

中标华信（北京）认证中心有限公司认监委备案的认证项目及认证规则

CSHCC-RZGZ-INS 网络空间安全管理体系认证规则及相关公示信息

中标华信（北京）认证中心有限公司认证规则公开方式或可获取的途径：本中心认证规则信息依法依申请公开，如需获取经备案的认证项目认证规则全文请发函至本中心邮箱 cshcc@cshcc.cn 或拨打电话 010-88255986 联系本机构技术信息部获取。

中标华信（北京）认证中心有限公司认证依据用标准或技术规范名称公开方式或可获取的途径：本中心按国家认监委要求备案及公示认证依据的封面和目录等关键信息，获取全文请购买和使用正版标准文件。

【认证规则、认证依据及认证证书公示信息及相关附件】

认证类别	认证领域	认证规则名称	认证规则编号	认证规则版本信息	状态标识	认证规则发布单位	认证规则发布/实施/修订日期	认证规则来源信息	认证依据用标准或技术规范名称	认证依据用标准或技术规范编号	认证依据用标准或技术规范发布单位	认证依据用标准或技术规范发布/实施日期	认证依据用标准或技术规范公开方式或可获取的途径	认证证书与认证标志发布/所有权单位	认证证书样式	标志样式
管理体系	其他管理体系	网络空间安全管理体系认证规则	CSHCC-RZGZ-INS	B0	新建	中标华信（北京）认证中心有限公司	20251215	自行制定	网络安全 互联网安全指南	ISO/IEC 27032:2023	国际标准化组织	20230627	见附页	网络空间安全管理体系认证证书	中标华信（北京）认证中心有限公司	见附页
									网络空间安全管理体系认证技术规范	CTS CSHCC010-2025	中标华信（北京）认证中心有限公司	20260101				



网络空间安全管理体系认证规则

文件编号：CSHCC-RZGZ-INS

文件版本：B0

编 制：李岩、金鹏

审 核：伍倩惠

批 准：刘伯利

2024-08-28 发布

2025-12-15 修订

2026-01-01 实施

中标华信（北京）认证中心有限公司 发布

CSHCC-RZGZ-INS

网络空间安全管理体系认证规则

目 录

1. 适用范围	3
2. 对认证人员的基本要求	3
3. 初次认证程序	3
4. 监督审核程序	9
5. 再认证程序	10
6. 认证证书状态管理	11
7. 认证证书及认证标志要求	13
8. 与其他管理体系的结合审核	14
9. 其他	14
附录 A. 审核时间要求	15
附录 B. 修订记录	18

INTERNATIONAL
STANDARD

ISO
27032

Second edition
2023-06-27

**Cybersecurity — Guidelines for
Internet security**

Cybersécurité — Lignes directrices relatives à la sécurité sur l'Internet



Reference number
ISO 27032:2023(E)

© ISO 2023

ISO 27032:2023(E)



COPYRIGHT PROTECTED DOCUMENT

© ISO 2023. Published in Switzerland.

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Cn de Blandonne 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

ii

© ISO 2023 – All rights reserved

ISO/IEC 27032:2023

Contents

	Page
Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	4
5 Relationship between Internet security, web security, network security and cybersecurity	5
6 Overview of Internet security	7
7 Interested parties	8
7.1 General	8
7.2 Users	9
7.3 Coordinator and standardization organisations	10
7.4 Government authorities	10
7.5 Law enforcement agencies	10
7.6 Internet service providers	10
8 Internet security risk assessment and treatment	11
8.1 General	11
8.2 Threats	11
8.3 Vulnerabilities	12
8.4 Attack vectors	12
9 Security guidelines for the Internet	13
9.1 General	13
9.2 Controls for Internet security	14
9.2.1 General	14
9.2.2 Policies for Internet security	14
9.2.3 Access control	14
9.2.4 Education, awareness and training	15
9.2.5 Security incident management	15
9.2.6 Asset management	17
9.2.7 Supplier management	17
9.2.8 Business continuity over the Internet	18
9.2.9 Privacy protection over the Internet	19
9.2.10 Vulnerability management	19
9.2.11 Network management	20
9.2.12 Protection against malware	21
9.2.13 Change management	21
9.2.14 Identification of applicable legislation and compliance requirements	22
9.2.15 Use of cryptography	22
9.2.16 Application security for Internet-facing applications	22
9.2.17 Endpoint device management	24
9.2.18 Monitoring	24
Annex A (informative) Cross-references between this document and ISO/IEC 27002	25
Bibliography	27

© ISO 2023 – All rights reserved

iii

中标华信（北京）认证中心有限公司认监委备案的认证项目及认证规则

CSHCC-RZGZ-INS 网络空间安全管理体系认证规则及相关公示信息

国际标准

ISO
27032

第二版 2023-
06-27

网络安全 - 互联网安全指南

网络安全 - 互联网安全指南



参考编号 ISO
27032:2023(E)

© ISO 2023

ISO 27032:2023(e)



受版权保护的文件

© ISO 2023, 瑞士出版

保留所有权利。除非另有说明，未经事先书面许可，不得以任何形式或通过任何电子或机械手段（包括影印、在互联网或内部网上发布）复制或利用本出版物的任何部分。可通过以下地址向国际标准化组织或申请者所属国的国际标准化组织成员机构申请许可。

国际标准化组织版权局
Case Postale 56 • CP 401
CH-1214 Vernier, Geneva, Switzerland
电话: +41 22 749 01 11 • +41 22 749
01 11
传真: +41 22 749 09 47
copyrights@iso.org
www.iso.org

ii

© ISO 2023 - 保留所有权利

ISO/IEC 27032:2023

目录

	页
前言	iv
简介	v
1 范围	1
2 规范性参考资料	1
3 术语和定义	1
4 简称	4
5 互联网安全、网络安全、网络安全和网络安全之间的关系	5
6 互联网安全概述	7
7 有关各方	8
7.1 一般	8
7.2 用户	9
7.3 协调员和标准化组织	10
7.4 政府当局	10
7.5 执法机构	10
7.6 互联网服务提供商	10
8 互联网安全风险评估和处理	11
8.1 总论	11
8.2 威胁	11
8.3 脆弱性	12
8.4 改善地带	12
9 互联网安全指南	13
9.1 总论	13
9.2 互联网安全控件	14
9.2.1 总论	14
9.2.2 互联网安全政策	14
9.2.3 门禁控制	14
9.2.4 教育、宣传和培训	15
9.2.5 安全事件管理	15
9.2.6 资产管理	17
9.2.7 供应商管理	17
9.2.8 互联网上的业务连续性	18
9.2.9 互联网上的隐私和保护	18
9.2.10 漏洞管理	19
9.2.11 网络管理	20
9.2.12 防范恶意软件	21
9.2.13 变革管理	21
9.2.14 确定适用立法和合规要求	22
9.2.15 将科学应用于...	22
9.2.16 面向互联网的应用程序安全	22
9.2.17 端点设备管理	24
9.2.18 监测	24
附件 A (资料性) 本文档与 ISO/IEC 27002 之间的对照索引	25
参考书目	27

© ISO 2023 - 保留所有权利

iii

ICS 35.040
A 00

认 证 技 术 规 范

CTS CSHCC010-2025

网络空间安全管理体系认证技术规范

Certification techniques specifications for Internet security
management systems

2025-12-15 发布

2026-01-01 实施

中标华信（北京）认证中心有限公司 发布

CTS CSHCC010-2025

目 录

1 范围	5
2 规范性引用文件	5
3 术语、定义和缩略语	5
4 组织环境	6
4.1 理解组织及其环境	6
4.2 理解相关方的需求和期望	6
4.3 确定管理体系范围	7
4.4 网络空间安全管理体系	7
5 领导作用	7
5.1 领导作用和承诺	7
5.2 方针	7
5.3 组织角色、责任和权限	8
6 策划	8
6.1 应对风险和机遇的措施	8
6.2 网络空间安全目标及其策划的实现	10
6.3 变更的策划	10
7 支持	10
7.1 资源	10
7.2 能力	10
7.3 意识	11
7.4 沟通	11
7.5 文件化信息	11
7.5.1 总则	11
7.5.2 创建和更新	11
7.5.3 文件化信息的控制	11
8 运行	12
8.1 运行策划和控制	12

2

CTS CSHCC010-2025

8.2 Internet 网络安全、web 网络安全、network 网络安全和 cyber 网络安全之间的关系	12
8.3 互联网安全概述	14
8.4 有关各方	15
8.4.1 总则	15
8.4.2 用户	16
8.4.3 协调者和标准化组织	17
8.4.4 政府部门	17
8.4.5 执法机构	17
8.4.6 互联网服务提供商	17
8.5 互联网安全风险评估和处理	18
8.5.1 总则	18
8.5.2 威胁	18
8.5.3 漏洞	19
8.5.4 攻击向量	19
8.6 互联网安全准则	20
8.6.1 总则	20
8.6.2 互联网安全控制	21
9 绩效评价	32
9.1 监视、测量、分析和评价	32
9.2 内部审核	33
9.3 管理评审	33
10 改进	34
10.1 持续改进	34
10.2 不符合和纠正措施	34

3

中标华信(北京)认证中心有限公司认监委备案的认证项目及认证规则

CSHCC-RZGZ-INS 网络空间安全管理体系认证规则及相关公示信息

