，询问是否对机房安装的防盗报警系统进行定期维护检查；应检查机房防盗报警设施是否正常运行，并查看运行和报警记录；
- b) 应检查机房是否安装了监控报警系统；应访谈机房维护人员，询问是否对机房安装的监控报警系统进行定期维护检查；应检查机房的摄像、传感等监控报警系统是否正常运行，并查看运行记录、监控记录和报警记录。

7.3.4.4 防雷击

除按照第2级的要求进行检测之外，还应访谈物理安全负责人，询问是否设置了防雷保安器，是否定期进行检查和维护；应检查是否有对防雷保安器定期检查和记录。

7.3.4.5 防火

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 应检查机房是否设置了自动检测火情（如使用温感、烟感探测器）、自动报警、自动灭火的自动消防系统；应检查自动消防系统是否正常工作，查看运行记录、报警记录、定期检查和维修记录；
- b) 应查看机房防火设计/验收文档，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；

- c) 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。

7.3.4.6 防水和防潮

除按照第2级的要求进行检测之外，还应检查机房是否安装了对水敏感的检测仪表或元件，对机房进行防水检测和报警；应检查检测仪表或元件是否正常工作，查看运行记录、报警记录、定期检查和维修记录。

7.3.4.7 防静电

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 应访谈物理安全负责人，询问机房内的主要设备是否采用了必要的接地等防静电措施，是否有控制机房湿度的措施；应检查机房内主要设备是否有安全接地；
- b) 应检查机房是否采用了防静电地板。

7.3.4.8 温湿度控制

同第2级要求。

7.3.4.9 防尘

同第2级要求。

7.3.4.10 电力供应

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 应访谈物理安全负责人，询问机房供电线路是否安装了冗余或并行的电力电缆线路（如双路供电方式）；询问冗余或并行的电力电缆线路（如双路供电方式）在双路供电切换时是否能够对机房正常供电；应检查冗余或并行的电力电缆线路（如双路供电方式，双路供电切换测试）定期检验的记录；
- b) 应访谈物理安全负责人，询问机房是否建立备用供电系统（如备用发电机）；是否定期检查备用供电系统（如备用发电机），是否能够在规定时间内正常启动和正常供电；应检查备用供电系统（如备用发电机）定期检测记录。

7.3.4.11 电磁防护

除按照第2级的要求进行检测之外，还应访谈物理安全负责人，询问是否有防止外界电磁干扰和设备寄生耦合干扰的措施（包括设备外壳有良好的接地，电源线和通信线缆隔离等）。

7.3.4.12 防鼠

应访谈相关管理和技术人员，询问互联网相关业务及应用系统所处机房是否采取防虫防鼠等保护措施，检查验证相关手段措施是否能够有效防范鼠虫蚁害。

7.3.5 管理安全检测要求

7.3.5.1 安全管理制度

7.3.5.1.1 管理制度

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 访谈安全主管，询问是否应对安全管理活动中的各类管理内容建立安全管理制度；检查安全管理制度，是否覆盖各类安全管理活动；
- b) 访谈安全主管，询问是否形成由安全策略、管理制度、操作规程等构成的全面的安全管理制度体系。检查安全管理制度相关文档是否由安全策略、管理制度、操作规程等构成。

7.3.5.1.2 制定和发布

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 访谈安全主管，询问安全管理制度是否按照统一的格式标准或要求制定；应检查安全管理制度文档，查看各项制度文档格式是否统一，是否有版本标识；
- b) 检查制度制定和发布要求管理文档，查看文档是否说明安全管理制度是否通过正式、有效的方式发布；
- c) 检查安全管理制度文档，查看是否注明发布范围；检查安全管理制度的收发登记记录，查看收发是否符合规定程序和发布范围要求。

7.3.5.1.3 评审和修订

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 访谈安全主管，询问安全小组是否定期对安全管理制度体系的合理性和适用性进行评审，评审周期多长；
- b) 访谈安全主管，询问是否定期或不定期地对安全管理制度进行评审，由何部门/何人负责；访谈负责定期评审的人员，询问定期对安全管理制度的评审、修订情况，评审周期多长，评审、修订程序如何；应检查安全管理制度评审记录，查看记录日期与评审周期是否一致。

7.3.5.2 安全管理机构

7.3.5.2.1 岗位设置

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 访谈安全主管，询问是否设立了安全管理工作的职能部门；
- b) 访谈安全主管，询问是否应成立指导和管理安全工作的委员会或领导小组，其最高领导是否由单位主管领导委任或授权；
- c) 检查安全管理制度文档，明确安全管理机构各个部门和岗位的职责、分工和技能要求。

7.3.5.2.2 人员配备

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 访谈安全主管，询问是否配备专职的安全管理员；检查安全管理人员名单，确认安全管理人员是否是专职人员；
- b) 访谈安全主管，询问关键事务岗位是否配备多人共同管理；检查安全管理人员名单和职责列表，确认关键事务岗位是否由多人共同管理。

7.3.5.2.3 3 授权和审批

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 访谈关键活动的批准人，询问是否根据各个部门和岗位的职责明确授权审批事项；

- b) 访谈安全主管，询问是否针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；应检查授权审批管理文件，查看文件是否明确审批程序；
- c) 访谈安全主管，询问是否定期审查审批事项，审查周期多长，是否及时更新需授权和审批的项目、审批部门和审批人等信息；检查授权审批管理文件，查看文件是否说明定期审查审批的事项、及时更新需审批的项目、审查周期等内容；检查审批记录，查看记录日期是否与审查周期一致；
- d) 访谈安全主管，询问是否记录审批过程并保存审批文档；检查是否有记录项目授权审批过程的文档。

7.3.5.2.4 沟通和合作

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 访谈安全主管，询问各类管理人员之间、组织内部机构之间以及网络安全职能部门内部是否定期或不定期召开协调会议，共同协作处理网络安全问题；检查会议记录文件，查看是否有会议内容、会议时间、参加人员和结果等的描述；
- b) 访谈安全主管，询问是否建立与相关外部单位的沟通、合作，与外联单位有哪些合作内容，沟通、合作方式有哪些；应检查外联单位说明文档，是否说明外联单位的联系人、联系方式、合作内容等；
- c) 访谈安全主管，询问是否聘请网络安全专家作为常年的安全顾问，指导网络安全建设，参与安全规划和安全评审等；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，查看由安全顾问指导网络安全建设、参与安全规划和安全评审的相关文档或记录，是否具有由安全顾问签字的相关建议。

7.3.5.2.5 审核和检查

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 访谈安全主管，询问是否由内部人员或上级单位定期进行全面安全检查；检查安全检查制度文档，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、安全管理制度等的执行情况等；
- b) 访谈安全管理人员，询问是否制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报；检查是否有安全检查报告，报告中是否有检查数据汇总表等的描述；
- c) 检查安全审核和安全检查制度文档，查看文档是否规定安全审核和安全检查的内容、程序和周期等；应检查安全审核和安全检查过程记录，查看报告日期与检查周期是否一致，查看记录的检查程序与文件要求是否一致。

7.3.5.3 人员安全管理

7.3.5.3.1 人员录用

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 访谈人事负责人，询问在人员录用时是否对被录用人资质进行审查；检查人员录用要求管理文档，查看是否要求对被录用人资质进行审查；检查是否有人员资质审查文档或记录；
- b) 访谈人事负责人，询问是否要求被录用人签订保密协议；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；

- c) 访谈人事负责人，询问是否从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议；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。

7.3.5.3.2 人员离岗

除按照第2级的要求进行检测之外，还应访谈人事工作人员，询问关键岗位人员离岗是否须承诺调离后的保密义务后方可离开；检查人员离岗管理文档，是否要求离岗人员承诺保密义务；应检查保密承诺文档，查看是否有调离人员的签字。

7.3.5.3.3 人员考核

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 访谈人事工作人员，询问是否对关键岗位的人员进行全面、严格的安全审查和技能考核；询问对人员的安全审查情况，审查人员是否包含所有岗位人员，审查内容有哪些（如操作行为、社会关系、社交活动等），是否全面；
- b) 检查考核记录，查看记录的考核人员是否包括各个岗位的人员，考核内容是否包含安全知识、安全技能等。

7.3.5.3.4 人员和技术支持能力

同第2级要求。

7.3.5.3.5 安全意识教育和培训

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 访谈各类技术人员和管理人员，考查其对工作相关的网络安全基础知识、安全责任和惩戒措施等的理解程度，被访谈人员对询问内容的表述是否清楚，是否与文件描述一致；检查安全管理制度，查看是否规定了安全责任和惩戒措施；
- b) 访谈安全管理人员，是否针对不同岗位制定不同的培训计划；检查安全教育培训计划，查看其是否明确了培训目的、培训方式、培训对象、培训内容、培训时间和地点等，培训内容是否包含网络安全基础知识、岗位操作规程等；
- c) 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；查看记录与培训计划是否一致。

7.3.5.3.6 外部人员访问管理

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 访谈安全主管，询问对外部人员（如向网络提供服务的软、硬件维护人员，业务合作伙伴、评估人员等）访问受控区域前是否需提出书面申请；检查外部人员访问受控区域批准文档，查看是否有外部人员访问受控区域的书面申请，是否有批准人允许访问的批准签字等；
- b) 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），外部人员进入条件（对哪些受控区域的访问须提出书面申请批准后方可进入），外部人员进入的访问控制（由专人全程陪同或监督等）和外部人员的离开条件等；检查外部人员访问受控区域的登记记录，查看记录是否描述了外部人员访问重要区域的进入时间、离开时间、访问区域、访问设备或信息及陪同人等信息。

7.3.5.4 安全建设管理

7.3.5.4.1 定级

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 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网络定级结果进行论证和审定；
- b) 检查网络定级文档，查看定级结果是否分级上报至全国或地区的主管部门，是否获得了上级主管部门的批准。

7.3.5.4.2 安全方案设计

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 访谈安全主管或网络建设负责人，询问是否指定和授权专门的部门对网络的安全建设进行总体规划，制定近期和远期的安全建设工作计划；检查网络的安全建设工作计划，查看文件是否明确了系统的近期安全建设计划和远期安全建设计划；
- b) 访谈网络建设负责人，询问是否根据网络的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件；
- c) 访谈网络建设负责人，询问是否组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才正式实施；检查网络总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等配套文件，查看各个文件是否有机构管理层的批准；
- d) 访谈网络建设负责人，询问是根据等级评测、安全评估的结果定期调整和修订总体安全策略、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；检查是否具有总体安全策略、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维护记录或修订版本，查看记录日期与维护周期是否一致。

7.3.5.4.3 产品采购

除按照第2级的要求进行检测之外，还应访谈网络建设负责人，询问网络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，是否定期审定和更新候选产品名单，审定周期多长；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或更新的候选产品名单。

7.3.5.4.4 自行软件开发

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 访谈网络建设负责人，询问开发人员和测试人员是否分离，测试数据和测试结果是否受到控制；
- b) 检查是否具备代码编写安全规范，开发人员是否参照规范编写代码；
- c) 访谈网络建设负责人，询问是否对程序资源库的修改、更新、发布进行授权和批准；查看是否具备程序资源库修改、更新和发布的记录及审批文档。

7.3.5.4.5 外包软件开发

同第2级要求。

7.3.5.4.6 工程实施

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 访谈网络建设负责人，询问工程实施单位是否能正确地执行安全工程过程；
- b) 检查工程实施管理制度，查看其是否规定工程实施过程的控制方法（如内部阶段性控制或外部监理单位控制）、实施参与人员的各种行为等方面内容。

7.3.5.4.7 测试验收

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 检查验收测试管理制度，查看是否包含网络测试验收的控制方法和人员行为准则；
- b) 访谈网络建设负责人，询问是否指定或授权专门的部门负责测试验收的管理，是否按照管理规定的要求完成测试验收工作。检查是否具有验收报告。

7.3.5.4.8 交付

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 检查网络交付管理制度，查看其是否规定了交付过程的控制方法和对交付参与人员行为准则等方面内容；
- b) 访谈网络建设负责人，询问是否指定或授权专门的部门负责网络交付的管理工作，并按照管理规定的要求完成交付工作；
- c) 访谈网络建设负责人，询问在正式投入使用前，是否根据实际情况进行了试运行，试运行期间是否制定相关应急预防措施；检查是否制定了相关文档，是否具有试运行报告、应急预防方案/措施；
- d) 访谈网络建设负责人，并通过实际操作检查在正式投入使用后，是否对建设、开发过程中涉及安全要求的配置、口令等内容重新修改、设定。

7.3.5.4.9 安全服务商的选择

同第2级要求。

7.3.5.4.10 等级评测

等级评测要求如下：

- a) 访谈安全主管，询问在网络运行过程中，是否至少每年对网络进行一次等级评测，发现不符合相应等级保护标准要求的是否及时整改；检查是否具备等级评测记录、整改记录；
- b) 访谈安全主管，询问是否在网络发生变更时及时对网络进行等级评测，发现级别发生变化的是否及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的是否及时整改；检查网络等级评测记录，是否能反映网络发生的变更、级别的变化；检查整改记录；
- c) 访谈安全主管，询问是否选择具有国家相关技术资质和安全资质的评测单位进行等级评测；检查评测单位的资质证明；
- d) 访谈安全主管，询问是否指定或授权专门的部门或人员负责等级评测的管理。

7.3.5.5 安全运维制度

7.3.5.5.1 运行维护能力

同第2级要求。

7.3.5.5.2 环境管理

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 访谈安全主管，是否有指定的部门负责机房安全，机房是否配置电子门禁系统，是否机房来访人员实行登记记录和电子记录双重备案管理；检查机房安全管理制度是否指定专门的部门负责机房安全；检查是否具备机房来访人员登记记录和电子记录；
- b) 检查办公环境管理文档，是否要求工作人员离开座位确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸档文件。

7.3.5.5.3 资产管理

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 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；检查是否根据资产的价值采取相应的管理措施；应检查资产清单中的资产，查看其是否具有相应标识，资产标识是否与资产分类标识文档中所要求的一致；
- b) 访谈安全主管，询问是否对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。检查资产安全管理制度，查看其内容是否按信息分类与标识的原则和方法对信息资产的使用、传输和存储作出规定；

7.3.5.5.4 介质管理

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 检查是否具备介质安全管理制度，查看是否对介质的存放环境、使用、维护和销毁等方面作出规定；
- b) 检查是否具备介质安全管理制度，查看是否对介质的物理传输过程中人员选择、打包、交付等情况进行控制；
- c) 访谈资产管理员，询问是否对存储介质的使用过程进行严格的管理，是否对带出工作环境的存储介质进行内容加密和监控管理，对保密性较高的存储介质未经批准是否可以自行销毁；
- d) 访谈资产管理员，询问是否根据数据备份的需要对某些介质实行异地存储，检查存储地的环境要求和管理方法是否与本地相同；
- e) 访谈资产管理员，询问是否对重要介质中的数据和软件采取加密存储。

7.3.5.5.5 设备管理

除按照第2级的要求进行检测之外，还应访谈系统管理员，询问是否建立配套设施、软硬件维护方面的管理制度，是否对其维护进行有效的管理；检查设备维护管理制度，查看是否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等内容。

7.3.5.5.6 网络安全管理

同第2级要求。

7.3.5.5.7 恶意代码防范管理

除按照第2级的要求进行检测之外，还应访谈安全员，询问是否定期检查网络内各种产品的恶意代码库的升级情况并进行记录，是否对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报；检查是否具备恶意代码库升级记录，病毒或恶意代码分析报告。

7.3.5.5.8 密码管理

除按照第2级的要求进行检测之外，还应检查是否具备密码使用管理制度。

7.3.5.5.9 变更管理

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

- a) 访谈网络运维负责人，询问是否具有建立变更管理制度，变更和变更方案是否有评审过程；检查是否具备变更管理制度；检查是否具备变更和变更方案的评审记录；

- b) 访谈网络运维负责人, 询问是否具有变更控制的申报和审批文件化程序, 是否对变更影响进行分析并文档化; 检查是否具备变更控制的申报和审批文件, 检查变更记录, 是否记录变更实施过程;
- c) 检查是否具备中止变更并从失败变更中恢复的程序文档, 是否明确过程控制方法和人员职责; 访谈网络运维负责人, 询问是否对恢复过程进行演练, 检查是否具备变更恢复演练记录。

7.3.5.5.10 备份与恢复管理

除按照第2级的要求进行检测之外, 还应按照本节内容进行检测:

- a) 访谈系统管理员, 询问是否具有备份与恢复管理相关的安全管理制度; 检查是否具有备份与恢复策略文档;
- b) 访谈系统管理员, 询问是否具有控制数据备份和恢复过程的程序, 是否对备份过程进行记录; 检查是否具有数据备份和恢复记录;
- c) 访谈系统管理员, 询问是否定期执行恢复程序, 检查和测试备份介质的有效性; 检查是否具有介质有效性测试记录。

7.3.5.5.11 安全事件处置

除按照第2级的要求进行检测之外, 还应按照本节内容进行检测:

- a) 检查是否具备安全事件的报告, 查看其是否包含安全事件的报告流程; 检查是否具备安全事件响应处理程序, 查看其是否包含响应和处置的范围、程度, 以及处理方法等;
- b) 检查安全事件记录分析文档, 查看是否分析和鉴定安全事件产生的原因;
- c) 访谈系统管理员, 询问是否对造成系统中断和造成信息泄密的安全事件采用不同的处理程序和报告程序; 检查相应的安全事件处理记录和报告。

7.3.5.5.12 应急预案管理

除按照第2级的要求进行检测之外, 还应按照本节内容进行检测:

- a) 访谈网络运维负责人, 询问是否从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障;
- b) 访谈网络运维负责人, 询问是否定期对应急预案进行演练; 检查是否具备应急预案演练记录, 查看演练周期是否符合规定;
- c) 访谈网络运维负责人, 询问是否对应急预案定期审查, 是否根据实际情况更新的内容, 是否能按实际内容执行; 检查是否具有应急预案审查记录, 查看是否有应急预案和灾难恢复计划中不适用内容的修订和更新记录, 检查记录是否说明修订和更新的原因以及相关审查结果。

7.4 第3.2级要求

同第3.1级要求。

7.5 第4级要求

同第3.2级要求。

7.6 第5级要求

待补充。