圣博润网络安全保障服务
体系手册

北京圣博润高新技术股份有限公司

2020 年 2 月

文档信息

文档名称	圣博润网络安全保障服务体系手册		
文档管理编号	20200212V8.0		
保密级别	内部	**文档版本号**	8.0
制作人	王彬	**制作日期**	2020-02-12
复审人	王秀毅	**复审日期**	2020-02-15
扩散范围	北京圣博润高新技术股份有限公司内部		
扩散批准人	公开		

适用范围

本文档是 **北京圣博润高新技术股份有限公司-安全服务事业部** 编写的服务介绍文件，仅供相关人员参考。

目 录

1 公司介绍

北京圣博润高新技术股份有限公司是一家专注于网络安全技术研究、产品研发和信息安全服务的高新技术企业。公司成立于 2000 年，目前员工总数 450 余人。公司于 2009 年在新三板挂牌，是中国网络安全五十强企业、2017 年新三板创新层企业。公司是国家网络与信息安全信息通报机制技术支持单位，承担了 2008 年北京奥运会、2016 年杭州 G20 峰会、2017 年“一带一路”国际合作高峰论坛、党的十九大、2018 上合组织青岛峰会、2018、2019 国家实战化网络攻防对抗行动、70 周年大庆等众多国家重大活动的网络安全保卫技术支持任务。

公司主营业务分为两大部分，一是网络与信息安全产品研发、生产、销售，二是信息安全服务。网络安全产品方面，公司累计推出了包括安全防护、安全检测与审计、安全管理、工控安全、云计算安全在内的五大系列近四十个产品，其中堡垒主机产品连续五年市场占有率第一。近年来，公司重点在工业互联网安全领域加快布局，推出了一系列产品和解决方案，获得了工信部 2018 工业互联网创新工程项目支持，为 2018 工业互联网安全防护演练、2018 首届工业互联网安全大赛等国家级活动提供了技术支持。信息安全服务业务方面，公司具有业内最高等级的信息安全服务资质，为政企用户提供等级保护咨询服务、风险评估服务、安全检测与加固服务、认证咨询服务、安全集成与运维服务等。

圣博润在政府和央企行业有着众多的客户案例。公安部、财政部、科技部、海关总署、国家发改委、国家税务总局、国家统计局、国家能源局等五十多个国家部委，中国人民银行、中国工商银行、中国银行等数十家金融机构，中国中车集团、航天科技集团、中航工业集团、华能集团等三十多家中央企业都选择了圣博润的产品与服务。

作为国内最早进入网络与信息安全领域的企业之一，通过多年的经营发展，公司的技术、产品与咨询服务在信息安全行业已经取得了较高的市场认可度，在各级政府机关、中央企业和地方国有企业拥有上万家客户，在全国拥有数百家合作伙伴。公司在运维安全管理和等级保护咨询服务等细分领域居于行业前列，近几年在工业互联网安全领域也开始崭露头角。

公司累计推出了近 40 款网络安全产品，取得了 50 多项软件著作权。公司取

得了中国信息安全认证中心的安全集成、应急处置、风险评估三项最高等级安全服务资质。公司主要用户覆盖政府、金融、军工、电力、烟草、智能制造等领域。

2 安全服务能力介绍

2.1.1 齐备的服务资质

圣博润具备齐备的安全服务资质，服务资质覆盖信息安全服务资质证书-安全工程类二级（次高级），信息安全服务资质认证证书-信息安全风险评估一级、信息安全服务资质认证证书-信息安全应急处理一级、信息安全服务资质认证证书-信息系统安全集成一级、信息安全等级保护安全建设服务机构能力评估合格证书、ISO9001 质量管理体系认证证书和信息安全管理体系证书、ISO27001 等信息安全服务资质，具备专业的信息安全服务能力，可为广大用户提供细致周到的专业信息安全服务。

2.1.2 优秀的服务团队

在人员能力方面，圣博润安全服务事业部现有安全服务人员 40 余名，并在各区域均配备具备丰富安全服务经验的技术人员，具备注册信息安全专业人员（CISP）、国际注册云安全系统专家（CCSSP）、信息安全保障人员认证证书（CISAW）、重要信息系统安全等级保护培训证书（CIIP-T）、注册网络安全防护工程师（CNSA）和信息系统项目管理师等人员资质认证证书，可满足用户的各类安全服务需求。

同时，圣博润安全服务人员具备良好的从业背景，多数服务顾问曾参与过国家部委和中央企业等大型客户安全服务项目，具备丰富的网络安全咨询与服务经验。

2.1.3 安全技术研究能力

多年以来，圣博润持续跟踪、深入分析和理解国家信息安全相关政策及法规，并以严格遵照各项标准为原则，指导产品设计和服务实施。同时根据行业用户网络信息安全需求特点，充分利用自身技术实力和研发优势，不断创新产品技术、

革新服务理念，为用户提供更具行业特色的信息安全解决方案。

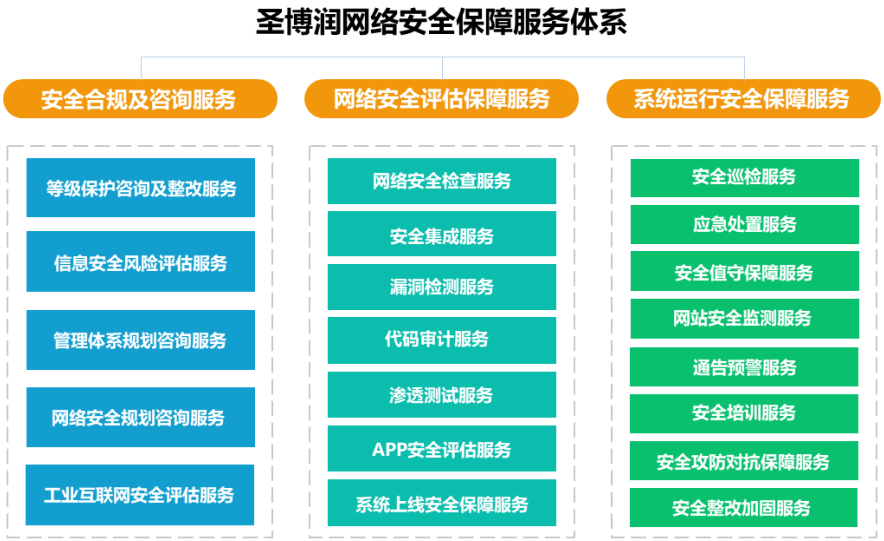
圣博润 2018 年成立攻防实验室，致力于前沿安全技术的跟踪、研究及分享，涉及领域包括：渗透测试、漏洞挖掘、代码审计及攻击溯源等。目的是通过不断分析和研究最新安全技术，为客户提供更为专业的安全咨询服务。

攻防实验室搭建多套常规漏洞靶场（常见 web 漏洞靶场、内网环境靶场、CTF 靶场等），还根据最新发布的漏洞，搭建了 weblogic、Struts2、Gohead、dedecms、wordpress、vulhub、ECSshop 漏洞靶场等测试环境，并对最新漏洞进行分析及复现。攻防实验室准备研发出属于一套网站监测预警系统，可对客户网站的可用性、安全事件及安全漏洞进行实时监测并发送预警，保障客户第一时间了解网站的安全状况。

3 网络安全保障服务体系

目前，我国网络安全领域已经步入新的时代，圣博润安全服务事业部不忘自身使命与义务，结合新形势、新要求下的网络安全治理需求，贯彻落实安全服务一体化交付理念。希望可以解决企业网络安全工作落实及强化痛点，帮助企业树立动态、综合的防护理意识，维护企业的网络安全。

为此，我们建立了完善的信息安全服务体系，服务方向包含网络安全合规及咨询服务、网络安全评估保障服务和系统运行安全保障服务三大层面，覆盖 20 类安全服务项目。可为广大用户提供常态化、体系化的安全咨询保障，帮助用户满足国家法规和政策要求，基于自身业务需求建立健全网络安全管理和技术防护体系，确保用户关键信息系统的持续安全运行。



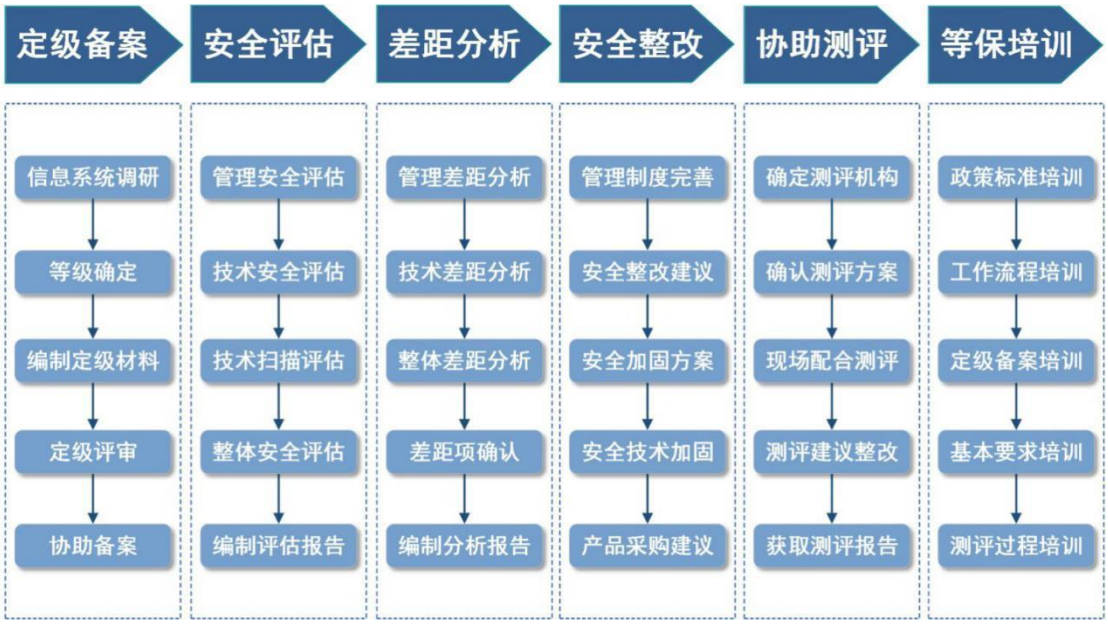
圣博润网络安全保障服务体系图

3.1 安全合规及咨询服务

3.1.1 等级保护咨询及整改服务

圣博润根据国家相关部门的要求，结合《信息系统等级保护定级指南》、《信息安全技术 网络安全等级保护的基本要求》、《信息安全技术 网络安全等级保护测评准则》等标准，为企事业单位有效的开展等级保护工作提供全面的等级保护

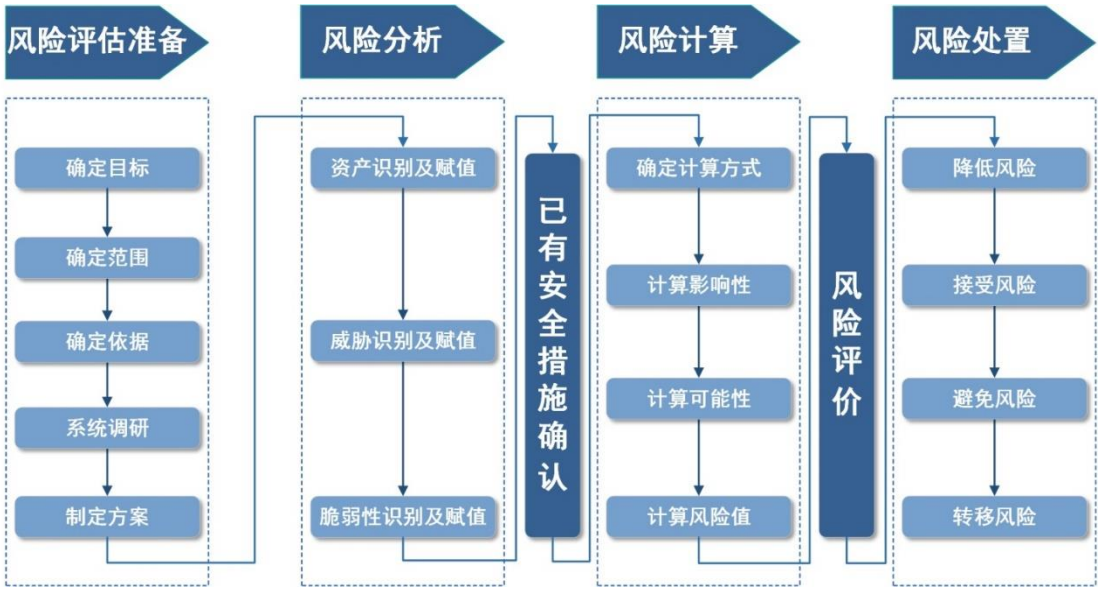
咨询服务，并且对于评估过程中发现的安全风险，我们可以提供完备的策略调优和安全加固服务，根据等级保护的实施流程，提供等级保护咨询服务总体框架如下图所示：



3.1.2 信息安全风险评估服务

圣博润将结合 GB/T 20984-2007、ISO13335、OCTAVE 等标准的内容，以半定量定性的方法对信息资产进行全面的风险评估工作。评估对象主要包括组织人员机构、管理制度、工作流程、网络架构、服务器应用、应用流程等方面。评估工作的进行主要就信息资产、威胁和脆弱性之间的相互关系，分别以资产和业务流程为核心完成其信息系统风险管理过程中的风险鉴定、分析、评价和处理等工作，帮助企业开展全面的风险管理工作。评估方法主要基于 SWOT 模型的业务分析，PDCA 可持续性实施；多元矩阵法的多方位分析；绩效测量机制的风险控制和绩效控制；全方位数据挖掘技术的多层面结果展示等。

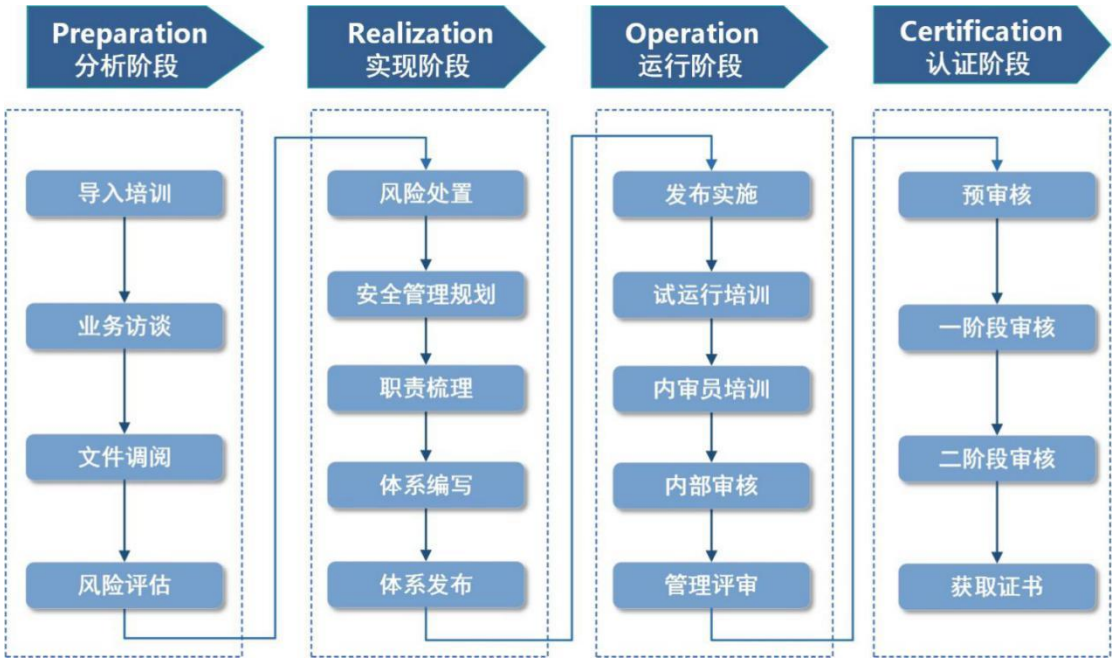
具体内容如下图所示：



3.1.3 网络安全管理体系规划咨询服务

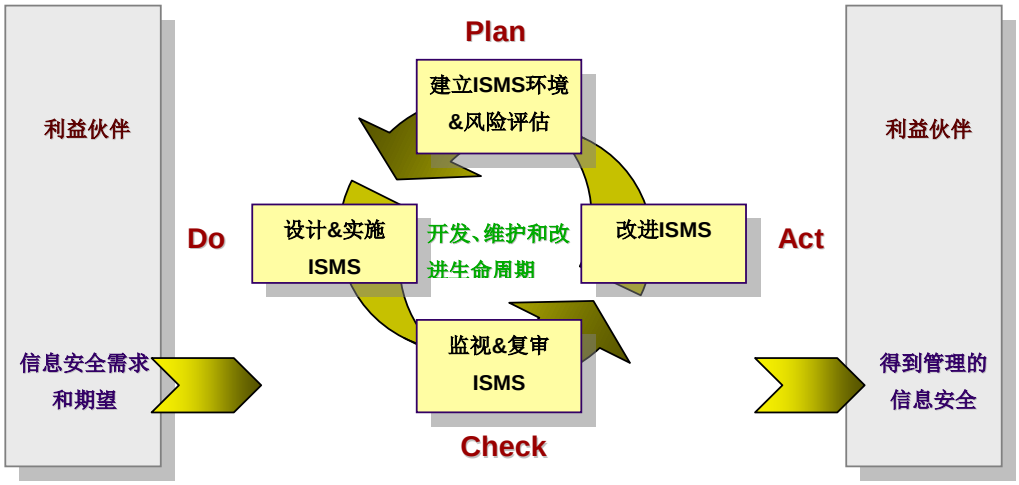
➢ ISO27001 认证咨询服务

圣博润依据 ISO27001 标准，将信息安全管理方法、理念、意识、技术和解决方案通过项目传递给客户，帮助客户解决切实的信息安全问题，并且掌握解决问题的机制和方法。从管理、技术、人员、过程等多角度定义、建立、实施信息安全管理体系，从多个层面保障组织的信息安全，进而解决大型企业和机构内不同部门信息安全建设不一致的问题。



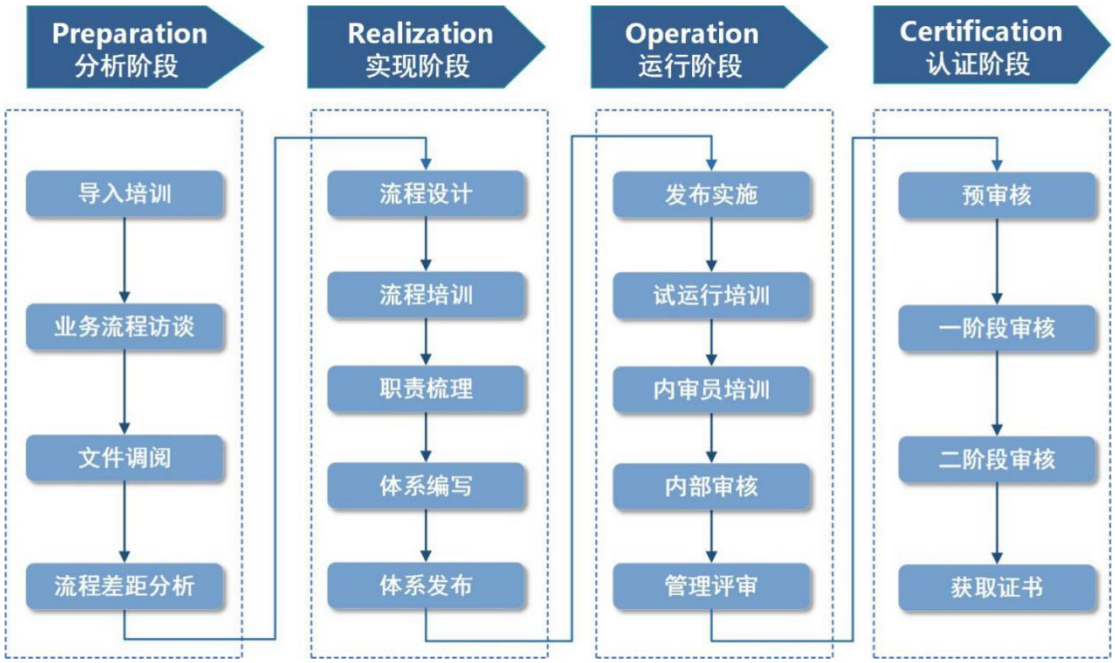
圣博润将根据评估结果，为企业制定具体安全方案、管理制度、工作流程和

操作指引。避免企业各部门在信息安全建设中容易产生的盲目性、重复性建设问题，帮助企业建立符合国际规范的有效的信息安全体系。其信息安全体系建设的基本模型如下：



- ISO20000 认证咨询服务

ITIL 是 ITSM 最佳实践标准，是了解及衡量 IT 服务价值的渠道。圣博润长期的研究和实践，帮助企业分析 IT 服务管理现状，设计、实施并结合 ITIL 服务管理标准，改进客户的 IT 服务管理体系，增强 IT 运作的可预见性，改善客户组织的整体绩效，为客户参与国际市场竞争和新业务拓展提供可靠的管理体系保障，并形成了一套先进的 ITIL 理念与我国国情密切结合、适合当前发展水平的 IT 服务管理解决方案，为金融、电力等行业的客户提供 ISO/IEC 20000 认证咨询服务，目的是帮助客户创建一个符合组织 IT 服务管理需要的，基于 ISO/IEC 20000 的系统，把服务支持、服务交付、日常运维等流程电子化、自动化。充分的将业务与 IT 进行有效的整合。



3.1.4 网络安全规划咨询服务

在充分了解用户需求及对用户开展详细的评估分析后，针对性的为用户提供网络安全规划设计、可行性研究和初步设计等服务。另外，可为用户提供网络安全相关的课题研究支持服务，帮助用户完成相关课题的研究工作。

3.1.5 工业互联网安全评估服务

基于《网络安全等级保护基本要求》（工控扩展要求）、《工业互联网安全防护工作指南》、《工业互联网安全防护检测指南》、《工业互联网安全评测过程指南》通过访谈、配置核查、漏洞扫描、渗透测试等手段，对工业企业系统进行安全评估，及时发现系统中存在的安全风险，并提出安全防护措施及整改建议。

3.2 网络安全评估保障服务

3.2.1 网络安全检查服务

全面提升国家关键基础设施网络安全防护保障能力和水平，依据《中华人民共和国网络安全法》等国家相关政策规定及国家网络安全技术标准规范，推动和加强政府部门和企事业单位网络安全检查工作，国家和主管部门陆续推动了一系

列的网络安全检查工作，发现网络安全漏洞隐患、风险和突出问题，督促安全整改工作，提升各单位网络安全防护能力和管理水平，防范重大网络安全事件的发生。

因此，圣博润结合丰富的安全检查经验，可为行业主管部门及政府部门和企事业单位，根据不同的工作要求，提供不同程度的网络安全检查服务。协助政府部门和企事业单位摸清网络安全风险、排除网络安全漏洞，落实网络安全责任。

圣博润可以从两个层面为用户提供网络安全检查服务：

1. 按照国家要求、自身监管职责等工作要求或计划，配合主管部门对下级单位开展网络安全大检查，制定检查工作方案，明确整体工作流程，从网络安全基本情况、等级保护工作开展情况、网络安全管理制度落实情况、网络安全监测预警情况、网络安全应急工作情况、网络安全教育培训情况等方面，辅助关键设备安全配置核查、关键系统渗透测试、漏洞扫描等技术工作，对下级单位网络安全工作开展和防护情况进行全面的检查。
2. 协助用户应对国家和上级主管部门网络安全大检查或从自身出发摸清网络安全工作情况。通过以下检查内容：网络安全基本情况、等级保护工作开展情况、网络安全管理制度落实情况、网络安全监测预警情况、网络安全应急工作情况、网络安全教育培训情况等方面的检查，辅助关键设备安全配置核查、关键系统渗透测试、漏洞扫描等技术工作，全面梳理当前网络安全工作和防护情况，以便于填写相关自查表单或报告，为用户出具安全整改建议，并配合现场检查工作。

3.2.2 网络安全集成服务

根据客户需求，圣博润可为客户提供安全产品和安全服务全过程咨询，包括确定业务需求、确定安全产品需求、安全产品选型、安全产品部署规划、安全产品运维机制建立等内容，为客户设计安全集成方案，帮助客户选择花费合理的资源，获得合适的安全产品，并确保安全产品起到真正效果，满足业务发展需求。

3.2.3 漏洞检测服务

漏洞扫描阶段是渗透测试的前提，负责收集网络和业务系统中存在的安全漏洞，收集相关安全漏洞信息，通过漏洞扫描收集的信息可以对网络和业务系统的安全情况有比较深入的了解。

圣博润漏洞扫描服务主要分为基于主机的和基于网络的两种，前者主要关注软件所在主机上的风险与漏洞，而后者则是通过网络远程探测其他主机的安全风险与漏洞，查找网络结构、网络设备、服务器主机、数据和用户账号/口令等安全对象目标存在的安全风险、漏洞和威胁。

3.2.4 代码审计服务

圣博润可对用户信息系统代码提供整体全面的代码安全审计服务。发现（源）代码存在的安全漏洞，并对导致安全漏洞的错误代码进行定位和验证，提供修复方案。语言方面可以支持：Java，JSP，C，C++，NET（C#），XML，ASP，PHP，JS，VB 等。运行环境支持：Windows，Red Hat Linux，Ubuntu，Centos，麒麟 Linux 等主流系统。

代码审计服务的范围包括使用 Java，JSP，C，C++，NET（C#），XML，ASP，PHP，JS，VB 等主流语言开发的 B/S、C/S 应用系统，以及使用 XML 语言编写的文件、SQL 语言和数据库存储过程等，运行环境支持 Windows，Red Hat Linux，Ubuntu，Centos，麒麟 Linux 等主流系统。

源代码安全审计服务从数据流分析、控制流分析、语义分析、配置分析、结构分析等五个方面全面分析软件源代码安全问题。

借助源代码分析工具，针对信息系统源代码扫描、分析，语言方面可以支持：Java/JSP C/C++，NET 平台，TSQL/PLSQL，Cold Fusion，XML，CFML，ASP，PHP，JS，VB 等。操作系统方面支持：Windows,Solaris，Red Hat Linux，Mac OS X，HP-UX，IBM AIX 等并对导致安全漏洞的错误代码进行定位和验证，提供修复方案。

源代码审计服务主要分为四个阶段，包括代码审计前期准备阶段、代码审计阶段实施、复查阶段实施以及成果汇报阶段：

➢ 前期准备阶段

在实施代码审计工作前，技术人员会和客户对代码审计服务相关的技术细节进行详细沟通。由此确认代码审计的方案，方案内容主要包括确认的代码审计范围、最终对象、审计方式、审计要求和时间等内容。

➢ 代码审计阶段实施

在源代码审计实施过程中，技术人员首先使用代码审计的扫描工具对源代码进行扫描，完成初步的信息收集，然后由人工的方式对源代码扫描结果进行人工的分析和确认。

根据收集的各类信息对客户要求的重要功能点进行人工代码审计。

结合自动化源代码扫描和人工代码审计两方的结果，代码审计服务人员需整理代码审计服务的输出结果并编制代码审计报告，最终提交客户和对报告内容进行沟通。

➢ 复测阶段实施

经过第一次代码审计报告提交和沟通后，等待客户针对代码审计发现的问题整改或加固。经整改或加固后，代码审计服务人员进行回归检查，即二次检查。检查结束后提交给客户复查报告和对复查结果进行沟通。

➢ 成果汇报阶段

根据一次代码审计和二次复查结果，整理代码审计服务输出成果，最后汇总形成《信息系统代码审计报告》。

3.2.5 渗透测试服务

渗透测试（Penetration Test）是完全模拟远程黑客攻击，利用各种主流的攻击技术和漏洞发现技术，对目标系统的一些隐形存在的安全漏洞和风险点作深入的探测，发现系统最脆弱的环节。渗透测试能够直观的让信息主管对信息系统的安全性有较深的感性认知，在系统进行了安全加固之后进行渗透测试，则可以用于验证经过安全保护后的网络是否真的达到了安全目标。

圣博润提供国内领先的专业网络渗透测试服务，对客户的信息管理系统、Web系统、邮箱系统、办公自动化系统等多种 B/S 和 C/S 架构的系统进行网络安全渗透测试。圣博润渗透测试工程师以模拟黑客团队的方式进行多角度的全面协同渗

透测试，渗透测试的范围主要包括对服务器端的注入攻击、访问控制攻击、非授权的认证和会话攻击测试等，以及对服务器端应用程序和操作系统的远程漏洞攻击测试等；还包括针对客户端的跨站脚本攻击、跨站请求伪造攻击、点击劫持攻击测试等，以求全面检测系统的入侵点和安全漏洞。最后根据渗透测试的结果给出相应的安全加固措施及其反制手段。

3.2.6 APP 安全评估服务

针对于 APP 类移动应用系统，圣博润提供 APP 安全检测服务，可通过通信数据分析、编译和运行模拟等方式，检测 Android 与 iOS 两大平台应用系统的漏洞、恶意代码和后门程序等，检测内容覆盖 APP 的客户端程序安全、组件安全、进程安全、敏感信息安全、网络通信安全和服务端安全。具体测试内容包含但不限于：

序号	测试项	测试内容
1	客户端程序安全	反编译保护检测
2		安装包签名检测
3		应用完整性校验检测
4		程序数据任意备份
5		程序可被任意调试
6	组件安全	Activity 越权检测
7		Activity 拒绝服务检测
8		Activity 劫持保护检测
9		Service 越权检测
10		Service 拒绝服务检测
11		Receiver 越权检测
12		Receiver 拒绝服务检测
13		Provider SQL 注入检测
14		Provider 目录遍历检测
15		WebView 代码执行检测
16		WebView 未移除接口检测
17	进程安全	Root 环境检测
18		Ptrace 注入检测
19	敏感信息安全	SQLite 加密检测
20		SQLite 敏感信息检测
21		SharedPref 加密检测
22		SharedPref 敏感信息检测
23		Log 敏感信息检测

序号	测试项	测试内容
24	网络通信安全	通信加密检测
25		关键字段加密检测
26		安全退出检测
27		网络切换保护检测
28		开放端口检测
29	服务端安全	跨站脚本攻击
30		用户名枚举

3.2.7 系统上线安全保障服务

在信息系统上线前，应确保新建信息系统得到足够的安全保障，无潜在安全风险，具备上线运行条件，满足合规要求。因此为保障新上线系统或升级改造系统的安全、稳定运行，降低因网络信息系统漏洞、配置错误、黑客攻击、病毒传播、系统故障等影响业务的风险。圣博润可提供系统上线安全检查服务，按照相关标准进行检测，确保新上线业务信息系统满足安全要求，提供评估报告，切实提高系统的整体安全防护能力。

系统上线前安全保障服务包括：源代码审计、安全配置检测、安全漏洞扫描和渗透测试等保障工作，切实提高用户新建系统防入侵、防窃密、防篡改的综合防护能力，坚决防止发生重大网络安全事件，使得信息安全工作能够居安思危，防患于未然。

3.3 系统运行安全保障服务

3.3.1 安全巡检服务

圣博润派遣专业服务工程师到现场进行安全维护服务，对客户网络及重要服务器进行分析，主要包括网络、安全设备的配置检查，对网络和安全设备的运行状态、安全策略、漏洞库等进行安全配置核查；服务器配置核查，对服务器资源、身份鉴别、默认配置、共享设置、补丁管理、日志等进行安全配置核查；安全设备日志分析，检查防火墙、入侵检测和其他安全设备的日志信息，对其进行分析，排查网络中可能发生的安全事件；服务器木马查杀，采用智能木马检测技术，可高效、准确识别服务器或终端电脑中存在的恶意程序，使安全管理员能够第一时

间获知安全隐患，避免不法分子利用肉鸡进行大规模的安全攻击。

3.3.2 应急处置服务

圣博润的“安全应急响应”服务能够向客户提供必须的资源来完善安全防护，抵抗攻击，进行安全修复，并减少未来安全漏洞产生的可能性。安全响应服务提供了快捷的服务支持和 7×24 的应急响应服务，确保当网络安全出现状况时，能够第一时间进行响应，配合客户将危险降到最低。应急响应服务的内容主要包括：入侵调查、主机系统异常响应、其他紧急安全事件等。

3.3.3 安全值守保障服务

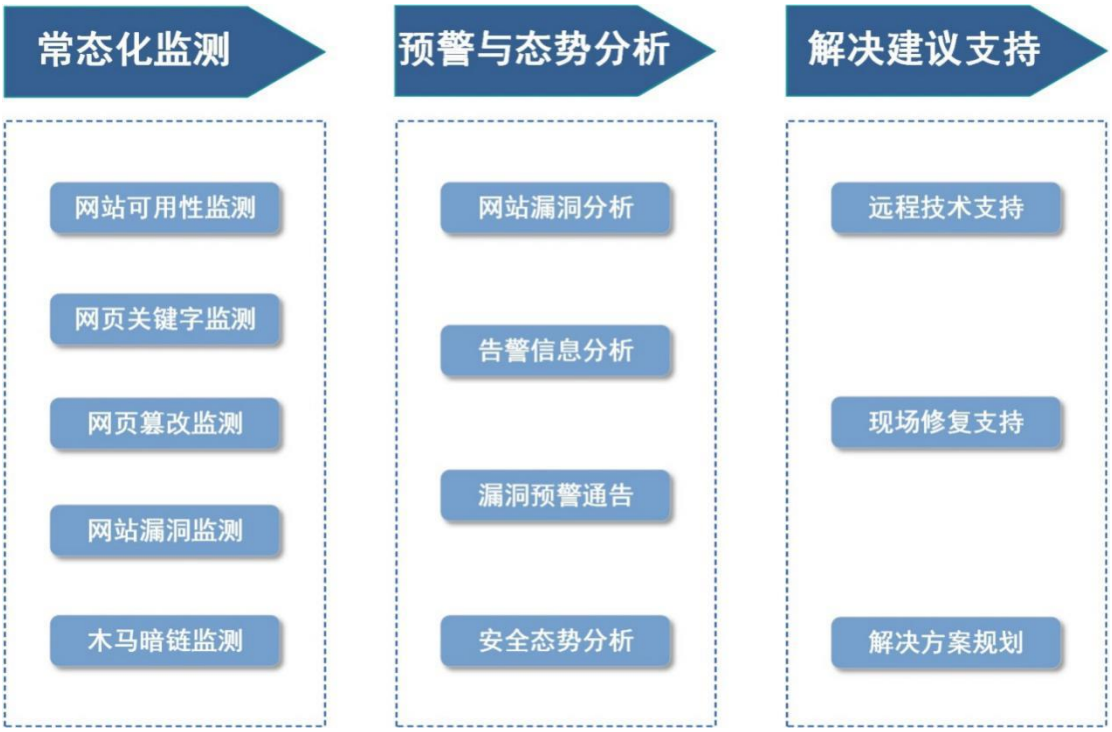
圣博润将秉承“总体工作筹划、事前排查整改、事中监控处置、事后分析总结”的思路开展具体实施工作，为用户提供重要时期安全值守保障服务。

具体工作内容如下：

- 总体工作筹划主要为重保活动前的网络安全，做好协调联动保障规划，包括建立安全保障小组、制定应急处置预案、应急演练，并开展相关的宣贯和培训等工作；
- 事前排查整改可以有效的减少现有安全风险，主要工作为互联网隐患排查、安全配置脆弱性检查、系统安全漏洞隐患排查、应用系统安全隐患排查和安全隐患加固；
- 事中监控处置是重保工作的核心，前期工作可以有效减少系统被攻破的可能性，事中的监控和处置则可以有效应对安全事件，减少安全事件影响，此阶段，圣博润将开展互联网安全监控、预警通告、现状安全值守和应急处置等工作。
- 事后分析总结主要对整个工作周期的各类数据进行整理，满足内部和监管要求，并且利用评估、监控和应急处置结果，可有效为未来的网络安全管理与防护工作进行系统化的规划设计。

3.3.4 网站安全检测服务

圣博润网站安全监测服务，是一项托管式服务，客户无需安装任何硬件或软件，无需改变目前的网络部署状况，无需专门的人员进行安全设备维护及分析日志。网站安全监测服务包括常态化监测、预警与态势分析、解决建议三大项服务，详细内容见下图：



3.3.5 安全通报预警服务

圣博润“安全通告服务”主要包括安全预警和安全报告两部分内容，首先圣博润结合当前信息安全的态势，针对重大安全漏洞和问题，发出安全预警通知，并提出有效的安全预警措施和方案。同时，圣博润密切关注黑客攻击技术的发展和安全防范技术的最新演变，跟踪操作系统、应用程序等各种最新的漏洞补丁更新，掌握最新的安全动态，将最新的重要网络安全问题报告给用户。

3.3.6 安全培训服务

根据客户自身实际需求，圣博润可提供安全培训，分为安全课程、实训平台演练、组织攻防竞赛三类。

安全课程培训主要包括安全法与标准类课程培训、安全管理类课程培训、安全技术类高级课程培训、安全技术类初级课程培训和安全意识类课程培训，从自身提高信息安全意识与技术水平；实训平台演练分为实训课程考核与攻防竞技演练两部分，讲究理论与实践的相结合，通过理论带动技术，通过技术加强实践，达到信息安全技术水平的双向提高；攻防竞赛主要是通过组织内部成员进行单兵演练、分组红蓝对抗或者混战的方式，模拟网络攻防的真实场景，提高自身的技术水平。

3.3.7 安全攻防对抗保障服务

网络安全的本质在对抗，对抗的本质在攻防两端能力的较量。从主管部门近年的动作也可以看出，实战的攻防演练力度越来越大，并总体上来看实战演练还处于阶段化和周期化。但从本质上来看，网络安全的本质在于对抗，信息系统时时刻刻不面临着真实的攻击威胁，单纯的专项实战可能在一个时段内带来较好的效果，可是当演练结束，各类技术支持退场，后续的安全防护和处置管理又该如何开展。

针对以上问题，我们认为，安全能力建设在于常态化，也就是开展常态化的网络安全实战演练，与渗透测试服务相比，常态化的网络安全实战演练服务比传统的渗透测试要更贴近实战，更类似红蓝对抗，通过全年不定时不定周期不定目标的实战攻击，在不破坏系统和全程可监控、可审计的前提下，随机发现内部信息系统的安全隐患，发现内部监控死角，锻炼内部安全监控和处置能力。对于用户的安全能力提升会有更大的提升。

为更好的应对实战化的网络安全演练需求，保障用户信息系统安全运行，应对主管部门和重保时期安全工作要求。圣博润网络安全实战演练支持服务整体内容包含三部分：

一、 常规技术检查

安全工作在于常态化，无论是日常的安全管理，还是应对主管部门组织攻防演练，还是重要时期的安全保障，都需要在前期开展常规化的技术检查。我们根据日常安全保障和实战演练攻防经验，可针对化的为用户提供资产梳理、风险识别、安全监测、安全巡检、安全加固和安全建设

等服务，识别现有安全风险、加强安全监控、进行安全整改，减少安全风险的同时提升整体安全防护能力。

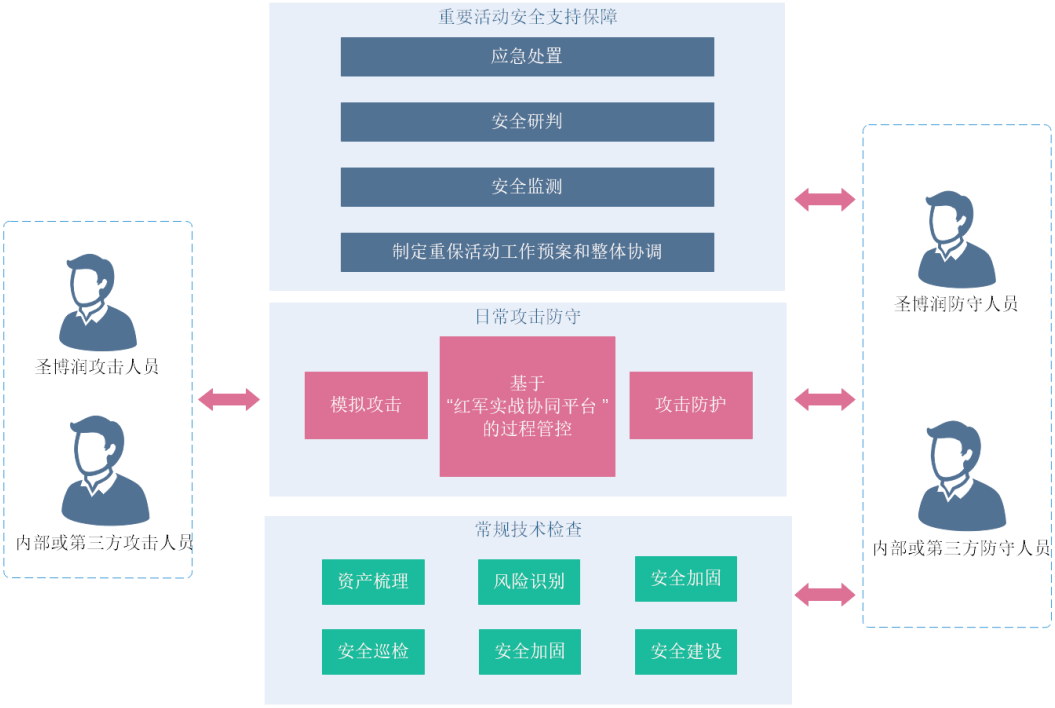
二、 日常攻击及防护

摒弃常规的渗透测试服务方式，提倡红蓝对对抗理念，加强整体的过程监控和能力提升，利用“红军实战协同平台”以我方驻场或非驻场、用户安排内部技术人员或第三方攻击人员的方式，开展长时间，不定目标、不定路径的模拟攻击，全面深入的发现用户网络内的安全问题，在攻击的同时，检验用户内部安全防护机制，不断的加强安全防护能力和内部监控处置能力。并且通过“红军实战协同平台”实现全过程的、全漏洞成功、全攻击工具的监控与管理，并形成知识的积累，为用户赋能。

三、 重要活动安全支持保障

最后，除日常工作外，主管部门组织的实战攻防演练和重保时期（两会、国家或地区重要活动）的安全防护和保障也是必不可少的。我们可以凭借丰富的保障服务经验，为用户提供切实可行的整体安全防护保障工作方案和协调服务、基于自有或第三方安全产品的安全监控服务、对监控到安全事件的分析研判服务，已确认安全事件的应急处置服务和整体总结复盘。

具体服务框架如下：

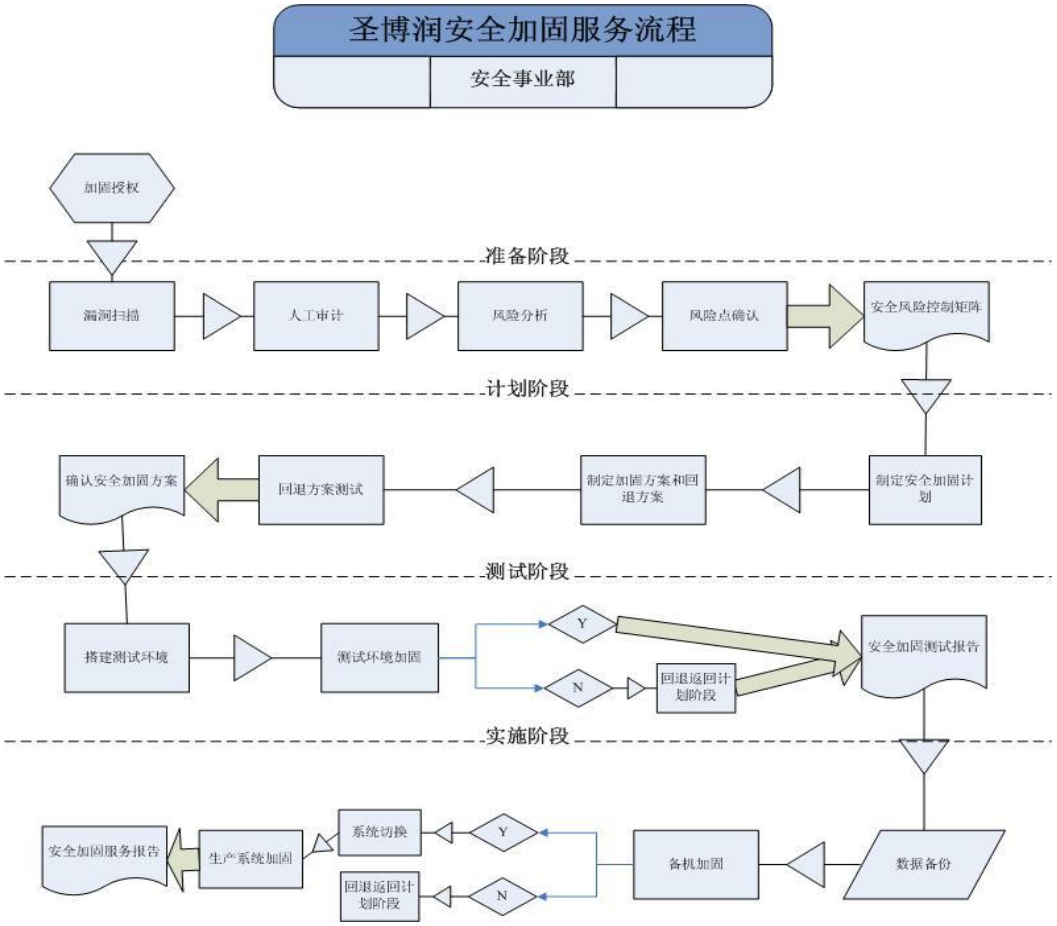


总体框架图

3.3.8 安全整改加固服务

系统安全加固是指通过一定的技术手段，对信息系统中的主机、网络系统、数据库系统、应用程序的脆弱性进行分析和修补。提高信息系统整体安全性和抗攻击能力。

根据客户的具体要求，圣博润设计出一套成熟的工作方法和流程来为客户进行加固服务。系统安全加固流程图如下：


圣博润安全加固服务流程
安全事业部
加固授权
准备阶段
漏洞扫描
人工审计
风险分析
风险点确认
安全风险控制矩阵
计划阶段
确认安全加固方案
回退方案测试
制定加固方案和回退方案
制定安全加固计划
测试阶段
搭建测试环境
测试环境加固
Y
N
回退返回计划阶段
安全加固测试报告
实施阶段
安全加固服务报告
生产系统加固
系统切换
回退返回计划阶段
Y
N
备机加固
数据备份

4 网络安全保障服务优势

（一）公司 2009 年成功上市

北京圣博润高新技术股份有限公司（以下简称“圣博润”）是中关村科技园区内的股份制高新技术企业，并于 2009 年在深圳证券交易所代办转让系统挂牌，进行股份报价转让。公司证券代码“430046”，公司自 2000 年成立以来专注于具有自主知识产权信息安全产品及服务的研究、开发与推广，是国内专业的信息安全咨询服务和信息安全产品解决方案提供商。

（二）服务团队与人员资质

圣博润具有领先的信息安全风险管理技术及丰富的信息安全咨询经验。公司安全服务事业部现有 40 余人，具有专业化的信息安全咨询人才（拥有多名 CISSP、CISA、CISP、ISO27001LA、CCIE、ITIL、CoBit 认证专家）。在信息安全风险评估、等级保护定级咨询、等级保护安全评估、等级保护建设整改方案规划、等级保护建设整改实施、渗透测试、网站监测、安全运维等方面具有丰富的经验。

（三）承担了国家发改委等级保护信息安全专项课题

圣博润自 2006 年开始关注和研究等级保护相关政策、技术、产品和服务。2009 年承担了国家发改委《重要信息系统安全测评和评估》专项中的重要信息系统测评支撑系统的研制开发，并于 2011 年顺利通过验收。该项目充分证明了圣博润在我国信息安全等级保护工作领域所具备的专业技术积累和丰富的咨询经验。

（四）参与了多项重大活动的网络安保技术支持工作

圣博润 2008 年在北京奥运会期间，为奥运会保驾护航，维护网络安全；2012 年参与了“十八大网络安全保卫”工作；2013 年和 2015 年参与了“全国重要信息系统和政府网站安全专项检查”工作；2016 年为“G20 峰会”提供网络安保服务，7*24 小时监测网络状态，保障了 G20 峰会期间网络与信息安全的平稳态势，确保信息系统安全可靠运行；2017 年圣博润助力“两会”、金砖会晤、“十九大”等重要会议，进驻重点保卫单位开展监测、值守、应急等工作，同时提供 7*24 小时网站监测服务，保障网站的安全运行。2018 全力支持了“上合组织青岛峰会”、“2018 护网行动”、“港珠澳大桥开通”“70 周年大庆”等 10 余个重要活动的网络安全保障工作。以上安保工作的出色完成充分证明了圣博润有着过硬的技术

能力和丰富的信息安全服务经验。

（五）与国内多加等级测评机构保持密切合作关系

圣博润与国内多家等级测评机构保持着密切的技术交流与合作。与国家信息安全测评中心、公安部三所、公安部一所、人民银行、电监会、教育部等国家级和行业的等级保护测评机构一致保持密切的合作关系。在信息等级保护技术支持工作中发挥着越来越重要的作用。

（六）推出了多款与等级保护政策配套的等级保护管理工具

圣博润在等级保护咨询服务基础上，配合我国等级保护相关政策，针对测评机构和信息系统运营使用单位，推出了多款等级保护管理工具。信息安全等级保护测评与评估支撑系统是一款针对测评机构开发的管理工具，等级保护综合管理系统是一款针对信息系统运营使用单位开发的管理工具。这些工具在国家部委、中央企业、地方国资委企业中拥有广泛的客户。这也充分展示了圣博润在等级保护方面的技术积淀和优势。

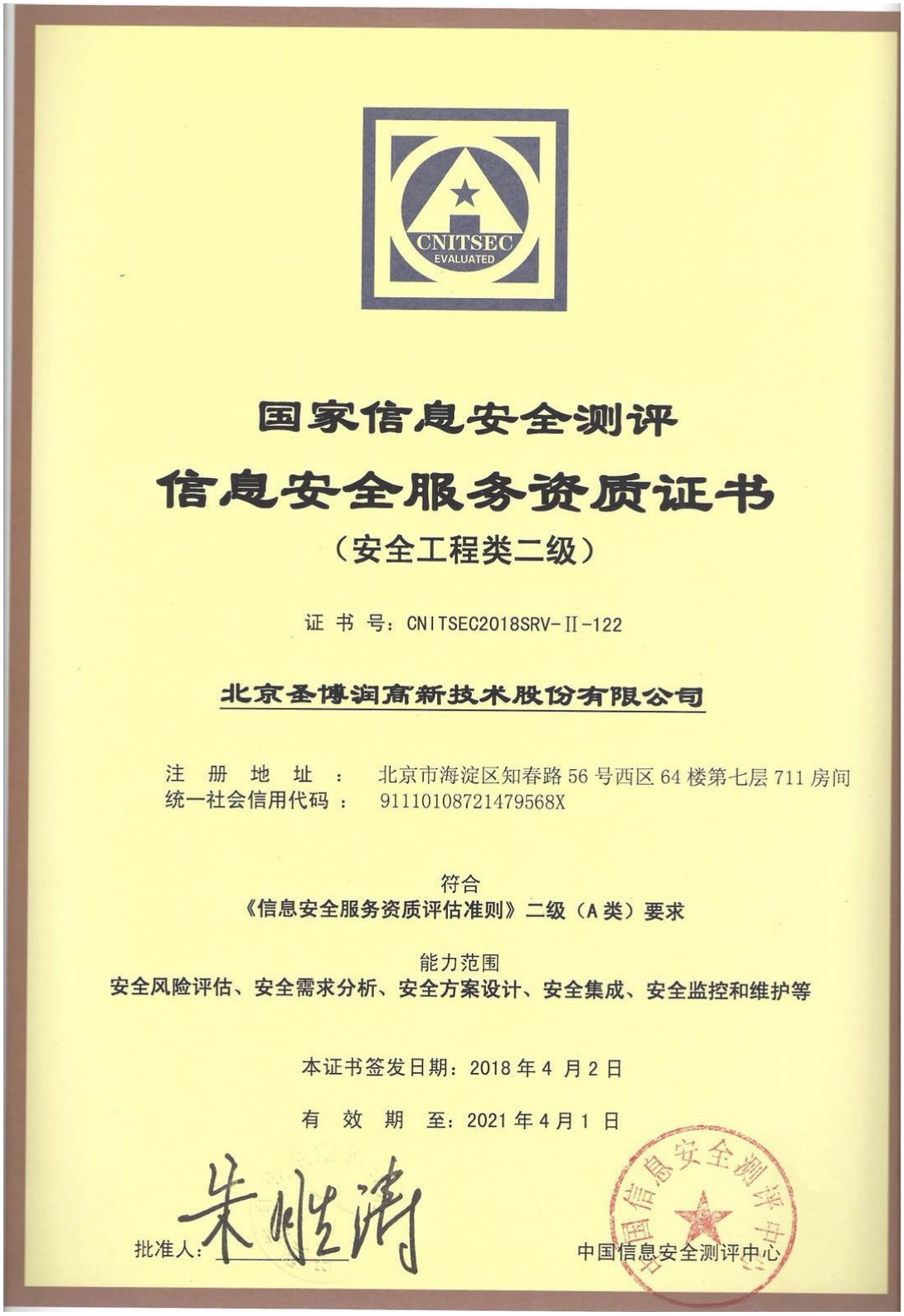
5 典型客户和案例

- 国家质量监督检验检疫总局质检系统 2017 年度网络安全检查项目
- 国家质量监督检验检疫总局质检政府网站信息安全监测服务项目
- 国家质量监督检验检疫总局国际检验检疫标准与技术法规研究中心信息安全咨询服务项目
- 中国地震台网中心信息系统安全等级保护测评项目
- 国家食品药品监督管理总局网络系统安全运行维护服务项目
- 国家食品药品监督管理总局执业药师注册管理网络信息系统安全集成服务
- 国家发展改革委员会信息系统风险评估项目
- 国家信息中心-全国信用信息共享平台项目（二期）风险评估
- 交通运输部公路科学研究院信息系统等级保护咨询服务项目
- 中国烟草总公司网络信息安全等级保护服务项目
- 中国中铁股份有限公司网络安全检查项目
- 中国中材集团有限公司信息安全规划咨询项目
- 中国盐业总公司服务区网络系统等级保护项目
- 中国建筑股份有限公司信息安全等级保护服务项目
- 兵工财务有限责任公司等级保护咨询服务项目
- 航天科技集团等级保护咨询服务项目
- 航天投资控股有限公司等级保护咨询项目
- 航天科技财务有限责任公司等级保护咨询项目
- 航天电子技术研究院等级保护咨询项目
- 中国宇航出版有限责任公司等级保护咨询服务
- 中国资源卫星应用中心等级保护咨询服务项目
- 中国卫通通信集团公司信息安全咨询服务项目
- 中国长城工业总公司信息系统安全评估项目
- 中国人民健康保险股份有限公司信息安全咨询规划项目
- 中材集团财务有限公司网上金融服务系统风险评估项目
- 人保财险信息系统等级保护评估项目
- 国药集团药业股份有限公司信息系统渗透测试项目

- 国家烟草局、中国烟草总公司安全评估项目
- 湖南中烟工业有限责任公司信息安全检查服务项目
- 湖南中烟等级保护安全测评及安全检查项目
- 湖北中烟等级保护安全测评及安全检查项目
- 青海烟草等级保护咨询服务项目
- 陕西省金保工程信息安全预警防范系统建设项目
- 广东省基层医疗卫生机构管理信息系统风险评估项目
- 青岛海尔工业互联网安全评估和标准化建设项目
- 中原农业保险股份有限公司网站检测项目
- 民生证券信息安全风险评估项目
- 北京市发展和改革委员会信息系统安全测评项目
- 北京市文化局安全评估、加固及渗透测试服务项目
- 北京市安全生产监督管理局安全运维项目
- 北京农学院网络信息安全运维服务项目
- 北京市经济和信息化委员会安全评估及加固项目
- 北京市丰台区财政局信息安全等级保护安全加固服务项目
- 北京市信访综合办公系统风险评估项目
- 北京市档案馆信息系统安全运维项目
- 信通院工业互联网安全检查项目
- 中国人寿保险股份有限公司研发中心安全技术服务项目

6 资质和荣誉

6.1 信息安全服务资质证书



CNITSEC EVALUATED

国家信息安全测评

信息安全服务资质证书

（安全工程类二级）

证 书 号：CNITSEC2018SRV-Ⅱ-122

北京圣博润高新技术股份有限公司

注 册 地 址 ： 北京市海淀区知春路 56 号西区 64 楼第七层 711 房间
统一社会信用代码 ： 91110108721479568X

符合
《信息安全服务资质评估准则》二级（A 类）要求

能力范围
安全风险评估、安全需求分析、安全方案设计、安全集成、安全监控和维护等

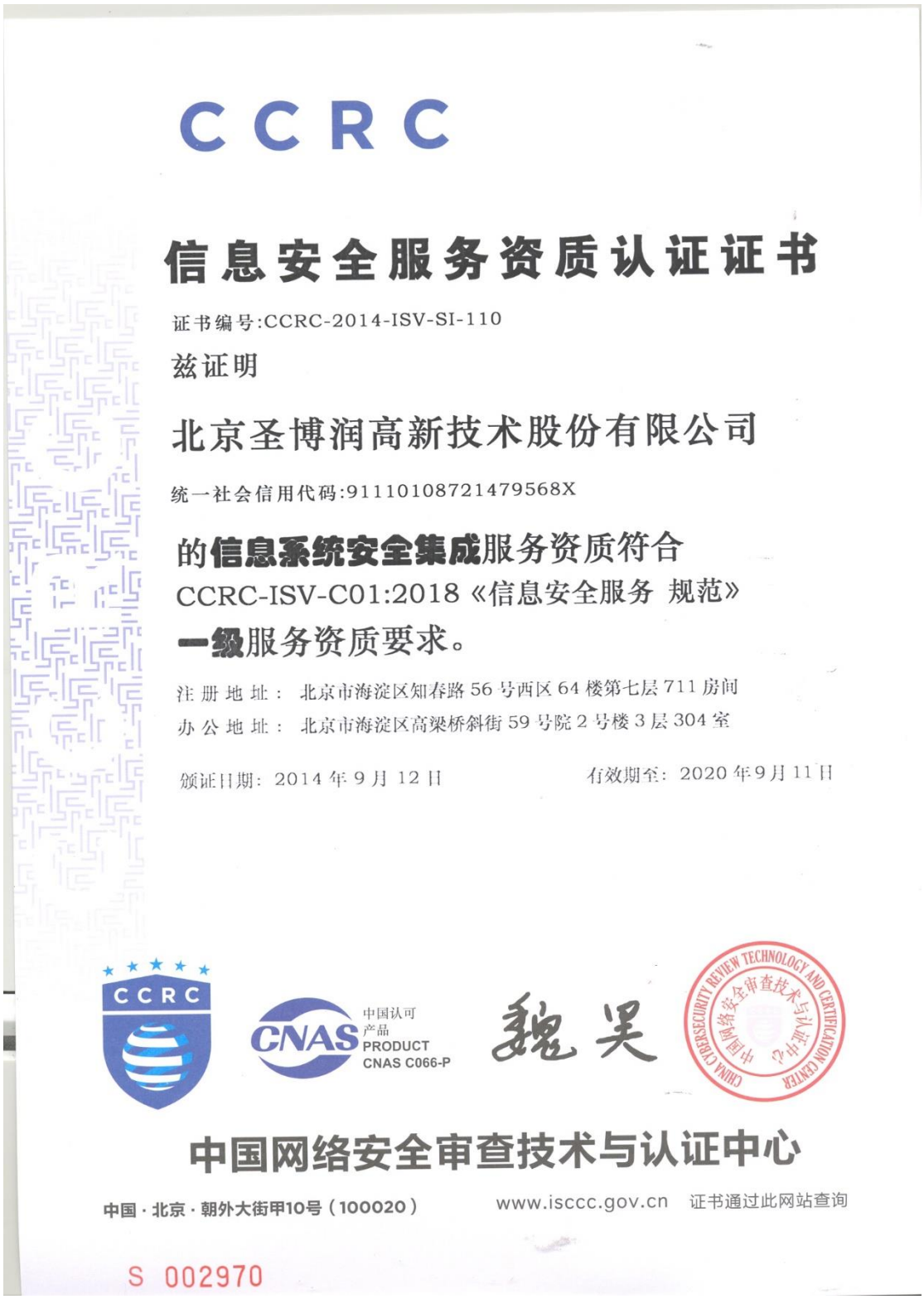
本证书签发日期：2018 年 4 月 2 日

有 效 期 至：2021 年 4 月 1 日

批准人：朱胜涛

中国信息安全测评中心

6.2 信息系统安全集成服务资质



CCRC

信息安全服务资质认证证书

证书编号:CCRC-2014-ISV-SI-110

兹证明

北京圣博润高新技术股份有限公司

统一社会信用代码:91110108721479568X

的**信息系统安全集成**服务资质符合

CCRC-ISV-C01:2018《信息安全服务 规范》

一级服务资质要求。

注册地址：北京市海淀区知春路 56 号西区 64 楼第七层 711 房间

办公地址：北京市海淀区高梁桥斜街 59 号院 2 号楼 3 层 304 室

颁证日期：2014 年 9 月 12 日　　有效期至：2020 年 9 月 11 日

CCRC

CNAS 中国认可 产品 PRODUCT CNAS C066-P

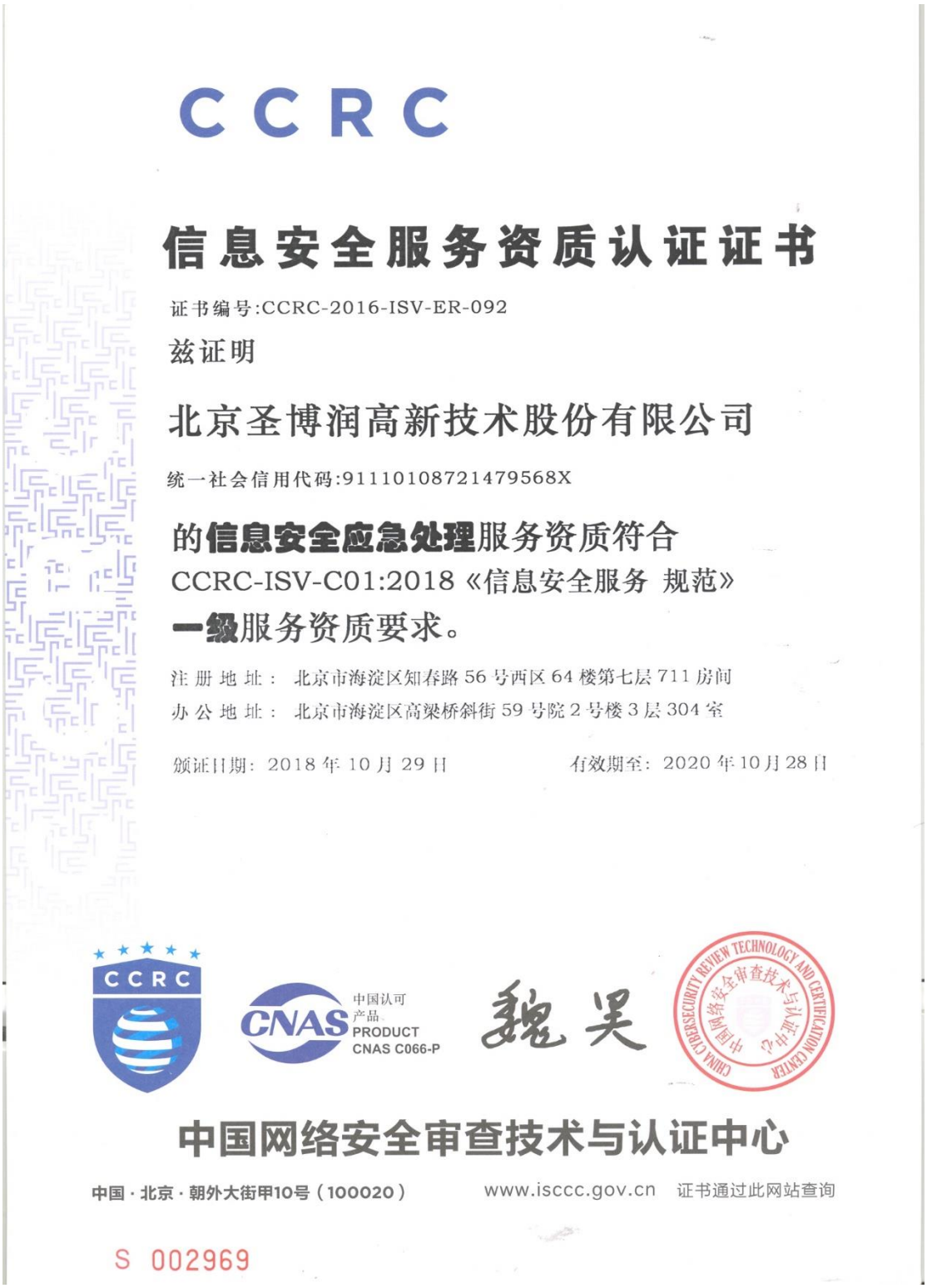
中国网络安全审查技术与认证中心

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

S 002970

6.3 信息安全应急处理服务资质证书



CCRC

信息安全服务资质认证证书

证书编号:CCRC-2016-ISV-ER-092

兹证明

北京圣博润高新技术股份有限公司

统一社会信用代码:91110108721479568X

的**信息安全应急处理**服务资质符合
CCRC-ISV-C01:2018《信息安全服务 规范》
一级服务资质要求。

注册地址：北京市海淀区知春路56号西区64楼第七层711房间
办公地址：北京市海淀区高梁桥斜街59号院2号楼3层304室

颁证日期：2018年10月29日　　有效期至：2020年10月28日

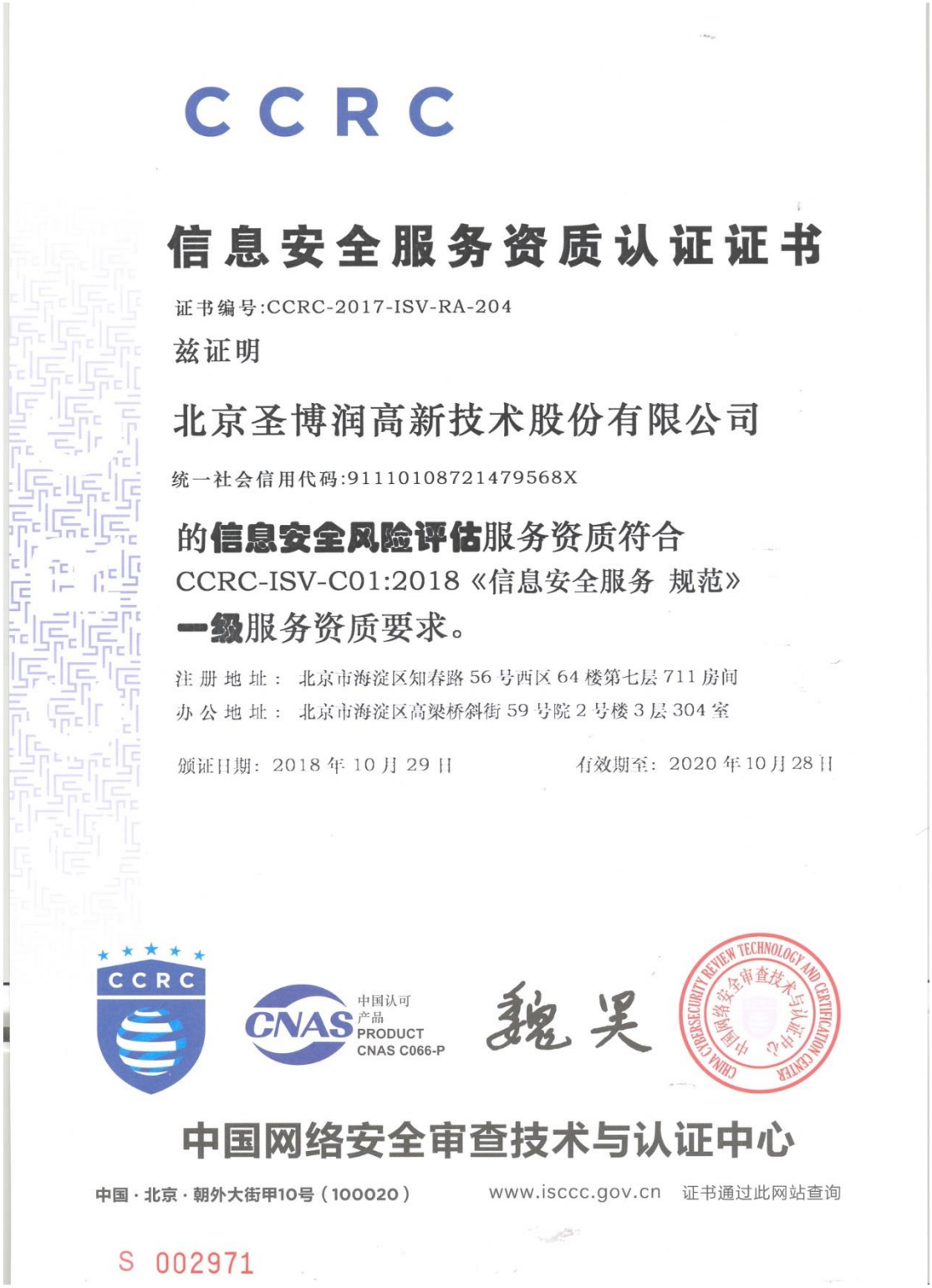
CCRC　CNAS 中国认可 产品 PRODUCT CNAS C066-P　魏吴　中国网络安全审查技术与认证中心

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

S 002969

6.4 信息安全风险评估资质



CCRC

信息安全服务资质认证证书

证书编号:CCRC-2017-ISV-RA-204

兹证明

北京圣博润高新技术股份有限公司

统一社会信用代码:91110108721479568X

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》
一级服务资质要求。

注册地址：北京市海淀区知春路56号西区64楼第七层711房间
办公地址：北京市海淀区高梁桥斜街59号院2号楼3层304室

颁证日期：2018年10月29日　　有效期至：2020年10月28日

CCRC　CNAS 中国认可 产品 PRODUCT CNAS C066-P　魏吴　中国网络安全审查技术与认证中心 CHINA CYBERSECURITY REVIEW TECHNOLOGY AND CERTIFICATION CENTER

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

S 002971

6.5 信息安全等级保护安全建设服务机构能力评估合格证书

6.6 ISO9000 证书

质量管理体系认证证书

注册号：016ZB18Q34671R4M
统一社会信用代码：91110108721479568X

兹 证 明

北京圣博润高新技术股份有限公司

质量管理体系符合
GB/T19001-2016/ISO9001:2015标准，适用于

系统集成、信息安全应用软件的设计、开发、实施及信息安全服务

注册地址：北京市海淀区知春路56号西区64楼第七层711房间
经营地址：北京市海淀区高梁桥斜街59号院2号楼3层304

初次发证日期：2006年12月26日
再认证日期：2018年11月01日
证书有效期至：2021年12月15日

新世纪检验认证股份有限公司
总裁：

BCC地址：北京市西城区国英园1号楼11层1101室
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
获证组织必须定期接受监督审核并经审核合格,此证书方继续有效。
证书有效性可通过网站：www.bcc.com.cn查询，也可二维码查询
本证书信息可在国家认监委网站www.cnca.gov.cn查询

中国认可
国际互认
管理体系
MANAGEMENT SYSTEM
CNAS C016-M

6.7 ISO27001 证书

管理体系认证证书

证书编号：01119IS20013R2M
OID 编号：1.2.156.1.2.01119IS20013R2M

兹 证 明

北京圣博润高新技术股份有限公司
（社会信用代码：91110108721479648X）
（北京市海淀区知春路 56 号西区 64 楼第七层 711 房间，100098）

信息安全管理体系符合标准：
GB/T 22080-2016/ISO/IEC27001:2013《信息技术 安全技术 信息安全管理体系 要求》

本 证 书 覆 盖 下 述 范 围：

位于北京市海淀区高梁桥斜街 59 号院 2 号楼三层 304 号
北京圣博润高新技术股份有限公司范围内的 LanSecS 内网安全管理系统
LanSecS（堡垒主机）内控管理平台、LanSecS 信息安全等级保护综合管理系统
LanSecS 网络安全管理工作平台、LanSecS 电子文件密级标志管理系统等产品的
研发、软件复制以及信息安全服务（安全工程、安全集成、应急处理、风险评估）
有关的信息安全管理活动。
信息安全适用性声明：V1.5.1

（本证书有效性依据发证机构的定期监督获得保持，证书有效性信息请登录 www.cc.cesi.cn 进行查询）
（本证书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 上查询）
注：认证注册范围不包括未获得有效的国家规定的相关行政许可，资质许可的产品服务范围

总 经 理

发证日期：2019 年 2 月 1 日

有效期至：2022 年 1 月 31 日

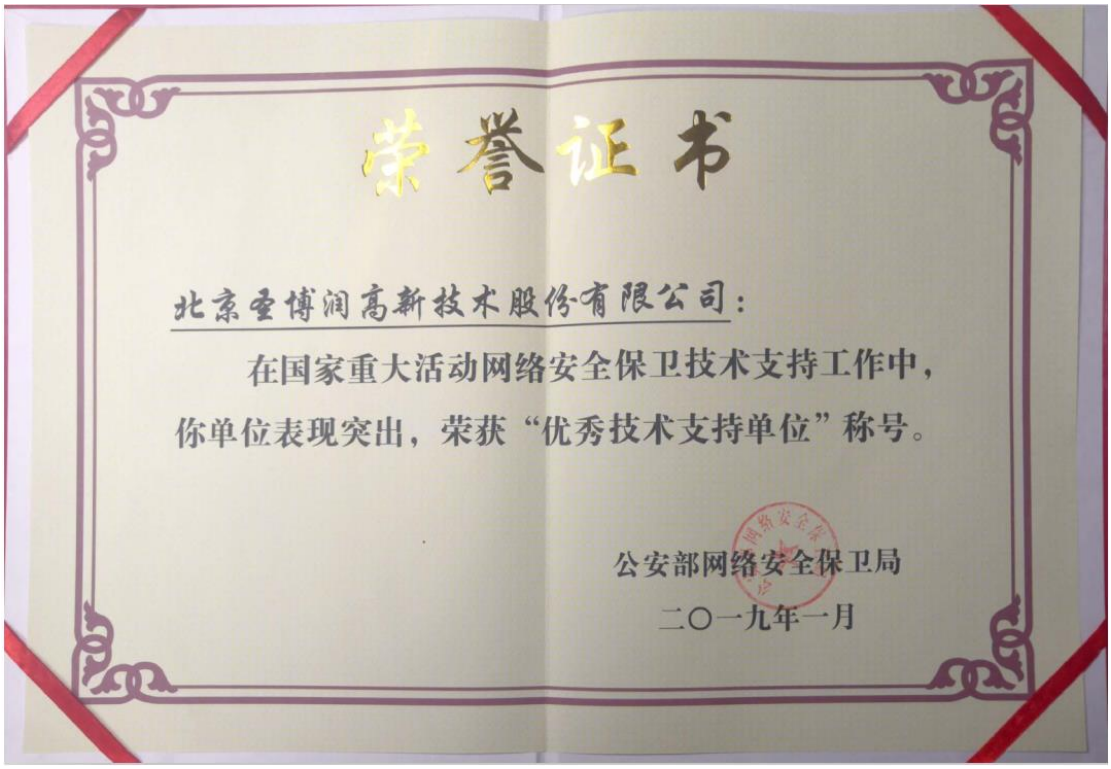
北京赛西认证有限责任公司

中国认可
国际互认
管理体系
MANAGEMENT SYSTEM
CNAS C011-M

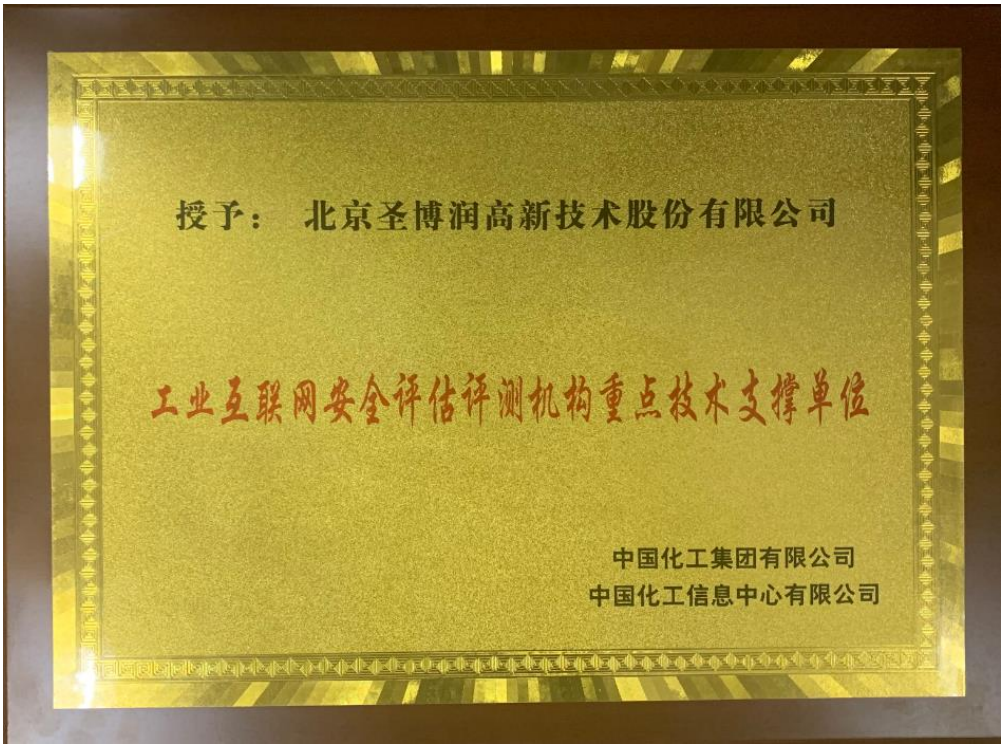
地址：北京市东城区安定门东大街 1 号　　客服电话：400-071-9000　　网址：www.cc.cesi.cn

6.8 “十九大”安保荣誉证书

6.9 国家重大活动网络安全保卫优秀技术支持单位



6.10 工业互联网安全评估测评机构重点技术支撑单位



6.11 国家信息安全漏洞库三级技术支撑单位

6.12 国家网络与信息安全信息通报中心的技术支持单位

6.13 G20 峰会网络安保技术支持单位

6.14 奥运政务网络和信息安全优秀服务企业