网络信息安全解决方案

NETWORK INFORMATION SECURITY SOLUTIONS

北京旗云天下科技有限公司

汇报人：刘博永

01

PART

公司与服务介绍

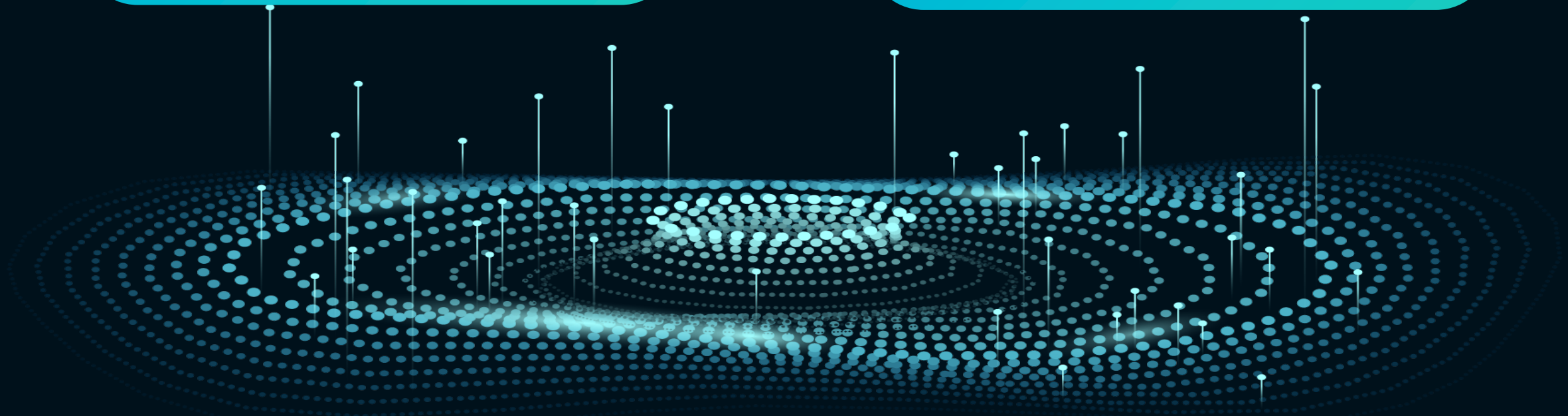
目　录

CONTENT

公司概况

成立于2014年，由数位资深的安全专家创办，在网络安全、漏洞挖掘、攻防研究、移动安全方面，有深厚的技术积累和独到的创新，可为客户提供完备的网络安全解决方案，赋能客户符合《中华人民共和国网络安全法》、《网络安全等级保护基本要求》、《信息安全风险评估规范》及《信息安全管理体系标准》的要求，提升客户整体网络安全防御能力。

认证中心团队负责网络安全等级保护与信息管理体系咨询;安全服务团队，致力于企业web安全、移动app、信息安全风险评估、代码审计的检测与研究；产品团队负责安全产品部署与实施，为企业客户提供专业的安全解决方案。
使命：通过技术服务让企业更安全更合规；
愿景：成为用户最值得信赖的企业；
价值观：客户为先 正直诚信 合作共赢 追求极致



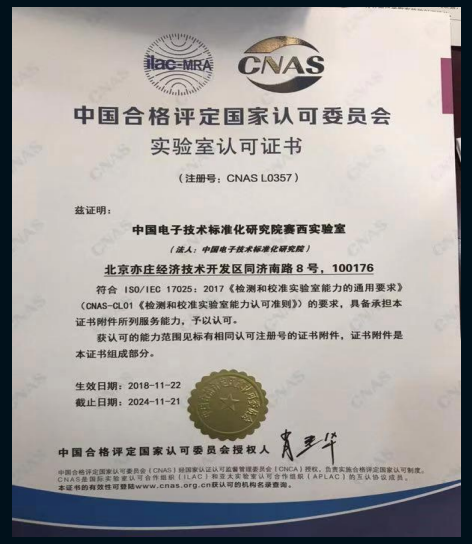
公司资质


高新技术企业
证书
企业名称：北京旗云天下科技有限公司
证书编号：GR201911006560
发证时间：2019年12月2日
有效期：三年
批准机关：


CCRC
信息安全服务资质认证证书
证书编号：CCRC-2021-ISV-RA-1288
兹证明
北京旗云天下科技有限公司
统一社会信用代码：91110228317919728D
的信息安全风险评估服务资质符合
CCRC-ISV-C01:2018《信息安全服务 规范》
三级服务资质要求。
注册地址： 北京市大兴区泰和路39号院3号楼3-1011
办公地址： 北京市大兴区泰和路39号院3号楼3-1011
颁证日期：2021年06月10日
有效期至：2022年06月09日
中国网络安全审查技术与认证中心
中国·北京·朝外大街甲10号（100020）
www.isccc.gov.cn 证书通过此网站查询


ISO9001
质量管理体系认证证书
证书编号：04621Q15337R0S
兹证明：
北京旗云天下科技有限公司
统一社会信用代码：91110228317919728D
质量管理体系符合：
GB/T19001-2016 / ISO9001:2015 标准
证书覆盖范围：
网络安全信息系统测评咨询
注册地址/实际地理地址：北京市大兴区泰和路 39 号院 3 号楼 3-1011
颁证日期：2021-08-04
有效期至：2024-08-03
IAF
CNAS
证书专用章
北京海德国际认证有限公司
中国·北京·朝阳区北苑东路19号院7号楼701室 (100012)


DJCP
网络安全等级保护测评机构
推荐证书
证书编号：DJCP2014110026
工业和信息化部电子工业标准化研究院
（中国电子技术标准化研究院赛西实验室）：
经审核，你单位符合网络安全等级保护测评机构有关规范要求，具备从事网络安全等级保护测评工作能力，现予以推荐。
证书有效期：2020年9月 至 2023年9月
国家网络安全等级保护工作协调小组办公室（代章）
二〇二〇年九月


ilac-MRA
CNAS
中国合格评定国家认可委员会
实验室认可证书
（注册号：CNAS L0357）
兹证明：
中国电子技术标准化研究院赛西实验室
（法人：中国电子技术标准化研究院）
北京亦庄经济技术开发区同济南路 8 号，100176
符合 ISO/IEC 17025：2017《检测和校准实验室能力的通用要求》（CNAS-CL01《检测和校准实验室能力认可准则》）的要求，具备承担本证书附件所列服务能力，予以认可。
获认可的能力范围见标有相同认可注册号的证书附件，证书附件是本证书组成部分。
生效日期：2018-11-22
截止日期：2024-11-21
中国合格评定国家认可委员会授权人


中华人民共和国国家版权局
计算机软件著作权登记证书
证书号：软著登字第4335050号
软件名称：信息安全等级保护测评系统 V1.0
著作权人：北京旗云天下科技有限公司
开发完成日期：2018年12月03日
首次发表日期：未发表
权利取得方式：原始取得
权利范围：全部权利
登记号：2019SR0912273
根据《计算机软件保护条例》和《计算机软件著作权登记办法》的规定，经中国版权保护中心审核，对以上事项予以登记。
No. 04469356
2019年09月02日


中华人民共和国国家版权局
计算机软件著作权登记证书
证书号：软著登字第4334911号
软件名称：悟安漏洞扫描软件 V1.0
著作权人：北京旗云天下科技有限公司
开发完成日期：2018年10月11日
首次发表日期：未发表
权利取得方式：原始取得
权利范围：全部权利
登记号：2019SR0914154
根据《计算机软件保护条例》和《计算机软件著作权登记办法》的规定，经中国版权保护中心审核，对以上事项予以登记。
No. 04452256
2019年09月03日


中华人民共和国国家版权局
计算机软件著作权登记证书
证书号：软著登字第4335026号
软件名称：信息安全网站与主机渗透测试管理软件 V1.0
著作权人：北京旗云天下科技有限公司
开发完成日期：2018年12月27日
首次发表日期：未发表
权利取得方式：原始取得
权利范围：全部权利
登记号：2019SR0912269
根据《计算机软件保护条例》和《计算机软件著作权登记办法》的规定，经中国版权保护中心审核，对以上事项予以登记。
No. 04469355
2019年09月02日

人员资质


信息安全保障人员认证证书
Information Security Assurance Worker Certification Certificate

兹证明 This is to certify that 刘博永 LIU BOYONG

认证考试成绩合格，并通过了认证评价，符合《信息安全保障人员认证准则》的要求，特颁此证。
has passed the examination, certification assessment, and successfully fulfilled the requirements of Certification Criteria for information Security Assurance Worker and is hereby awarded the professional-level in risk management field.

认证方向/Certification field：风险管理（专业级）RM/PL
证书编号/Certificate No.：2020CISAWRM2682
序列号/Serial No.：1026704
发证日期/Date of Issue：2020年11月17日
有效期/Term of Validity：2023年11月16日

魏吴


信息安全保障人员认证证书
Information Security Assurance Worker Certification Certificate

兹证明 This is to certify that 卢彩霞 LU CAIXIA

认证考试成绩合格，并通过了认证评价，符合《信息安全保障人员认证准则》的要求，特颁此证。
has passed the examination, certification assessment, and successfully fulfilled the requirements of Certification Criteria for information Security Assurance Worker and is hereby awarded the professional-level in risk management field.

认证方向/Certification field：风险管理（专业级）RM/PL
证书编号/Certificate No.：2021CISAWRM0257
序列号/Serial No.：1029380
发证日期/Date of Issue：2021年01月29日
有效期/Term of Validity：2024年01月28日

魏吴


HUAWEI

Huawei Certification

Song Tang

has successfully completed the Huawei certification requirements and is recognized as a

Routing & Switching

HCIP

Valid Through Sep 19, 2023

CEO
Huawei Technologies Co., Ltd.


中国信息安全测评中心
China Information Technology Security Evaluation Center
注册信息安全专业人员（CISP）
Certified Information Security Professional

注册信息安全工程师
CERTIFIED INFORMATION SECURITY ENGINEER

（证书编号：CNITSEC2014CISE00542）
Certificate No.

兹证明 This is to certify that

李桃 LI TAO

（证件号：432503198209277719）
ID No.

经中国信息安全测评中心的考试和审定，符合《注册信息安全专业人员资质评估准则》的要求，获准 注册信息安全工程师(CISE) 资质。
has successfully fulfilled the requirements prescribed by CNITSEC for certification and is hereby awarded this professional designation.

首次注册：2014年5月20日
Certified Since

发证日期：2018年6月15日
Issue Date

有效期：2018年6月15日至2021年6月14日
Valid thru

批准人 Signed by 朱晓清

中国信息安全测评中心 CNITSEC


中国信息安全测评中心
China Information Technology Security Evaluation Center
注册信息安全专业人员（CISP）
Certified Information Security Professional

注册信息安全管理人员
CERTIFIED INFORMATION SECURITY OFFICER

（证书编号：CNITSEC2020CISO00083）
Certificate No.

兹证明 This is to certify that

罗肖云 LUO XIAOYUN

（证件号：420921199610265111）
ID No.

经中国信息安全测评中心的考试和审定，符合《注册信息安全专业人员资质评估准则》的要求，获准 注册信息安全管理人员(CISO) 资质。
has successfully fulfilled the requirements prescribed by CNITSEC for certification and is hereby awarded this professional designation.

发证日期：2020年6月30日
Issue Date

有效期：2020年6月30日至2023年6月29日
Valid thru

批准人 Signed by 朱晓清

中国信息安全测评中心 CNITSEC 证书专用章


DJCP

信息安全等级测评师证书

姓　名：牟家刘
身份证号：513021198108060314
证书编号：10000361103140418
证书等级：高级

持有人参加信息安全等级测评师培训及考核，成绩合格，特颁发此证书。

证书查询网址：http://www.djbh.net
发证日期：2010年12月2日

批准人：闫古鹏


DJCP

网络安全等级测评师证书

姓　名：韩亮
身份证号：130624198510121451
证书编号：18043121114510111
证书等级：初级

持有人参加网络安全等级测评师培训及考核，成绩合格，特颁发此证书。

证书查询网址：http://www.djbh.net
发证日期：2018年11月22日

中关村信息安全测评联盟

批准人：金波


DJCP

网络安全等级测评师证书

姓　名：田一
身份证号：321283199407296017
证书编号：18018371160170314
证书等级：中级

持有人参加网络安全等级测评师培训及考核，成绩合格，特颁发此证书。

证书查询网址：http://www.djbh.net
发证日期：2018年11月23日

中关村信息安全测评联盟

批准人：金波


DJCP

信息安全等级测评师证书

姓　名：赵新强
身份证号：370687198910183870
证书编号：16026371138700118
证书等级：初级（技术）

持有人参加信息安全等级测评师培训及考核，成绩合格，特颁发此证书。

证书查询网址：http://www.djbh.net
发证日期：2016年5月12日

中关村信息安全测评联盟

批准人：闫古鹏

方案全景图

认证服务-网络安全等级保护
信息安全管理体系

安全服务-渗透测试
APP安全
代码审计
风险评估

安全咨询-等级保护咨询
安全体系咨询

安全产品-下一代防火墙
Web应用防火墙
堡垒机
数据库审计
日志审计
终端安全

安全巡检-漏洞扫描
基线检查

安全培训-安全意识培训
开发运维培训

02
PART

网络信息安全解决方案

等级保护法律依据

第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求， 履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被 窃取、篡改。

第二十五条 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行 业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、 公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。

第三十八条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能从在的风险每年至少进行一次检测评估。

第五十九条 网络运营者不履行网络安全保护义务的，由有关主管部门责令改正， 给予警告;拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款;对直接负责的主管人员处五千元以上五万元以下罚款。

等级保护及标准

系统分等级保护

- 对国家重要信息、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护

产品按等级管理

- 对信息系统中使用的信息安全产品实行按等级管理

事件分等级响应处置

- 对信息系统中发生的信息安全事件分等级响应、处置

- 《计算机信息系统安全保护等级划分准则》（GB17859-1999）
- 《信息安全技术 信息系统安全等级保护定级指南》(GB/T22240-2020)
- 《信息安全技术 网络安全等级保护基本要求》（GB/T22239—2019）
- 《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T25070—2019）
- 《信息安全技术 网络络安全等级保护测评要求》（GB/T28448-2019）
- 《信息安全技术 网络安全等级保护测评过程指南》（GB/T28449-2018）
- 《信息安全技术 网络安全等级保护安全管理中心技术要求》 GB/T 36958-2018）

等级保护发展历程

1994年《中华人民共和国计算机信息系统安全保护条例》颁布实施

1999年《计算机信息系统安全等级保护划分准则》（GB17859）发布。

2008年 等级保护1.0元年
《信息安全技术　信息系统安全等级保护基本要求》相关标准发布实施。

2017年施行《中华人民共和国网络安全法》

2019年 等级保护2.0元年
5月13日正式发布等级保护2.0版本《信息安全技术网络安全等级保护基本要求》

等级保护划分要求

信息系统受到破坏后，会对国家安全造成特别严重损害。

信息系统受到破坏后，会对社会秩序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。

信息系统受到破坏后，会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。

信息系统受到破坏后，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损害，但不损害国家安全。

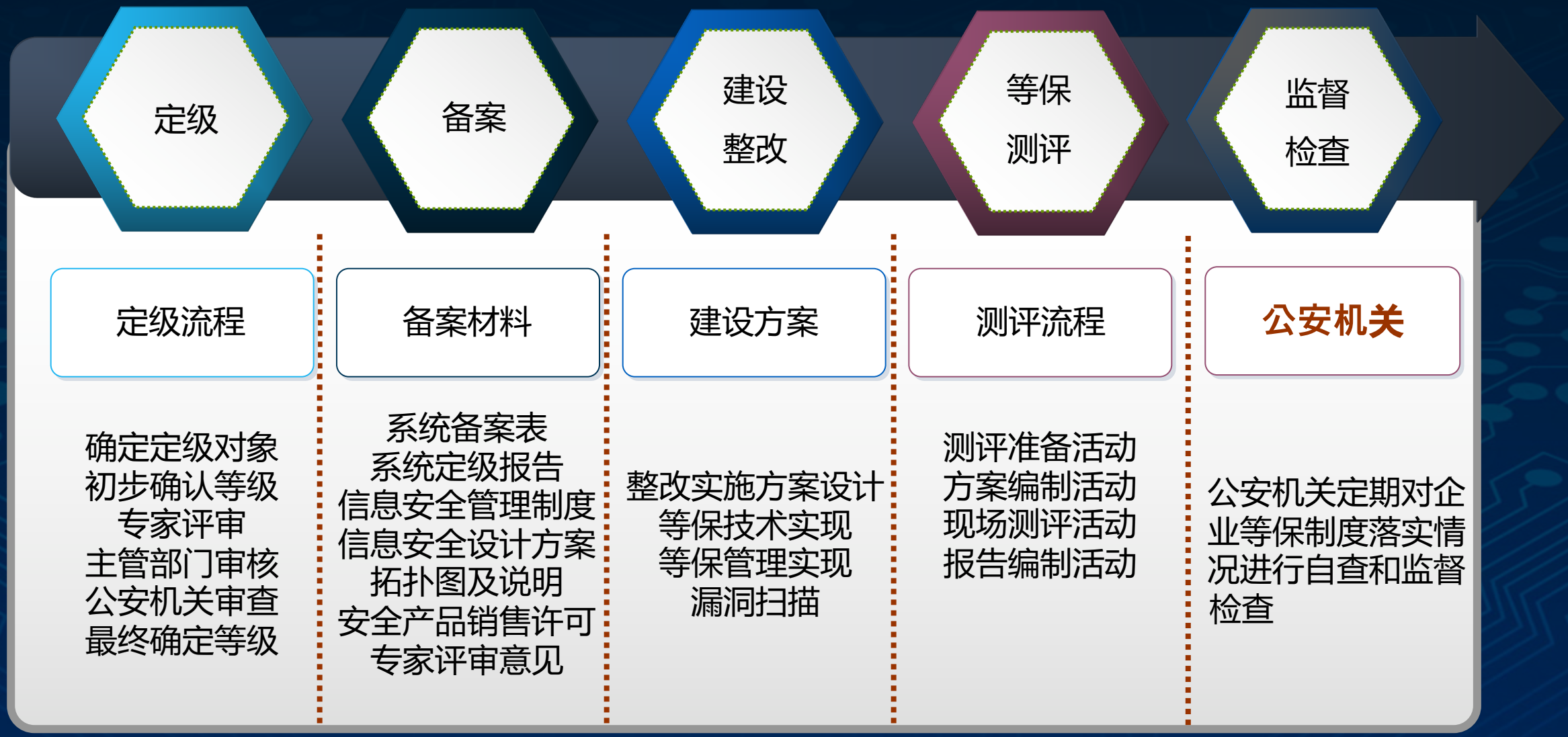
信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

等级保护对象范围

网络/平台类	信息系统类	数据类
电信网	计算机信息系统	大数据
广播电视网	工业控制系统	数字资产
互联网	移动互联系统	数据资源
行业专网	物联网系统	
云计算服务平台		
大数据服务平台		

等保进入2.0时代，保护对象从传统的网络和信息系统，向“**云移物工大**”上扩展，基础网络、重要信息系统、互联网、大数据中心、云计算平台、物联网系统、移动互联网、工业控制系统、公众服务平台等都纳入了等级保护的范围。

等级保护工作流程


定级
备案
建设
整改
等保
测评
监督
检查
定级流程
备案材料
建设方案
测评流程
公安机关
确定定级对象
初步确认等级
专家评审
主管部门审核
公安机关审查
最终确定等级
系统备案表
系统定级报告
信息安全管理制度
信息安全设计方案
拓扑图及说明
安全产品销售许可
专家评审意见
整改实施方案设计
等保技术实现
等保管理实现
漏洞扫描
测评准备活动
方案编制活动
现场测评活动
报告编制活动
公安机关定期对企业等保制度落实情况进行自查和监督检查

等级保护定级流程

确定定级对象

包括基础信息网络、工业控制系统、云计算平台、物联网、其他信息系统、大数据等

初步确认等级

包括确定受侵害的客体、侵害对客体的侵害程度以及综合判定侵害程度

专家评审

定级对象的运营、使用单位应组织信息安全专家和业务专家，对初步定级结果的合理性进行评审，出具专家评审意见

主管部门审核

定级对象的运营、使用单位应将初步定级结果上报行业主管部门或上级主管部门进行审核

公安机关备案审查

定级对象的运营、使用单位应按照相关管理规定，将初步定级结果提交公安机关进行备案审查，审查不通过，其运营使用单位应组织重新定级。审查通过后最终确定定级对象的安全保护等级。

最终确定的等级

等级保护备案要求

备案步骤

- 根据《信息安全等级保护管理办法》，已运营（运行）的第二级以上信息系统，应当在安全保护等级确定后30日内，由其运营、使用单位到所在地设区的市级以上公安机关办理备案手续。
- 新建第二级以上信息系统，应当在投入运行后30日内，由其运营、使用单位到所在地设区的市级以上公安机关办理备案手续。

备案要求

- **隶属于中央的在京单位，**其跨省或者全国统一联网运行并由主管部门统一定级的信息系统，由主管部门向公安部备案；其他信息系统向北京市公安局备案。
- **隶属于省级的备案单位**，其跨地（市）联网运行的信息系统，由省级公安机关受理备案。
- **隶属于中央的非在京单位的信息系统，**由当地省级公安机关（或其指定的地市级公安机关）受理备案。
- 地市级以上公安机关**受理本辖区**内备案单位的备案。

等级保护备案流程

准备《授权委托书》和《营业执照》进行线上单位注册，进入等待审核

收到VPN和等保备案预约平台的账户密码

需准备技术材料《备案表》《定级报告》《拓扑图及说明》《安全产品清单》等，商务材料《服务器托管协议》《单位租赁协议》《应急联系表》及签字文件等16个文件

线上填写单位信息、系统信息、上传盖章版《技术材料》《专家评审意见》等PDF文件，进入等待审核。

审核通过三个工作日后，可向网安部门要PDF版备案证明，进入测评阶段工作，并同步进行线下预约材料提交时间，带着《商务材料》和《技术材料》线下提交，拿到纸质版备案证明。

等级保护安全产品配置建议

序号	一个中心三重防护	控制点概述	推荐产品	三级基础版	合规对应要求	选择项
1	安全通信网络	划分不同的网络区域，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段，建设高可用、冗余的网络。	云防火墙	√	根据服务器角色和重要性，对网络进行安全域划分；确保网络带宽和处理能力能满足业务高峰期需要；	必选
		应采用校验技术、密码技术保证通信过程中数据的完整性和保密性	Ssl证书	√	确保通信传输过程数据的完整性和保密性。根据服务器角色和重要性，对网络进行安全域划分；确保网络带宽和处理能力能满足业务高峰期需要；	必选
2	安全区域边界	应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为	ddos攻击	√	满足等保要求中关于异常流量检测要求和业务高可用性要求，针对异常流量检测要求和业务高可用性要求、检测限制外部发起网络攻击的要求、网络各个部分的带宽满足业务高峰期需要。	可选
		应具有提供访问控制、边界防护、入侵防范等安全机制	web应用防火墙	√	满足行业自身的安全需求； 满足等保要求中的入侵防范等要求；满足等保要求中关于应用安全防护的要求。 实现对网站完整性安全防护，防范各种页面篡改攻击行为；检测限制外部发起网络攻击的要求、记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警.	必选
3	安全计算环境	应能发现已知漏洞，并在经过充分测试评估后，及时修补漏洞	渗透测试	✖	上线前进行安全性测试，并出具安全测试报告。	可选
		应启用安全审计功能，对用户行为和安全事件进行审计	数据库审计	√	满足等保要求中关于数据库安全审计的要求，满足信息安全等级保护数据库管理要求以及访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级，针对业务层面的审计.	必选
		能够检测到入侵行为，并能够对恶意代码进行防范，提供报警并有效阻断。	云安全中心（主机安全）	√	解决当前服务器面临的主要网络安全风险，帮助企业构建服务器安全防护体系，防止数据泄露。 满足等保要求中关于主机防病毒的要求。 满足等保要求中关于对补丁统一升级要求。	必选
4	安全管理中心	应对用户（系统管理、审计管理、安全管理）进行身份鉴别、访问控制、运维审计	堡垒机	√	满足等保要求中身份鉴别、访问控制和安全审计等要求；满足信息安全等级保护数据库管理要求以及访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级.	必选

等级保护管理要求

安全管理制度

- 制定安全策略
- 建立安全管理制度
- 专人负责制定和发布管理
- 定期评审和修订管理制度

安全管理机构

- 设立相应领导、管理、审计、运维机构和岗位
- 配备系统管理、审计管理和安全管理员
- 明确授权和审批事项和制度
- 加强内部和外部安全专家沟通协作
- 定期审核和检查安全策略和安全管理制度

安全管理人员

- 考核录用人员专业技能，签署保密协议。
- 离岗人员及时回收权限、证照等
- 加强安全意识和安全技能教育培训
- 定期进行安全技术考核

安全建设管理

- 等保定级和备案
- 安全方案设计
- 安全产品采购和使用
- 自主和外包软件开发管理
- 安全保护工程实施管理
- 安全防护测试验收
- 系统验收交付
- 定期等保测评
- 监督、评审和审核安全服务提供商

安全运维管理

- 环境管理
- 资产管理
- 介质管理
- 设备维护管理
- 漏洞和风险管理
- 网络和系统安全管理
- 恶意代码防范管理
- 配置管理、密码管理、变更管理
- 备份与恢复管理
- 安全事件和应急预案管理
- 外包运维管理

等级保护测评要求

技术要求

安全管理中心

- 系统管理
- 审计管理
- 安全管理
- 集中管控

安全计算环境

- 身份鉴别
- 访问控制
- 安全审计
- 入侵防范
- 恶意代码防范
- 可信验证
- 数据完整性
- 数据保密性
- 数据备份恢复
- 剩余信息保护
- 个人信息保护

安全区域边界

- 边界防护
- 访问控制
- 入侵防范
- 可信验证
- 恶意代码和垃圾邮件防范
- 安全审计

安全通信网络

- 网络架构
- 通信传输
- 可信验证

安全物理环境

- 物理位置选择
- 物理访问控制
- 防盗窃和防破坏
- 防雷击
- 防火
- 防水和防潮
- 防静电
- 温湿度控制
- 电力供应
- 电磁防护

管理要求

安全管理制度

- 安全策略
- 管理制度
- 制定和发布
- 评审和修订

安全管理机构

- 岗位设置
- 人员配备
- 授权和审批
- 沟通和合作
- 审查和检查

安全管理人员

- 人员录用
- 人员离岗
- 安全意识教育和培训
- 外部人员访问管理

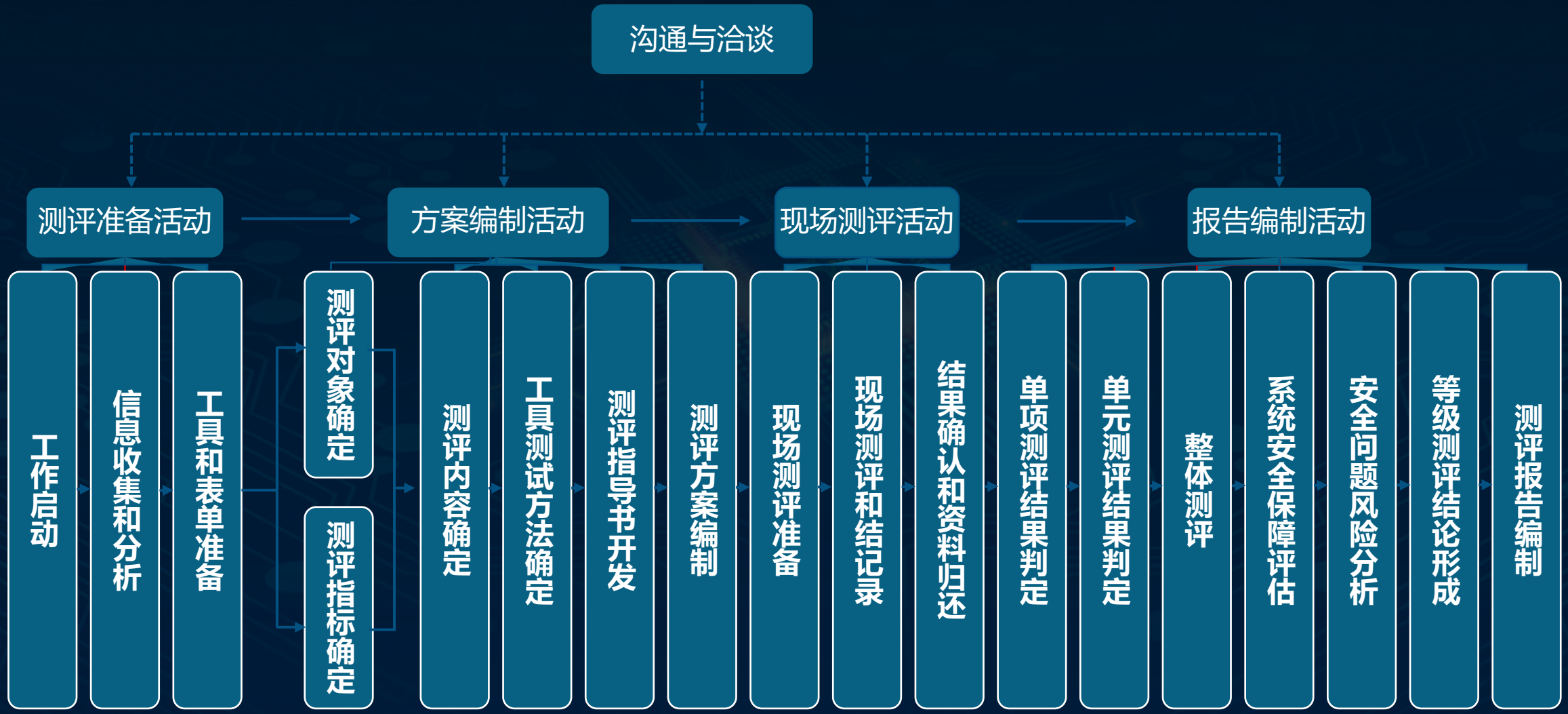
安全建设管理

- 定级和备案
- 安全方案设计
- 产品采购和使用
- 自行软件开发
- 外包软件开发
- 工程实施
- 测试验收
- 系统交付
- 等级测评
- 服务供应商选择

安全运维管理

- 环境管理
- 资产管理
- 介质管理
- 设备维护管理
- 漏洞和风险管理
- 网络和系统安全管理
- 恶意代码防范管理
- 配置管理
- 密码管理
- 备份与恢复管理
- 变更管理
- 安全事件处置
- 应急预案管理
- 外包运维管理

等级保护测评实施流程


沟通与洽谈
测评准备活动
方案编制活动
现场测评活动
报告编制活动
工作启动
信息收集和分析
工具和表单准备
测评对象确定
测评指标确定
测评内容确定
工具测试方法确定
测评指导书开发
测评方案编制
现场测评准备
现场测评和结记录
结果确认和资料归还
单项测评结果判定
单元测评结果判定
整体测评
系统安全保障评估
安全问题风险分析
等级测评结论形成
测评报告编制

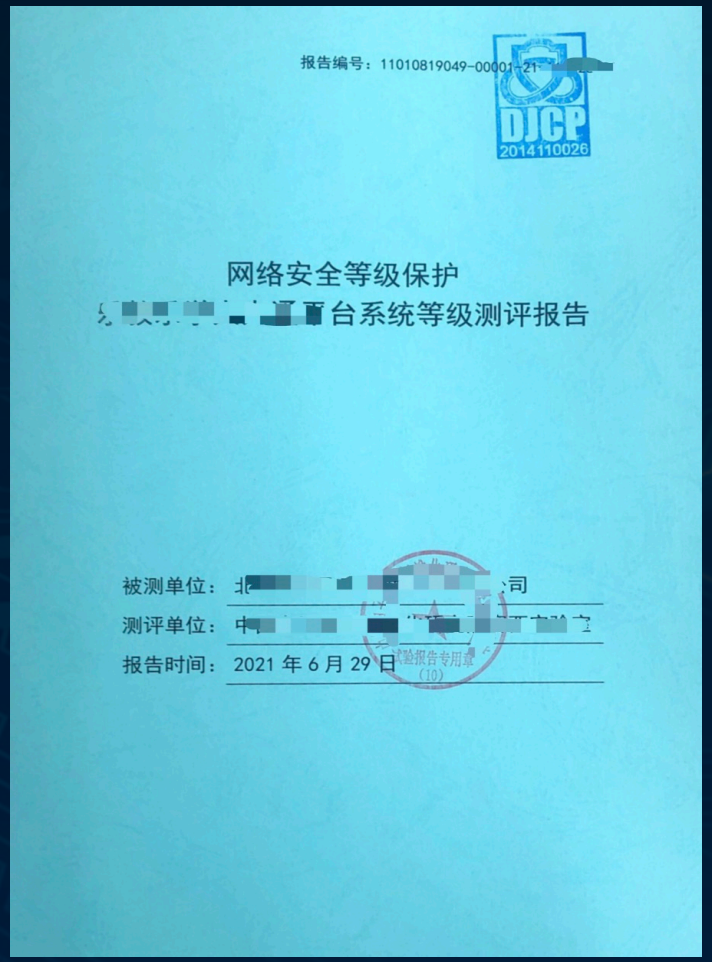
等级保护测评方法

访谈	核查	漏扫	渗透
访谈负责人 机房管理员 网络管理员 主机管理员 应用管理员	文档审查 实地查看 配置核查	获得授权后扫描 服务器扫描 数据库扫描 网络设备扫描 对应用系统扫描	获得授权后渗透 内部渗透 外部渗透

等级保护工作计划

序号	项目阶段	时间	乙方（旗云）	甲方（配合人员）
1	第一阶段 系统定级	10个工作日	等保专家1名、项目经理1名	运维技术1名
2	第二阶段 系统备案	10个工作日	等保专家1名、项目经理1名	运维技术1名、商务1名
3	第三部分 测评前期准备	5个工作日	等保专家1名、项目经理1名	运维技术1名、行政1名
4	第四部分 现场等级测评	5个工作日	等保专家1名、测评师3名	运维技术1名、研发人员1名、行政1名
5	第五部分 安全整改	10个工作日	等保专家1名	运维技术1名、研发人员1名
6	第六阶段 复测且整理报告	15个工作日	测评师3名	运维技术1名

等级保护测评结论


报告编号：11010819049-00001-21

网络安全等级保护

[redacted]台系统等级测评报告

被测单位：[redacted]

测评单位：[redacted]

报告时间：2021 年 6 月 29 日

评 价 标 准（等保2.0）

※ **优**

被测对象中存在安全问题，但不会导致被测对象面临中、高等级安全风险，且系统综合得分90分以上（含90分）。

※ **良**

被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险，且系统综合得分80分以上（含80分）。

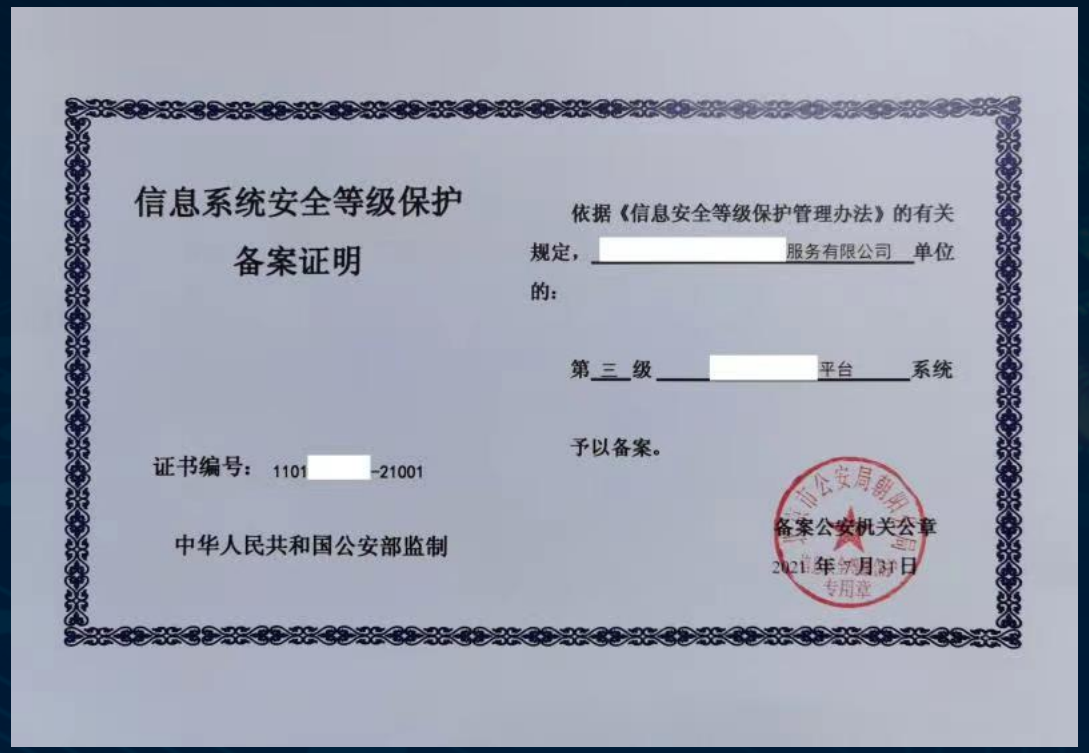
※ **中**

被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险，且系统综合得分70分以上（含70分）。

※ **差**

被测对象中存在安全问题，而且会导致被测对象面临高等级安全风险，或被测对象综合得分**低于70分**。

等级保护交付物



信息系统安全等级保护
备案证明

依据《信息安全等级保护管理办法》的有关规定，[redacted]服务有限公司单位的：

第三级[redacted]平台系统

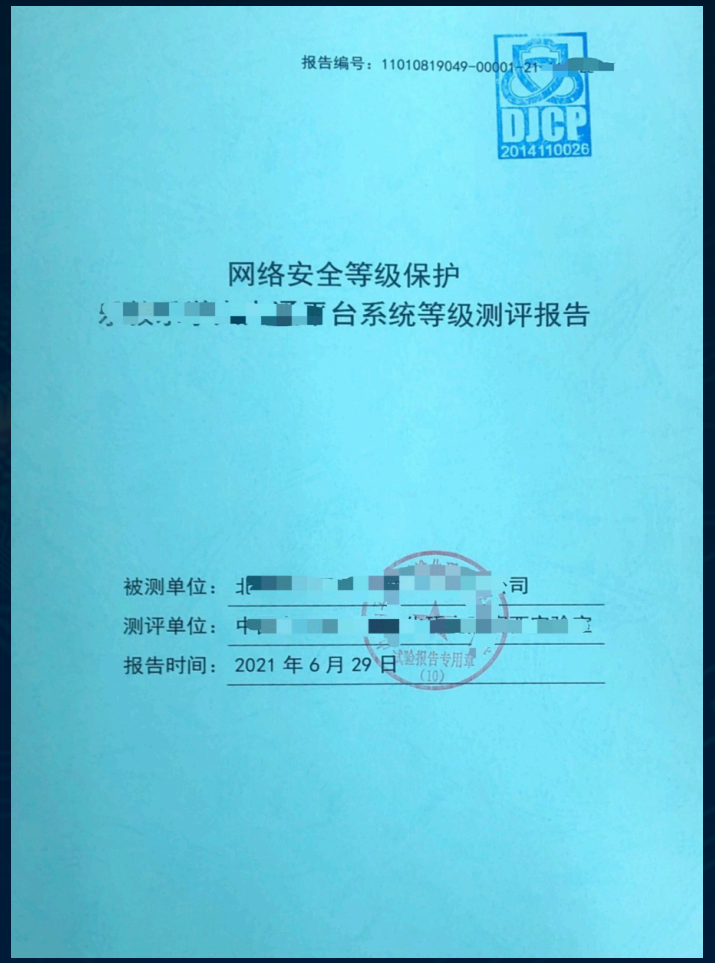
予以备案。

证书编号：1101[redacted]-21001

中华人民共和国公安部监制

备案公安机关公章

2021年7月21日



报告编号：11010819049-00001-21[redacted]

DJCP
2014110026

网络安全等级保护
[redacted]台系统等级测评报告

被测单位：北[redacted]司

测评单位：中[redacted]

报告时间：2021 年 6 月 29 日

信息安全管理体系

信息安全管理体系（ISMS）是组织整体管理体系的一个部分，是基于风险评估建立、实施、运行、监视、评审、保持和持续改进信息安全等一系列的管理活动，是组织在整体或特定范围内建立信息安全方针和目标，以及完成这些目标所用的方法的体系。

阶段	1 项目启动和差异分析	2 风险评估	3 体系设计与发布	4 体系运行与监控	5 认证及持续改进
主要任务	▸ 项目启动会议，确定项目团队、建立项目组管理架构 ▸ 信息安全管理现状的快速评估 ▸ 信息安全管理体系差异分析 ▸ 设计信息安全方针 ▸ 设计信息安全管理组织架构 ▸ 信息安全管理培训 ▸ 阶段项目总结会议	▸ 制定资产识别标准（包含保密级别划分） ▸ 资产收集及风险评估方法培训 ▸ 信息资产收集 ▸ 识别威胁、脆弱性、并安全漏洞扫描 ▸ 评估风险，划分风险等级 ▸ 阶段项目总结会议	▸ 确定风险容忍度和风险偏好 ▸ 确定风险处置措施并实施整改计划 ▸ 制度整合及信息安全管理体系文档编写 ▸ 信息安全体系技术控制及管理落地建议 ▸ 信息安全管理体系发布及培训 ▸ 阶段项目总结会议	▸ 制定信息安全管理绩效监控流程 ▸ 信息安全管理体系试运行 ▸ 体系运行监控 ▸ 业务连续性管理培训 ▸ 阶段项目总结会议	▸ ISMS内审培训 ▸ ISMS内审 ▸ ISMS外审 ▸ ISMS管理评审 ▸ 纠正、预防措施持续改进建议 ▸ 项目总结会议 ▸ 协助后续的内审和临审
主要交付品	▸ 项目计划 ▸ 差异分析报告 ▸ 信息安全管理组织架构 ▸ 信息安全方针	▸ 资产收集及风险评估方法与标准 ▸ 资产级别划分标准 ▸ 技术弱点扫描报告 ▸ 资产清单、威胁列表、脆弱性列表、风险列表 ▸ 风险评估报告	▸ 风险容忍标准及风险处置计划 ▸ 适用性声明 ▸ ISMS制度和流程 ▸ ISMS体系、事故响应培训 ▸ 信息安全体系技术落地建议书	▸ ISMS绩效监控流程 ▸ 信息安全推广培训	▸ ISMS内审报告 ▸ ISMS外审报告及改进 ▸ ISMS管理评审报告 ▸ 项目总结报告
	Plan	Do	Check	Act	

渗透测试

渗透测试服务（黑盒测试）是指在客户授权许可的情况下，安全专家将通过模拟黑客攻击的方式，在没有网站代码和服务器权限的情况下，对企业的在线平台进行全方位渗透入侵测试，来评估企业业务平台和服务器系统的安全性。

APP安全检测

随着移动互联网的高速发展，手机APP已成为了人们生活中密切相关的一部分，同时移动APP安全问题也愈发突出，移动应用恶意破解、重打包、核心代码泄露、恶意代码注入、APP劫持、数据泄漏等网络安全风险和安全事件层出不穷。

源代码审计

源代码安全审计是依据CVE漏洞、OWASP 10漏洞、CWE以及设备、软件厂商公布的漏洞库，结合专业源代码扫描工具对各种程序语言编写的源代码进行安全审计。为客户提供包括安全编码规范咨询、源代码安全现状测评、定位源代码中存在的安全漏洞、分析漏洞风险、给出修复建议等一系列服务。

审计内容

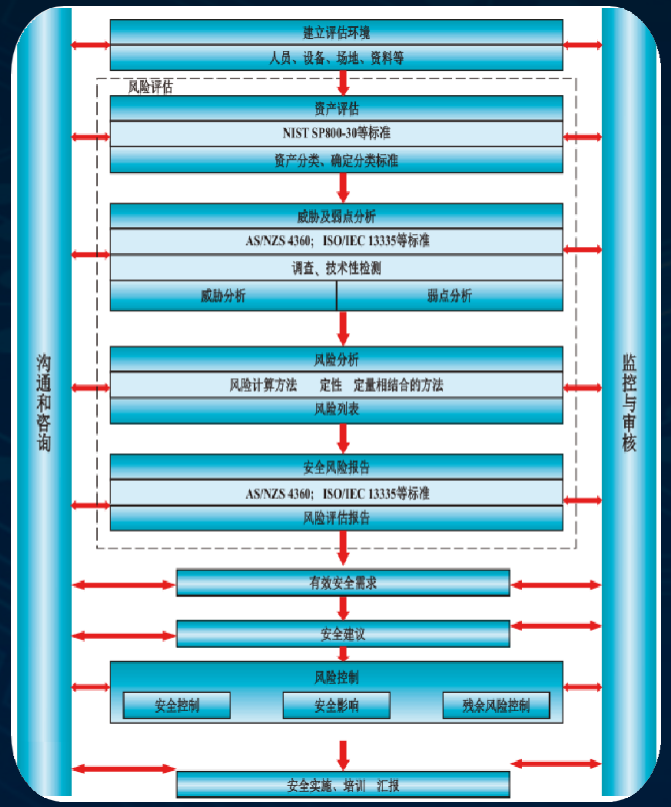
系统所用开源框架 包含java反序列化漏洞，导致远程代码执行。Spring、Struts2的相关安全。	**应用代码关注要素** 日志伪造漏洞，密码明文存储，资源管理，调试程序残留，二次注入，反序列化。	**资源滥用** 不安全的文件创建 / 修改 / 删除，竞争冲突，内存泄露。	**API滥用** 不安全的数据库调用、随机数创建、内存管理调用、字符串操作，危险的系统方法调用。
源代码设计 不安全的域、方法、类修饰符未使用的外部引用、代码。	**SQL注入** 不安全的用户数据输入、判断或过滤机制。	**跨站脚本** 未对用户提交数据进行转义处理或者过滤不足。	**业务逻辑错误** 欺骗密码找回功能，规避交易限制,越权缺陷Cookies和session的问题。
错误处理不当 程序异常处理、返回值用法、空指针、日志记录。	**直接对象引用** 直接引用数据库中的数据、文件系统、内存空间。	**规范性权限配置** 数据库配置规范，Web服务的权限配置SQL语句编写规范。	**代码质量** 未优化代码、未遵循代码编写规范

服务流程

信息安全风险评估

从风险管理角度，运用科学的方 法和手段，系统地分析网络与信息系统所面临的威胁及其存 在的脆弱性，评估安全事件一旦发生可能造成的危害程度， 提出有针对性的防护对策和整改措施，防范和化解信息安全 风险，或将风险控制在可接受的水平。

评估流程



三级资质

CCRC

信息安全服务资质认证证书

证书编号：CCRC-2021-ISV-RA-1288

兹 证 明

北京旗云天下科技有限公司

统一社会信用代码：91110228317919728D

的 **信息安全风险评估** 服务资质符合

CCRC-ISV-C01:2018《信息安全服务 规范》

三级服务资质要求。

注 册 地 址：　北京市大兴区睿和路39号院3号楼3-1011

办 公 地 址：　北京市大兴区睿和路39号院3号楼3-1011

颁证日期：2021年06月10日　　有效期至：2022年06月09日

中国网络安全审查技术与认证中心

中国 · 北京 · 朝外大街甲10号（100020）　www.isccc.gov.cn　证书通过此网站查询

评估内容

服务内容	内容介绍
资产评估	资产评估是对信息系统的各类资产进行识别，对资产进行价值分析，了解资产利用、维护和管理现状；明确资产具备的保护价值和需要的保护层次，从而使组织能够更合理地利用现有资产，更有效地进行资产管理，更有针对性地进行资产保护，进而策略性地进行新的资产投入。
主机安全性评估	主机安全性评估是对各种操作系统，通过技术手段进行分析，发现系统配置和运行中存在的安全隐患。
数据库安全性评估	数据库安全性评估通过分析数据库系统的配置信息，全面检查数据库存在的各种安全弱点，并结合组织的业务特点分析数据库的安全性。
安全设备评估	安全设备评估主要分析安全设备自身的安全配置情况、设备性能等信息，检查安全设备是否对信息系统起到应有的保护作用、是否引入新的安全风险。
网络安全性评估	通过对组织的网络体系进行深入分析,全面地对网络设备配置、网络架构、数据流等方面进行分析,从而了解整个网络的状况，发现网络中存在的安全隐患，并提出网络安全规划解决建议。
安全管理评估	对安全组织机构、安全管理制度、安全运行维护、安全人员培训等方面进行全面评估和分析。
安全加固（可选）	在主机、数据库、安全设备、网络安全性评估的基础上，根据信息系统各种业务的具体应用情况，对发现的风险点进行加固，消除信息系统存在的弱点。

安全产品

安全培训

01

安全意识培训

面向全体员工，包括：个人信息、密码保护意识、终端安全意识、数据安全意识、物理环境安全意识

02

安全开发培训

面向开发人员，主要在软件安全需求分析、安全设计、软件安全测试、安全编码、安全部署及安全开发项目管理

03

数据安全 & 个人信息保护培训

与中国电子标准化研究院合作，提供个人信息保护、数据安全的知识培训，培养个人信息安全保护工程师。

04

安全运维培训

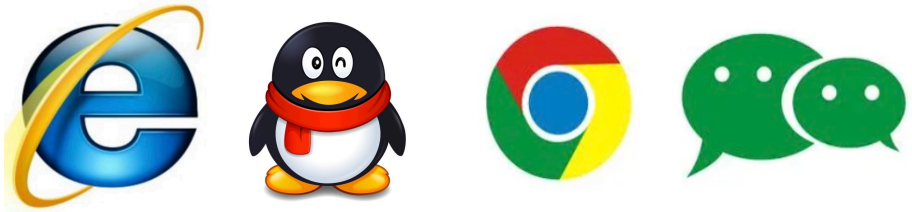
面向运维人员，设备配置与漏洞，信息泄漏，文件泄密，应用层漏洞扫描，服务器安全配置

安全巡检之漏扫

通过web漏洞扫描检查应用层漏洞、网页篡改、挂马、敏感词、可用性等；通过系统漏洞扫描和配置核查可检查操作系统、数据库、服务器、网络设备等的漏洞、弱口令和配置安全。

Web漏扫

Web应用



系统漏扫　　**配置核查**

系统软件

基础硬件

安全巡检之配置核查


主机
操作系统、数据库系统的身份鉴别方式、帐号安全设置、远程管理方式等。
配置核查
中间件
系统和中间件的可用性、完整性、应用的性能等。
网络设备
网络设备的访问控制、路由协议、日志审核等
安全设备
帐号安全设置、管理权限远程访问等安全情况。

安全咨询

等保咨询

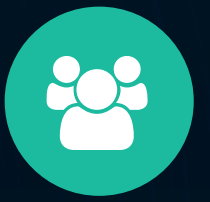
定级服务、差距分析
建设方案整改
等保测评辅助

体系咨询

组织体系、制度体系
技术体系、运行体系
风险识别能力
安全防御能力
安全响应能力
安全恢复能力
安全检测能力

规划咨询

规划范围确认
信息安全需求分析
信息安全愿景目标
信息安全四大体系
信息安全实施计划
安全能力全面提升



攻击溯源

本地攻击溯源分析
攻击事件展示
系统弱点分析
分析防护报告

03

PART

服务优势与客户收益

服务优势

◆ 专业的安全服务团队

拥有国内最专业的安全服务团队，其团队由一批经验丰富，富有责任心和使命感的专业技术人员组成，多人拥有CISP、CISAW、ISO27001等证书及能力；同时拥有大批漏洞发掘和分析人员。

◆丰富的安全技术积累

长期密切跟踪国家等级保护、数据安全法、个人信息保护法等相关政策，参与了等级保护标准制定与研讨，可以在最大程度上使得客户等保相关工作符合国家等级保护相关政策、标准、规范的要求国家项目等多项相关工作；

◆超百家企业的等保服务经验

国内最早从事等级保护咨询的司之一，具有金融/政府/大型企业/医疗/教育等行业的标志性客户，得到 户各级领导认可。成功案例如：商务部等级保护咨询项目、盛银消金等级保护咨询项目、去哪儿网安全等级 防护测评项目。

◆标准化项目管理

每个客户均建立项目工作群组，等保技术专家与客户技术直接对接，便捷高效的沟通，更能高效率的完成项目；项目的实施和管理依据国际化的项目管理规范，通过实施项目管理可以很好地控制项目范围、时间和质量，保证项目能够按照计划按时按质量地顺利完成。

客户收益

满足等保合规要求

- 帮助用户规避合规性风险
- 提高整体网络防护的能力
- 满足行业主管部门的监管要求

降低网络安全风险

- 降低保护对象安全风险
- 被攻击、被窃取

构建主动防御体系

- 被动防御到主动防御转变
- 应急响应到持续响应转变
- 构建监测-分析-预警-响应-优化自适应安全能力

提升应急和安全运维能力

- 实现全网安全威胁可视、可信、可控、可管

04

PART

典型客户案例

客户案例


中工 工会
京能集团
商务部流通产业促进中心 Circulation Industry Promotion Center
国新久其数字科技(北京)有限公司 China Reform Join-Cheer Digital Technology (Beijing) Co.Ltd
中烟云链
顺义环境保护局
360 WWW.360.CN
TAI 太合音乐集团 TAIHE MUSIC GROUP
去哪儿旅行 总有你要的低价
58同城
NANCAL
东方时尚 EASTERN PIONEER
阳光保险集团 Sunshine Insurance Group
天道保险经纪 SPACELINE INSURANCE BROKERS
盛银消费金融 SHENGJING BANK CONSUMER FINANCE
优保联 YOU BAO LIAN 专注科技创新，让保险更简单！
荷叶保严选
惠金所Hfax.com 阳光保险集团旗下成员企业
MAINBO EDUCATION 明博教育
乐教乐学
PU-XIN 朴新教育
龙文教育
VIPKID 在线青少儿英语
成功之道
PONY
精准高心 健康管理有限公司
数坤科技 SHUKUN
HY 汇医慧影 huiyihuiying.com
云柿信息 CLOUD VISION
搏时医疗 TACMED SYSTEM&SOLUTION
拓课云 Talk-Cloud
羚羊云
百家云 BAIJIAYUN.COM
华风爱科 气象科技(北京)有限公司
易宝支付 YEEPAY.COM
神州租车 CAR
哔啦啦
易快报
墨迹天气 关心天气·更关心你
Moka 智能化招聘管理系统
薪八达
大账房

感谢您的聆听

THANK YOU FOR LISTENING