ICS 35.040
L 80

中华人民共和国国家标准

GB/T 35284—2017

信息安全技术
网站身份和系统安全要求与评估方法

Information security technology—
Requirements and assessment methods for website identity and system security

2017-12-29 发布　　2018-07-01 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

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:中国电子技术标准化研究院、北龙中网(北京)科技有限责任公司、上海凭安网络科技有限公司、北京奇虎科技有限公司、北京天威诚信电子商务服务有限公司、北京数字认证股份有限公司、陕西省网络与信息安全测评中心、中国信息安全认证中心。

本标准主要起草人:许东阳、刘贤刚、范科峰、叶润国、上官晓丽、毛伟、杨茂江、石晓虹、郝萱、傅大鹏、杨帆、王楠、张斌。

引　言

互联网应用的迅速普及，各种网站得到快速发展，但由此产生的网站信任问题也逐渐突出和严重。大量的假冒网站和钓鱼网站的出现已严重影响了我国网站的健康发展，很多的网民被假冒网站和钓鱼网站欺诈过，每年造成巨大的经济损失，这引发了互联网的诚信危机，也对社会和经济的发展造成了一定负面的影响。

本标准从网站身份和系统安全两个方面提出要求与评估方法，使得网站标识颁发机构可以评估网站的身份真实性与系统安全，互联网各终端软件厂商（浏览器、搜索引擎、微博、安全软件和即时通讯软件等）可查询网站标识颁发机构验证的标识信息，并以适当的方式展示给网民，以实现对网民上网行为的保护，帮助网民有效甄别真假网站，净化网络环境。

信息安全技术
网站身份和系统安全要求与评估方法

1 范围

本标准规定了网站身份和系统安全要求与评估方法，包括网站基本级要求、网站增强级要求、评估方法、评估结果展示和撤销等内容。

本标准适用于我国合法接入的互联网网站，也可为网站的开发、运维及评估等提供参考。

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。

GB/T 21052—2007 信息安全技术 信息系统物理安全技术要求

GB/T 25069—2010 信息安全技术 术语

3 术语和定义

GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

网站系统 website system

网站及支撑其运行的物理环境、网络环境、服务器操作系统和数据库系统等。

3.2

交易类网站 transactional website

以产品的网络销售为核心目的与盈利模式的网站，涉及支付、交易等行为，如网络商店、网络商城等。

3.3

网站标识 website identity

用于公众识别网站身份和系统安全的电子图形标识。

3.4

网站标识颁发机构 website identity issuer

负责网站标识整个生命周期(包括注册、签发、发布和废除)管理的、用户信任的颁发机构。

4 缩略语

下列缩略语适用于本文件。

HTTP：超文本传输协议(Hypertext Transfer Protocol)

ICP：网络内容服务商(Internet Content Provider)

IP：互联网协议/网间协议(Internet Protocol)

PV：页面访问量(Page View)
SQL：结构化查询语言(Structured Query Language)
SSH：安全外壳协议(Secure Shell)
VPN：虚拟专用网(Virtual Private Network)

5 概述

网站身份信息包括网站名称、网站 IP 地址、域名、网站实际经营者身份证明信息等。

普通用户通过互联网访问网站系统提供的服务，管理员用户通过专用的管理终端从本地网络或通过可信的 VPN 安全通道等方式访问内容管理及系统管理子系统。由于构成网站系统的物理层、网络层、主机层、数据层、网站层中的任何一层存在脆弱性，都可能导致网站出现内容篡改、服务中断、信息泄露及恶意控制等安全风险。为了实现上述安全目标，需要针对构成网站系统的各层面存在的脆弱性提出安全要求，并采取相应的技术措施，包括运行支撑、攻击防范、安全监控、应急响应等。

本标准中的网站身份和系统安全要求可划分为基本级、增强级两个等级。各网站经营者可依据网站的类别、访问量、注册用户数和业务重要性选择相应级别的要求与评估级别，见表 1。满足表 1 中任意一项指标的网站宜选择增强级要求进行评估。

本标准网站增强级要求描述中的粗体字表示较高等级要求中应加强的内容。

表 1 网站评估级别选择方法

级别选择因素	级别选择指标		适用的评估级别
类别	重要交易类网站或省部级政务门户网站	是	增强级
		否	基本级
访问量	有效日均访问次数≥20 万 PV	是	增强级
		否	基本级
注册用户数	累计注册用户总数≥50 万	是	增强级
		否	基本级
业务重要性	网站受到破坏后，会对公民、法人和其他组织的合法权益产生特别严重损害，或者对社会秩序和公共利益造成严重损害，或者对国家安全造成损害	是	增强级
		否	基本级
注：有效日均访问次数需避免重复统计同一访问源在短时间内进行的多次访问。			

6 网站基本级要求

6.1 身份要求

网站经营者：

a) 应向评估机构提供身份相关证明材料，包括但不限于：网站名称、ICP 备案信息、网站 IP 地址、域名所有权属、统一社会信用代码、工商登记信息、身份证明信息等；

b) 提供的证明材料应真实有效，不应存在身份假冒、钓鱼欺诈等问题；

c) 提供的身份证明信息如果为经办人信息，应提供网站负责人授权证明。

6.2 系统安全要求

6.2.1 物理安全

机房场地与网站系统应在设备安全、环境安全、系统物理安全等方面符合 GB/T 21052—2007 中第二级物理安全技术要求。

6.2.2 网络边界安全

本项要求包括：

a) 应在网站系统和互联网之间的网络边界部署边界隔离设备，如防火墙等，并应配置合理的边界访问控制策略，实现网站系统和互联网之间的逻辑隔离；

b) 应明确网站系统安全域与其他安全域之间的访问需求，合理配置相应的安全域边界过滤策略；

c) 应仅允许互联网用户和内部用户访问指定的服务和端口，如 Web 服务器提供的 HTTP 服务等，默认禁止访问不必要的服务和端口。

6.2.3 服务器安全

本项要求包括：

a) 服务器操作系统和数据库系统应遵循最小安装原则，仅安装业务系统必需的软件、服务和组件等；

b) 应对登录服务器操作系统及数据库系统的用户进行身份标识和鉴别；

c) 服务器应具有用户登录失败处理功能，配置并启用登录失败后结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；

d) 服务器应设置必要的用户访问控制策略，为用户授予其所需的最小权限；

e) 应及时更改或清除服务器操作系统及数据库系统中的默认口令、无用账号；

f) 如确有需要对服务器进行远程管理时，应采用 SSH 等安全方式实现；

g) 服务器应仅开启业务所需的最少服务和端口；

h) 应实现服务器操作系统及数据库系统的安全审计，对用户的登录和注销、系统开关机、重要服务访问和核心配置变更等操作进行日志记录；

i) 应对审计日志及审计策略设置必要的访问控制，禁止未授权的删除或修改。

6.2.4 管理终端安全

本项要求包括：

a) 应根据网站管理需求，设置端口、协议等访问控制策略，禁止非授权远程访问管理终端；

b) 应设置并启用管理终端的移动存储介质接入安全策略，并对接入的移动存储介质进行安全性检验；

c) 不应长期设置共享目录，共享文件应明确共享权限，不再使用时应及时取消相应目录的共享设置；

d) 应对管理终端的软件增加、修改、删除等变更情况进行日志审计，审计信息应包括时间、用户、操作及结果等；

e) 应定期对管理终端进行安全漏洞扫描，及时评估和修补已知的软件安全漏洞。

6.2.5 Web 应用安全

本项要求包括：

a) 网站对浏览用户可不进行鉴别，对注册用户应进行身份标识和鉴别；
b) 网站应具有注册用户登录失败处理功能，配置并启用登录失败后结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；
c) 应提供访问控制功能，为用户授予其所需的最小权限；
d) 应提供安全审计功能，对用户的注册、登录和注销、关键业务操作等行为进行日志记录；
e) 应对审计日志及审计策略设置必要的访问控制，禁止未授权的删除或修改；
f) 应根据网站实际访问需求限制用户最大并发会话连接数；
g) 如用户在一段时间内未作任何操作，网站 Web 应用应自动结束当前会话；
h) 应定期对 Web 应用程序、运行环境等进行漏洞扫描，及时修补已知的安全漏洞。

6.2.6 域名安全

本项要求包括：

a) 应选择国家主管部门批准的域名注册服务机构进行域名注册和托管，并进行域名信息报备；
b) 应遵循国家相关域名监督审批流程，有效开展域名变更、解析地址变更等工作，当域名信息需要变化时，应由指定专人负责实施并及时记录。

6.2.7 内容发布及数据安全

本项要求包括：

a) 网站内容管理模块应提供网站内容编辑与审核发布权限相分离的功能；
b) 网站应仅向注册用户提供信息发布功能，且应具有内容发布前的审核功能；
c) 应保护收集到的个人信息、关键配置参数、重要业务数据等，在远程传输及本地存储过程中应采用相应措施进行安全保护，如采用密码技术等确保个人信息与数据安全；
d) 应对网站系统的应用程序、系统数据、配置数据及审计日志等定期进行备份。

6.2.8 运行支撑

本项要求包括：

a) 网站系统运行环境应选择在物理安全、网络边界安全、服务器安全等方面符合本标准基本级要求；
b) 网站经营者应分析网站系统的性能需求，从应用程序的并发处理能力、服务器性能、网络带宽等方面保障网站系统性能。

6.2.9 攻击防范

本项要求包括：

a) 应在网络边界、服务器、管理终端等处采取恶意代码防范措施，拦截并清除企图进入网站系统的恶意代码；
b) 应严格控制外来介质的使用，防止恶意代码通过介质传播；
c) 应针对网站系统中的安全事件进行实时监控，监测和阻断端口扫描、拒绝服务攻击、木马攻击、缓冲区溢出攻击、网络蠕虫攻击、目录遍历攻击、SQL 注入、跨站脚本攻击等攻击行为。

6.2.10 安全监控与应急响应

本项要求包括：

a) 应利用网站安全监控系统或人工监控的方式，监测网站的运行状态，对网站停止服务、网站挂马、网页篡改等异常状况进行报警和处置；

b) 可根据网站系统的具体特点，制定应急响应预案，当发生信息安全事件时，应按照应急预案的要求及时实施应急响应措施并记录，以便将影响和损失减到最低。

7 网站增强级要求

7.1 身份要求

网站经营者：

a) 应向评估机构提供身份相关证明材料，包括但不限于：网站名称、ICP 备案信息、网站 IP 地址、域名所有权属、统一社会信用代码、工商登记信息、身份证明信息等；

b) 提供的证明材料应真实有效，不应存在身份假冒、钓鱼欺诈等问题；

c) 提供的身份证明信息如果为经办人信息，应提供网站负责人授权证明。

7.2 系统安全要求

7.2.1 物理安全

机房场地与网站系统应在设备安全、环境安全、系统物理安全等方面符合 GB/T 21052—2007 中**第三级**物理安全技术要求。

7.2.2 网络边界安全

本项要求包括：

a) 应在网站系统和互联网之间的网络边界部署边界隔离设备，如防火墙等，并应配置合理的边界访问控制策略，实现网站系统和互联网之间的逻辑隔离；

b) 应明确网站系统安全域与其他安全域之间的访问需求，合理配置相应的安全域边界过滤策略；

c) 应仅允许互联网用户和内部用户访问指定的服务和端口，如 Web 服务器提供的 HTTP 服务等，默认禁止访问不必要的服务和端口；

d) **应仅允许指定的 IP 地址访问网站系统提供的内容管理、系统管理等重要服务和端口**。

7.2.3 服务器安全

本项要求包括：

a) 服务器操作系统和数据库系统应遵循最小安装原则，仅安装业务系统必需的软件、服务和组件等；

b) 应对登录服务器操作系统及数据库系统的用户进行身份标识和鉴别；

c) 服务器应具有用户登录失败处理功能，配置并启用登录失败后结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；

d) 服务器应设置必要的用户访问控制策略，为用户授予其所需的最小权限；

e) 应及时更改或清除服务器操作系统及数据库系统中的默认口令、无用账号；

f) 如确有需要对服务器进行远程管理时，应采用 SSH 等安全方式实现，**并对远程管理员采用数字证书等高强度鉴别方式**；

g) 服务器应仅开启业务所需的最少服务和端口；

h) 应实现服务器操作系统及数据库系统的安全审计，对用户的登录和注销、系统开关机、重要服务访问和核心配置变更等操作进行日志记录；

i) 应对审计日志及审计策略设置必要的访问控制，禁止未授权的删除或修改。

7.2.4 管理终端安全

本项要求包括：

a) **应采取技术措施对接入的管理终端进行身份鉴别，身份鉴别通过后方可接入和使用网络资源；**

b) 应根据网站管理需求，设置端口、协议等访问控制策略，禁止非授权远程访问管理终端；

c) 应设置并启用管理终端的移动存储介质接入安全策略，并对接入的移动存储介质进行安全性检验；

d) 不应长期设置共享目录，共享文件应明确共享权限，不再使用时应及时取消相应目录的共享设置；

e) 应对管理终端的软件增加、修改、删除等变更情况进行日志审计，审计信息应包括时间、用户、操作及结果等；

f) 应定期对管理终端进行安全漏洞扫描，及时评估和修补已知的软件安全漏洞。

7.2.5 Web 应用安全

本项要求包括：

a) 网站对浏览用户可不进行鉴别，对注册用户根据安全需求**应采用数字证书等不同强度的身份鉴别机制；**

b) 网站应具有注册用户登录失败处理功能，配置并启用登录失败后结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；

c) 应提供访问控制功能，为用户授予其所需的最小权限；

d) 应提供安全审计功能，对用户的注册、登录和注销、关键业务操作等行为进行日志记录；

e) 应对审计日志及审计策略设置必要的访问控制，禁止未授权的删除或修改；

f) 应根据网站实际访问需求限制用户最大并发会话连接数；

g) 如用户在一段时间内未作任何操作，网站 Web 应用应自动结束当前会话；

h) 应定期对 Web 应用程序、运行环境等进行漏洞扫描，及时修补已知的安全漏洞。

7.2.6 域名安全

本项要求包括：

a) 应选择国家主管部门批准的域名注册服务机构进行域名注册和托管，并进行域名信息报备；

b) 应遵循国家相关域名监督审批流程，有效开展域名变更、解析地址变更等工作，当域名信息需要变化时，应由指定专人负责实施并及时记录；

c) **应对域名解析的正确性进行监控，以发现可能的恶意攻击。**

7.2.7 内容发布及数据安全

本项要求包括：

a) 网站内容管理模块应提供网站内容编辑与审核发布权限相分离的功能；

b) 网站应仅向注册用户提供信息发布功能，且应具有内容发布前的审核功能；

c) **应提供技术手段辅助进行网站用户论坛、留言板等信息发布内容的过滤；**

d) **应根据网站规模和信息内容选择相应的网页防篡改产品，对网站关键的静态页面和动态页面进行监控和保护；**

e) 应保护收集到的个人信息、关键配置参数、重要业务数据等，在远程传输及本地存储过程中应

采用相应措施进行安全保护，如采用密码技术等确保个人信息与数据安全；

f) 应对网站系统的应用程序、系统数据、配置数据及审计日志等定期进行备份，**必要时应采取异地备份措施，并实施备份恢复演练**。

7.2.8 运行支撑

本项要求包括：

a) 网站系统运行环境应选择在物理安全、网络边界安全、服务器安全等方面符合本标准**增强级**要求；

b) **网站系统的 Web 应用程序与数据库系统应分开部署在不同的独立物理服务器或虚拟服务器上**；

c) 网站经营者应分析网站系统的性能需求，从应用程序的并发处理能力、服务器性能、网络带宽等方面保障网站系统性能。

7.2.9 攻击防范

本项要求包括：

a) 应在网络边界、服务器、管理终端等处采取**恶意代码防范软件等**措施，拦截并清除企图进入网站系统的恶意代码；

b) **应对恶意代码防范软件的运行状态进行监测，防止修改配置或关闭进程的行为**；

c) 应严格控制外来介质的使用，防止恶意代码通过介质传播；

d) 应针对网站系统中的安全事件进行实时监控，监测和阻断端口扫描、拒绝服务攻击、木马攻击、缓冲区溢出攻击、网络蠕虫攻击、目录遍历攻击、SQL 注入、跨站脚本攻击等攻击行为；

e) **应加强人员安全意识教育和培训，防御社会工程攻击**。

7.2.10 安全监控与应急响应

本项要求包括：

a) 应利用**网站安全监控系统或第三方安全服务等方式**，监测网站的运行状态，对网站停止服务、网站挂马、网页篡改等异常状况**进行实时报警和处置**；

b) 可根据网站系统的具体特点，制定应急响应预案，当发生信息安全事件时，应按照应急预案的要求及时实施应急响应措施并记录，以便将影响和损失减到最低。

8 网站基本级评估方法

8.1 身份真实性评估

本项评估方法与结果判定如下：

a) 评估方法

1) 网站经营者作为申请单位可参照附录 A 所示网站身份和系统安全评估流程，提交包括但不限于：申请表原件、ICP 备案信息、域名所有权属、工商营业执照副本复印件或统一社会信用代码证复印件以及经办人身份证复印件等材料；

2) 评估机构对材料完整性进行核验，并采用技术手段与相应的数据库信息进行比对测试，核验其真实性与有效性，需要年检的证明材料应核验是否通过年检，评估项目如表 2 中所示。

表 2　身份真实性评估项目

序号	项目	评估内容
1	网站名称	评估机构验证网站注册名称的一致性
2	ICP 备案信息一致性	评估机构验证网站相关信息是否与 ICP 备案信息一致
3	网站 IP 地址	评估机构采用技术手段进行 IP 地址检测，验证网站 IP 地址的一致性，包括地址范围，是否动态分配，网站服务器是否在国内或者国外等
4	域名所有权属	评估机构验证网站域名注册信息，核验该网站是否具有域名所有权属
5	统一社会信用代码	评估机构验证网站实际经营单位统一社会信用代码的一致性
6	工商登记信息一致性	评估机构验证网站相关信息是否与工商登记信息一致
7	身份证明信息	评估机构验证身份证明信息一致性，身份证明信息可以为网站实际经营者身份证明信息或者经办人信息及授权证明

b）　结果判定

如果身份真实性的全部要求都能得到满足，则符合本项要求，否则不符合或部分符合本项要求。

8.2　系统安全评估

8.2.1　物理安全

本项评估方法与结果判定如下：

a）　评估方法

检查其机房场地与网站系统在设备安全、环境安全、系统物理安全等方面是否符合 GB/T 21052—2007 中第二级物理安全技术要求。

b）　结果判定

如果运行的网站系统与机房能够满足上述物理安全的要求，则符合本项要求，否则不符合或部分符合本项要求。

8.2.2　网络边界安全

本项评估方法与结果判定如下：

a）　评估方法

1）　检查网站系统与互联网之间的网络边界处是否部署防火墙等边界隔离设备，是否实现网站系统与互联网之间的逻辑隔离；

2）　检查网站系统安全域与其他安全域之间是否配置相应的安全域边界过滤策略；

3）　验证互联网用户和内部用户仅能访问网站服务器提供的 HTTP 服务等指定的服务和端口，尝试访问其他服务和端口。

b）　结果判定

如果能够满足以下全部预期结果，则符合本项要求，否则不符合或部分符合本项要求：

1）　网站系统与互联网已实现逻辑隔离；

2）　网站系统已配置相应的边界过滤策略；

3）　互联网用户和内部用户仅能访问指定的服务和端口。

8.2.3 服务器安全

本项评估方法与结果判定如下：

a) 评估方法

1) 检查网站服务器的操作系统和数据库系统是否遵循最小安装原则，是否仅安装业务必需的软件、服务和组件等；
2) 验证服务器操作系统及数据库系统是否对登录用户进行身份标识和鉴别；
3) 验证服务器操作系统及数据库系统是否具有用户登录失败处理功能，是否配置并启用登录失败后结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；
4) 检查服务器是否设置必要的用户访问控制策略，是否为用户授予其所需的最小权限；
5) 检查服务器操作系统及数据库系统中是否存在默认口令、无用账号；
6) 检查网站 Web 服务器、数据库服务器等重要服务器的远程管理方式，验证是否采用 SSH 等安全方式实现服务器的远程管理；
7) 验证服务器操作系统及数据库系统是否仅开启业务所需的最少服务及端口，尝试访问其他服务和端口；
8) 验证服务器操作系统及数据库系统是否具有安全审计功能，是否对用户的登录和注销、系统开关机、重要服务访问和核心配置变更等操作进行日志记录；
9) 验证安全审计日志及审计策略是否设置必要的访问控制，尝试未授权的删除或修改审计日志及审计策略等。

b) 结果判定

如果服务器安全的全部要求都能得到满足，则符合本项要求，否则不符合或部分符合本项要求。

8.2.4 管理终端安全

本项评估方法与结果判定如下：

a) 评估方法

1) 检查管理终端是否设置端口、协议等访问控制策略，尝试是否能非授权远程访问管理终端；
2) 验证管理终端是否设置并启用移动存储介质接入安全策略，尝试插入外来移动存储介质，验证是否启动安全检验程序；
3) 验证是否存在长期设置的共享目录，短期的共享文件是否明确共享权限；
4) 验证管理终端对软件的增加、修改、删除等变更情况是否具有日志审计功能，查看审计信息是否包括时间、用户、操作及结果等要素；
5) 验证管理终端是否定期进行软件安全漏洞扫描，是否及时评估和修补已知的软件安全漏洞。

b) 结果判定

如果能够满足以下全部预期结果，则符合本项要求，否则不符合或部分符合本项要求：

1) 能阻止非授权远程访问；
2) 能启用安全程序对移动存储介质进行检验；
3) 应正确设置文件共享功能；
4) 能对软件变更情况产生审计日志，并记录时间、用户、操作及结果等要素；
5) 应进行软件安全漏洞扫描与修复。

8.2.5 Web 应用安全

本项评估方法与结果判定如下：

a） 评估方法

1） 验证网站是否对注册用户进行身份标识和鉴别；

2） 验证网站是否具有注册用户登录失败处理功能，是否配置并启用登录失败后结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；

3） 验证网站是否提供访问控制功能，是否授予网站用户所需的最小权限；

4） 验证网站是否提供安全审计功能，是否对用户的注册、登录和注销、关键业务操作等行为进行日志记录；

5） 验证安全审计日志及审计策略是否设置必要的访问控制，尝试未授权的删除或修改审计日志及审计策略等；

6） 验证网站是否根据实际访问需求限制用户最大并发会话连接数；

7） 尝试用户在一段时间内未作任何操作，验证网站是否自动结束当前会话；

8） 验证网站是否定期针对 Web 应用程序、运行环境等进行漏洞扫描，是否及时修补已知的安全漏洞。

b） 结果判定

如果 Web 应用安全的全部要求都能得到满足，则符合本项要求，否则不符合或部分符合本项要求。

8.2.6 域名安全

本项评估方法与结果判定如下：

a） 评估方法

1） 检查网站是否在国家主管部门批准的域名注册服务机构进行域名注册和托管，是否进行域名信息报备；

2） 检查网站是否遵循国家相关监督审批流程开展域名变更、解析地址变更等工作，当发生域名信息变更时，是否由指定专人负责实施并及时记录。

b） 结果判定

如果域名安全的全部要求都能得到满足，则符合本项要求，否则不符合或部分符合本项要求。

8.2.7 内容发布及数据安全

本项评估方法与结果判定如下：

a） 评估方法

1） 检查网站内容管理模块是否提供网站内容编辑与审核发布权限相分离的功能；

2） 验证网站是否仅向注册用户提供信息发布功能，是否具有内容发布前的审核功能；

3） 验证网站是否保护收集到的个人信息、关键配置参数、重要业务数据等，是否在远程传输及本地存储过程中采用相应安全措施进行安全保护；

4） 验证网站是否对应用程序、系统数据、配置数据及审计日志等定期进行备份。

b） 结果判定

如果能够满足以下全部预期结果，则符合本项要求，否则不符合或部分符合本项要求：

1） 网站具有内容发布前的审核功能；

2） 网站对个人信息与重要数据的传输与存储采取安全措施进行保护；

3） 网站定期进行备份。

8.2.8 运行支撑

本项评估方法与结果判定如下：

a) 评估方法

1) 确认网站的运行模式，如采用主机托管或虚拟主机模式建设运行，检查其数据中心在物理安全、网络边界安全、服务器安全等方面是否符合本标准基本级要求；

2) 验证网站系统的应用程序的并发处理能力、服务器的处理能力、网络带宽等方面是否满足性能需求。

b) 结果判定

如果运行支撑的全部要求都能得到满足，则符合本项要求，否则不符合或部分符合本项要求。

8.2.9 攻击防范

本项评估方法与结果判定如下：

a) 评估方法

1) 检查网站是否在网络边界、服务器、管理终端等处采取恶意代码防范措施，是否对企图进入网站系统的恶意代码进行有效拦截和清除；

2) 验证网站是否及时对接入介质及其文件进行安全扫描；

3) 验证网站是否针对信息系统中的安全事件进行实时监控，模拟针对网站的端口扫描、拒绝服务攻击、木马攻击、缓冲区溢出攻击、网络蠕虫攻击、目录遍历攻击、SQL 注入、跨站脚本攻击等常见网络攻击行为，验证是否能监测和阻断。

b) 结果判定

如果攻击防范的全部要求都能得到满足，则符合本项要求，否则不符合或部分符合本项要求。

8.2.10 安全监控与应急响应

本项评估方法与结果判定如下：

a) 评估方法

1) 检查网站是否利用安全监控系统或人工监控的方式监测网站的运行状态；对网站触发停止服务、网站挂马、网页篡改等事件，查看是否有对异常状况进行报警和处置；

2) 检查网站是否根据系统的具体特点已制定应急响应预案，当信息安全事件发生时，是否能按照应急预案的要求及时实施应急响应措施并记录。

b) 结果判定

如果能够满足以下全部预期结果，则符合本项要求，否则不符合或部分符合本项要求：

1) 可以显示出网站的运行状态以及出现异常时显示告警信息；

2) 对于报警信息能够给出解释和建议解决方案；

3) 对于安全事件能够及时实施应急响应措施。

9 网站增强级评估方法

9.1 身份真实性评估

本项评估方法与结果判定如下：

a) 评估方法

1) 网站经营者作为申请单位可参照附录 A 所示网站身份和系统安全评估流程，提交包括但不限于：申请表原件、ICP 备案信息、域名所有权属、工商营业执照副本复印件或统一社会

信用代码证复印件以及经办人身份证复印件等材料；

2） 评估机构对材料完整性进行核验，并采用技术手段与相应的数据库信息进行比对测试，核验其真实性与有效性，需要年检的证明材料应核验是否通过年检，评估项目如表 2 中所示。

b） 结果判定

如果身份真实性的全部要求都能得到满足，则符合本项要求，否则不符合或部分符合本项要求。

9.2 系统安全评估

9.2.1 物理安全

本项评估方法与结果判定如下：

a） 评估方法

检查其机房场地与网站系统在设备安全、环境安全、系统物理安全等方面是否符合 GB/T 21052—2007 中**第三级**物理安全技术要求。

b） 结果判定

如果运行的网站系统与机房能够满足上述物理安全的要求，则符合本项要求，否则不符合或部分符合本项要求。

9.2.2 网络边界安全

本项评估方法与结果判定如下：

a） 评估方法

1） 检查网站系统与互联网之间的网络边界处是否部署防火墙等边界隔离设备，是否实现网站系统与互联网之间的逻辑隔离；

2） 检查网站系统安全域与其他安全域之间是否配置相应的安全域边界过滤策略；

3） 验证互联网用户和内部用户仅能访问网站服务器提供的 HTTP 服务等指定的服务和端口，尝试访问其他服务和端口；

4） **验证是否仅允许指定的 IP 地址访问网站系统提供的内容管理、系统管理等重要服务和端口，尝试其他 IP 地址是否能访问。**

b） 结果判定

如果能够满足以下全部预期结果，则符合本项要求，否则不符合或部分符合本项要求：

1） 网站系统与互联网已实现逻辑隔离；

2） 网站系统已配置相应的边界过滤策略；

3） 互联网用户和内部用户仅能访问指定的服务和端口；

4） **仅指定的 IP 地址能够访问网站系统提供的重要服务和端口。**

9.2.3 服务器安全

本项评估方法与结果判定如下：

a） 评估方法

1） 检查网站服务器的操作系统和数据库系统是否遵循最小安装原则，是否仅安装业务必需的软件、服务和组件等；

2） 验证服务器操作系统及数据库系统是否对登录用户进行身份标识和鉴别；

3） 验证服务器操作系统及数据库系统是否具有用户登录失败处理功能，是否配置并启用登

录失败后结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；

4） 检查服务器是否设置必要的用户访问控制策略，是否为用户授予其所需的最小权限；

5） 检查服务器操作系统及数据库系统中是否存在默认口令、无用账号；

6） 检查网站 Web 服务器、数据库服务器等重要服务器的远程管理方式，验证是否采用 SSH 等安全方式实现服务器的远程管理，**验证对远程管理的管理员是否采用数字证书等高强度鉴别方式**；

7） 验证服务器操作系统及数据库系统是否仅开启业务所需的最少服务及端口，尝试访问其他服务和端口；

8） 验证服务器操作系统及数据库系统是否具有安全审计功能，是否对用户的登录和注销、系统开关机、重要服务访问和核心配置变更等操作进行日志记录；

9） 验证安全审计日志及审计策略是否设置必要的访问控制，尝试未授权的删除或修改审计日志及审计策略等。

b） 结果判定

如果服务器安全的全部要求都能得到满足，则符合本项要求，否则不符合或部分符合本项要求。

9.2.4 管理终端安全

本项评估方法与结果判定如下：

a） 评估方法

1） **检查是否对接入的管理终端采取技术措施进行身份鉴别，是否身份鉴别通过后方可接入和使用网络资源**；

2） 检查管理终端是否设置端口、协议等访问控制策略，尝试是否能非授权远程访问管理终端；

3） 验证管理终端是否设置并启用移动存储介质接入安全策略，尝试插入外来移动存储介质，验证是否启动安全检验程序；

4） 验证是否存在长期设置的共享目录，短期的共享文件是否明确共享权限；

5） 验证管理终端对软件的增加、修改、删除等变更情况是否具有日志审计功能，查看审计信息是否包括时间、用户、操作及结果等要素；

6） 验证管理终端是否定期进行软件安全漏洞扫描，是否及时评估和修补已知的软件安全漏洞。

b） 结果判定

如果能够满足以下全部预期结果，则符合本项要求，否则不符合或部分符合本项要求：

1） **应在使用网络资源前进行身份鉴别**；

2） 能阻止非授权远程访问；

3） 能启用安全程序对移动存储介质进行检验；

4） 应正确设置文件共享功能；

5） 能对软件变更情况产生审计日志，并记录时间、用户、操作及结果等要素；

6） 应进行软件安全漏洞扫描与修复。

9.2.5 Web 应用安全

本项评估方法与结果判定如下：

a） 评估方法

1） 验证网站是否对注册用户**采用数字证书等不同强度的身份鉴别机制**；

2） 验证网站是否具有注册用户登录失败处理功能，是否配置并启用登录失败后结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；
3） 验证网站是否提供访问控制功能，是否授予网站用户所需的最小权限；
4） 验证网站是否提供安全审计功能，是否对用户的注册、登录和注销、关键业务操作等行为进行日志记录；
5） 验证安全审计日志及审计策略是否设置必要的访问控制，尝试未授权的删除或修改审计日志及审计策略等；
6） 验证网站是否根据实际访问需求限制用户最大并发会话连接数；
7） 尝试用户在一段时间内未作任何操作，验证网站是否自动结束当前会话；
8） 验证网站是否定期针对 Web 应用程序、运行环境等进行漏洞扫描，是否及时修补已知的安全漏洞。

b） 结果判定

如果 Web 应用安全的全部要求都能得到满足，则符合本项要求，否则不符合或部分符合本项要求。

9.2.6 域名安全

本项评估方法与结果判定如下：

a） 评估方法

1） 检查网站是否在国家主管部门批准的域名注册服务机构进行域名注册和托管，是否进行域名信息报备；
2） 检查网站是否遵循国家相关监督审批流程开展域名变更、解析地址变更等工作，当发生域名信息变更时，是否由指定专人负责实施并及时记录；
3） 检查网站是否**对域名解析的正确性进行监控，以发现可能的恶意攻击**。

b） 结果判定

如果域名安全的全部要求都能得到满足，则符合本项要求，否则不符合或部分符合本项要求。

9.2.7 内容发布及数据安全

本项评估方法与结果判定如下：

a） 评估方法

1） 检查网站内容管理模块是否提供网站内容编辑与审核发布权限相分离的功能；
2） 验证网站是否仅向注册用户提供信息发布功能，是否具有内容发布前的审核功能；
3） **验证网站是否提供技术手段辅助进行网站用户论坛、留言板等信息发布内容的过滤；**
4） **验证网站是否根据规模和信息内容已选择相应的网页防篡改产品，是否对网站关键的静态页面和动态页面进行监控和保护，尝试对网站关键的页面内容进行非授权修改；**
5） 验证网站是否保护收集到的个人信息、关键配置参数、重要业务数据等，是否在远程传输及本地存储过程中采用相应安全措施进行安全保护；
6） 验证网站是否对应用程序、系统数据、配置数据及审计日志等定期进行备份，**是否根据网站需求采取异地备份措施，并实施备份恢复演练**。

b） 结果判定

如果能够满足以下全部预期结果，则符合本项要求，否则不符合或部分符合本项要求：

1） 网站具有内容发布前的审核功能；
2） **网站具有信息发布内容的过滤功能；**
3） **非授权用户无法修改网站页面；**

4） 网站对个人信息与重要数据的传输与存储采取安全措施进行保护；

5） 网站定期进行备份，**根据需求实施备份恢复演练**。

9.2.8 运行支撑

本项评估方法与结果判定如下：

a） 评估方法

1） 确认网站的运行模式，如采用主机托管或虚拟主机模式建设运行，检查其数据中心在物理安全、网络边界安全、服务器安全等方面是否符合本标准**增强级**要求；

2） **确认网站系统的 Web 应用程序与数据库系统是否分开部署在不同的独立物理服务器或虚拟服务器上**；

3） 验证网站系统的应用程序的并发处理能力、服务器的处理能力、网络带宽等方面是否满足性能需求。

b） 结果判定

如果运行支撑的全部要求都能得到满足，则符合本项要求，否则不符合或部分符合本项要求。

9.2.9 攻击防范

本项评估方法与结果判定如下：

a） 评估方法

1） 检查网站是否在网络边界、服务器、管理终端等处采取**恶意代码防范软件等**措施，是否对企图进入网站系统的恶意代码进行有效拦截和清除；

2） **验证网站是否对恶意代码防范软件的运行状态进行监测，是否对修改配置或关闭进程的行为进行监测**；

3） 验证网站是否及时对接入介质及其文件进行安全扫描；

4） 验证网站是否针对信息系统中的安全事件进行实时监控，模拟针对网站的端口扫描、拒绝服务攻击、木马攻击、缓冲区溢出攻击、网络蠕虫攻击、目录遍历攻击、SQL 注入、跨站脚本攻击等常见网络攻击行为，验证是否能监测和阻断；

5） **验证网站经营者是否提供人员意识教育和培训，以防御社会工程攻击**。

b） 结果判定

如果攻击防范的全部要求都能得到满足，则符合本项要求，否则不符合或部分符合本项要求。

9.2.10 安全监控与应急响应

本项评估方法与结果判定如下：

a） 评估方法

1） 检查网站是否利用**网站安全监控系统或第三方安全服务等方式**，监测网站的运行状态；对网站触发停止服务、网站挂马、网页篡改等事件，查看是否有对异常状况**进行实时报警和处置**；

2） 检查网站是否根据系统的具体特点已制定应急响应预案，当信息安全事件发生时，是否能按照应急预案的要求及时实施应急响应措施并记录。

b） 结果判定

如果能够满足以下全部预期结果，则符合本项要求，否则不符合或部分符合本项要求：

1） 可以显示出网站的运行状态以及出现异常时实时显示告警信息；

2） 对于报警信息能够及时给出解释和建议解决方案；

3） 对于安全事件能够及时实施应急响应措施。

10 评估结果展示

评估结果展示流程如下：

a) 网站经营者作为申请单位满足相应级别的网站身份与系统安全要求，并通过评估机构核验后，可获得由网站标识颁发机构颁发的网站标识；

b) 申请单位网站可在支持网站评估结果的浏览器、搜索引擎、微博、安全软件以及即时通讯软件等平台上展示电子网站标识；

c) 公众可查询网站标识详细信息，包括网站等级、评估日期与有效期等。

11 评估结果撤销

评估结果撤销情形如下：

a) 网站经营者在网站信息变更后应及时提交变更材料到网站标识颁发机构更改信息，若信息未及时更改，将导致网站标识暂停解析，直至取消网站评估结果；

b) 网站若出现木马、病毒、黄赌毒等内容或该网站被国家相关部门查处、新闻机构曝光、公众投诉等严重情况，网站标识颁发机构将暂停网站标识解析，直至取消网站评估结果；

c) 网站经营者擅自出租、出借和转让网站标识，或者出现其他应予撤销的情形，网站标识颁发机构将停止网站标识解析，取消网站评估结果。

附 录 A
（资料性附录）
评估流程示例

A.1 评估准备

评估开始前，评估机构应做好以下准备工作：

——根据网站身份和系统安全要求，明确评估项；

——根据评估项，建立评估系统；

——对评估项、评估流程、评估方法、评估结果表示方法进行公示。

A.2 评估阶段

A.2.1 信息采集

根据评估项，可以通过计算机或者人工方式采集网站的信息。

A.2.2 评估

评估流程如下：

a) 网站经营者作为申请单位按照要求提交相应的申请材料；

b) 评估机构对申请材料完整性进行核验，并采用技术手段与相应的数据库信息进行比对测试，核验其真实性；

c) 如申请单位需要进行基本级评估，评估机构按照网站基本级要求与评估方法，核验是否通过评估；

d) 如申请单位需要进行增强级评估，评估机构按照网站增强级要求与评估方法，核验是否通过评估；

e) 对于符合要求的网站，评估机构向网站标识颁发机构申请，网站标识颁发机构发放网站标识并纳入到数据库中。

A.2.3 跟踪

对于已通过评估的网站，网站标识颁发机构应定期或不定期进行跟踪：

a) 应明示网站其评估通过日期与有效期，每年要核验其营业执照是否经过了年检，网站域名是否过期、申请者与网站域名的一致性是否持续，并且每个季度应核验一次该网站营业者单位是否被注销；

b) 每年应核验网站电子网站标识是否显示正确，并安装在所对应网站的规定位置；

c) 应根据网站重要性对其进行周期性评估（推荐以周为单位或以月为单位），并进行不定期跟踪、验证工作，确定其系统安全性是否达到相应评估要求；

d) 如果跟踪发现网站身份信息发生变化并且未申报变更、系统安全性未达到相应评估要求等，网站标识颁发机构有权撤销网站标识。

参 考 文 献

[1] GB/T 20269—2006 信息安全技术 信息系统安全管理要求
[2] GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求
[3] GB/T 20983—2007 信息安全技术 网上银行系统信息安全保障评估准则
[4] GB/T 31506—2015 信息安全技术 政府门户网站系统安全技术指南
[5] NIST SP800—53 联邦信息系统和组织的安全与隐私控制措施