

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-CSISMS 云服务信息安全管理体系认证规则 相关公示信息

【前言】

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	认证证书名称	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	云服务信息安全管理体系认证规则	CSHCC-RZGZ-CSISMS	A3	修订	中标华信（北京）认证中心有限公司	20260501	自行制定	信息技术-安全技术-基于ISO/IEC 27002的云服务信息安全控制实施规程	ISO/IEC 27017:2015	国际标准化组织	20151215	见附页	云服务信息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	不适用
									网络安全技术 信息安全管理体系 要求	GB/T 22080-2025/ISO/IEC 27001:2022	国家市场监督管理总局；国家标准化管理委员会	20260101					

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-CSISMS 云服务信息安全管理体认证规则 相关公示信息



云服务信息安全管理体认证规则

文件编号：CSHCC-RZGZ-CSISMS
文件版本：A3
编制：金鹏、李一辉
复核：江雪
审核：伍倩惠
批准：刘伯钊

2021 01 27 首次发布 2026 04 20 修订 2026 05 01 实施
中标华信（北京）认证中心有限公司 发布

目录

1 适用范围	4
2 认证依据	4
3 对认证机构的基本要求	4
4 对认证人员的基本要求	5
5 认证程序	6
5.1 认证申请	6
5.2 申请评审	7
5.3 认证合同及相关责任	8
5.4 审核方案和审核策划	9
5.4.1 审核方案	9
5.4.2 审核时间	9
5.4.3 多场所抽样方案	10
5.4.4 组建审核组	10
5.4.5 审核计划	11
5.5 实施审核	11
5.6 初次认证审核	12
5.6.1 总则	12
5.6.2 第一阶段审核	12
5.6.3 第二阶段审核	13
5.7 监督审核	13
5.8 再认证审核	14
5.9 特殊审核	14
5.9.1 扩大认证范围	14
5.9.2 提前较短时间通知的审核	14
5.10 不符合项及其验证	15

5.11 审核报告	15
5.12 认证决定	16
6 认证证书和认证标志	17
6.1 总则	17
6.2 认证证书	18
6.3 认证标志	19
7 认证证书的暂停、撤销和注销	19
7.1 总则	19
7.2 认证证书的暂停	19
7.3 认证证书的撤销	20
7.4 认证证书的注销	20
8 申诉（投诉）处理	20
9 信息公开与报告	21
10 认证记录	21
11 其他	23
11.1 认证标准改版	23
11.2 内部审核	23
11.3 CSISMS 技术服务	23
11.4 认证数据安全	23
12 附则	23
附录 A 云服务信息安全管理体审核时间要求	25
附录 B 证书编号规则	26
修订记录	27

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-CSISMS 云服务信息安全管理体系认证规则 相关公示信息

INTERNATIONAL STANDARD ISO/IEC 27017

First edition
 2015-12-15

Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

Technologies de l'information — Techniques de sécurité — Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage



Reference number
 ISO/IEC 27017:2015(E)

© ISO/IEC 2015

CONTENTS

	Page
1 Scope	1
2 Normative references	1
2.1 Identical Recommendations International Standards	1
2.2 Additional References	1
3 Definitions and abbreviations	1
3.1 Terms defined elsewhere	1
3.2 Abbreviations	2
4 Cloud sector-specific concepts	2
4.1 Overview	2
4.2 Supplier relationships in cloud services	2
4.3 Relationships between cloud service customers and cloud service providers	3
4.4 Managing information security risks in cloud services	3
4.5 Structure of this standard	3
5 Information security policies	4
5.1 Management direction for information security	4
6 Organization of information security	5
6.1 Internal organization	5
6.2 Mobile devices and teleworking	6
7 Human resource security	6
7.1 Prior to employment	6
7.2 During employment	6
7.3 Termination and change of employment	7
8 Asset management	7
8.1 Responsibility for assets	7
8.2 Information classification	8
8.3 Media handling	8
9 Access control	8
9.1 Business requirements of access control	8
9.2 User access management	9
9.3 User responsibilities	10
9.4 System and application access control	10
10 Cryptography	11
10.1 Cryptographic controls	11
11 Physical and environmental security	12
11.1 Secure areas	12
11.2 Equipment	12
12 Operations security	13
12.1 Operational procedures and responsibilities	13
12.2 Protection from malware	14
12.3 Backup	14
12.4 Logging and monitoring	15
12.5 Control of operational software	16
12.6 Technical vulnerability management	16
12.7 Information systems audit considerations	17
13 Communications security	17
13.1 Network security management	17
13.2 Information transfer	17
14 System acquisition, development and maintenance	18
14.1 Security requirements of information systems	18
14.2 Security in development and support processes	18

Rec. ITU-T X.1631 (07/2015) iii

	Page
14.3 Test data	19
15 Supplier relationships	19
15.1 Information security in supplier relationships	19
15.2 Supplier service delivery management	20
16 Information security incident management	20
16.1 Management of information security incidents and improvements	20
17 Information security aspects of business continuity management	22
17.1 Information security continuity	22
17.2 Redundancies	22
18 Compliance	22
18.1 Compliance with legal and contractual requirements	22
18.2 Information security reviews	23
Annex A – Cloud service extended control set	25
Annex B – References on information security risk related to cloud computing	29
Bibliography	30

iv Rec. ITU-T X.1631 (07/2015)

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-CSISMS 云服务信息安全管理体系认证规则 相关公示信息

中标华信认证中心 内部使用翻译稿
 ISO/IEC27017:2015 信息技术 安全技术 基于 ISO/IEC 27002 的云服务信息安全控制实施规程

国际
 标准

ISO/IEC
 27017

第一版
 2015-12-15

信息技术—安全技术—基于 ISO/IEC 27002 的云服务
 信息安全控制实施规程

信息技术—安全技术—基于信息安全控制的实践 ISO/IEC 27002 云服务



参考编号
 ISO/IEC 27017:2015(E)

© ISO/IEC 2015

中标华信认证中心 (www.cshcc.cn) 内部使用翻译稿-20210317

中标华信认证中心 内部使用翻译稿
 ISO/IEC27017:2015 信息技术 安全技术 基于 ISO/IEC 27002 的云服务信息安全控制实施规程

目录

1 范围.....	1
2 规范性引用文件.....	1
2.1 同文建议 国际标准.....	1
2.2 附加参考资料.....	1
3 定义和缩写.....	1
3.1 其他地方定义的术语.....	1
3.2 缩写.....	2
4 云部门特有的概念.....	2
4.1 概述.....	2
4.2 云服务中的供应商关系.....	2
4.3 云服务客户与云服务提供商之间的关系.....	3
4.4 管理云服务中的信息安全风险.....	3
4.5 标准结构.....	3
5 信息安全策略.....	4
5.1 信息安全管理指导.....	4
6 信息安全组织.....	5
6.1 内部组织.....	5
6.2 移动设备和远程工作.....	7
7 人力资源安全.....	7
7.1 任用前.....	7
7.2 任用中.....	7
7.3 任用的终止和变更.....	8
8 资产管理.....	8
8.1 有关资产的责任.....	8

中标华信认证中心 (www.cshcc.cn) 内部使用翻译稿-20210317

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-CSISMS 云服务信息安全管理体认证规则 相关公示信息

中标华信认证中心 内部使用翻译稿
 ISO/IEC27017:2015 信息技术 安全技术 基于 ISO/IEC 27002 的云服务信息安全控制实施规程

8.2 信息分级.....	9
8.3 介质处理.....	9
9 访问控制.....	9
9.1 访问控制的业务要求.....	9
9.2 用户访问管理.....	10
9.3 用户责任.....	11
9.4 系统和应用程序访问控制.....	11
10 密码.....	12
10.1 密码控制.....	12
11 物理和环境安全.....	13
11.1 安全区域.....	14
11.2 设备.....	14
12 运行安全.....	15
12.1 运行规程和责任.....	15
12.2 恶意软件防范.....	16
12.3 备份.....	17
12.4 日志和监视.....	17
12.5 运行软件控制.....	19
12.6 技术方面的脆弱性管理.....	19
12.7 信息系统审计的考虑.....	19
13 通信安全.....	19
13.1 网络安全管理.....	19
13.2 信息传输.....	20
14 系统获取、开发和维护.....	20
14.1 信息系统的安全要求.....	20
14.2 开发和支持过程中的安全.....	21
14.3 测试数据.....	22

中标华信认证中心 内部使用翻译稿
 ISO/IEC27017:2015 信息技术 安全技术 基于 ISO/IEC 27002 的云服务信息安全控制实施规程

15 供应商关系.....	22
15.1 供应商关系中的信息安全.....	22
15.2 供应商服务交付管理.....	23
16 信息安全事件管理.....	24
16.1 信息安全事件的管理和改进.....	24
17 业务连续性管理的信息安全方面.....	25
17.1 信息安全的连续性.....	25
17.2 冗余.....	26
18 符合性.....	26
18.1 符合法律和合同要求.....	26
18.2 信息安全评审.....	27
附件 A-云服务扩展控制集.....	29
附件 B-云计算相关信息安全风险的参考资料.....	33
参考文献.....	35

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-CSISMS 云服务信息安全管理体认证规则 相关公示信息

ICS 35.030
CCS L 80



中华人民共和国国家标准

GB/T 22080—2025/ISO/IEC 27001:2022
代替 GB/T 22080—2016

网络安全技术 信息安全管理体 要求

Cybersecurity technology—Information security management systems—
Requirements

(ISO/IEC 27001:2022, Information security, cybersecurity and privacy
protection—Information security management systems—Requirements, IDT)

2025-06-30 发布

2026-01-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

GB/T 22080—2025/ISO/IEC 27001:2022

目次

前言	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 组织环境	1
4.1 理解组织及其环境	1
4.2 理解相关方的需求和期望	1
4.3 确定信息安全管理体系范围	2
4.4 信息安全管理体系	2
5 领导	2
5.1 领导和承诺	2
5.2 方针	2
5.3 组织的角色、责任和权限	2
6 规划	3
6.1 应对风险和机会的措施	3
6.2 信息安全目标及其实现规划	4
6.3 针对变更的规划	4
7 支持	4
7.1 资源	4
7.2 能力	4
7.3 意识	5
7.4 沟通	5
7.5 文件化信息	5
8 运行	6
8.1 运行规划和控制	6
8.2 信息安全风险评估	6
8.3 信息安全风险处置	6
9 绩效评价	6
9.1 监视、测量、分析和评价	6
9.2 内部审计	6
9.3 管理评审	7
10 改进	7

GB/T 22080—2025/ISO/IEC 27001:2022

10.1 持续改进	7
10.2 不符合与纠正措施	7
附录 A (规范性) 信息安全控制参考	9
参考文献	15

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-CSISMS 云服务信息安全管理体系认证规则 相关公示信息



中标华信(北京)认证中心
CSHCC.CN

云服务信息安全管理体系认证证书

证书编号: XXXXXXXXXXXXXXXX

兹证明

XXXXXXXXXXXXX 有限公司

统一社会信用代码: XXXXXXXXXXXXXXXX
注册地址: XXXXXXXXXXXXXXXX
办公地址: XXXXXXXXXXXXXXXX
生产地址: XXXXXXXXXXXXXXXX

云服务信息安全管理体系符合标准:
GB/T 22080-2025/ISO/IEC 27001:2022
《网络安全技术 信息安全管理体系 要求》
ISO/IEC 27017:2015 《信息技术-安全技术-
基于 ISO/IEC27002 的云服务信息安全控制实施规程》

通过认证的范围:
与 XXXXXXXXXXXXXXXX 相关的云服务信息安全活动
(适用性声明版本: XXXX)

本证书在国家规定的各行政许可、资质许可有效期内使用有效。
在按受监督审核并经审核合格后,与证书下方二维码一并使用有效。

发证日期: XXXX-XX-XX 初次发证: XXXX-XX-XX
有效期至: XXXX-XX-XX 换证日期: XXXX-XX-XX

签发: 刘例刘

中标华信(北京)认证中心
有限公司



中心地址: 北京市石景山区石景山路3号玉泉大厦5层 中心电话: 010-88255986 中心邮编: 100049
注: 证书详细信息可在国家认证认可监督管理委员会官方网站 (www.cnca.gov.cn)
及本机构网站 (www.cshcc.cn) 或扫描左侧二维码查询



中标华信(北京)认证中心
CSHCC.CN

Authentication Certificate of Cloud Services Information Security Management Systems

Registration No. XXXXXXXXXXXXXXXX

This is to certify that

XXXXXXXXXXXXX Ltd.

Unified Social Credit Code: XXXXXXXXXXXX
Registered Address: XXXXXXXXXXXXXXXX
Office Address: XXXXXXXXXXXXXXXX
Production Address: XXXXXXXXXXXXXXXX

Cloud Services Information Security Management Systems satisfy:
GB/T 22080-2025/ISO/IEC 27001:2022
Cybersecurity technology-Information security
management systems-Requirements
ISO/IEC 27017:2015
Information technology - Security techniques - Code of practice for
information security controls based on ISO/IEC 27002 for cloud services

The certificate is valid for the following scope:
Cloud services information security management activities related to XXXX
(Statement of Applicability: XXXX)

This certificate is valid for use within the validity period of various administrative and
qualification licenses stipulated by the state. It is valid when used together with the QR code below the certificate
after undergoing supervision audit and passing the review.

Date of Issue: XXXX-XX-XX Date of Initial Certification: XXXX-XX-XX
Date of Expiry: XXXX-XX-XX Date of Change: XXXX-XX-XX

Prohan lin
General Manager

China Standard Huaxin (Beijing)
Certification Center Co., Ltd.



Address of Certification Authority: 5 Floor, YuQuan Building, No.3 Shijingshan Road, Shijingshan District, Beijing Tel: 010-88255986 P.C.: 100049
Note: The detailed information is available on the Certification and Accreditation Administration of the People's Republic of China official website
(www.cnca.gov.cn) the authority's website(www.cshcc.cn) and the Quick Response Code on the left.