宁波图书馆信息系统安全服务采购要求

一、服务简介

1、服务对象

宁波图书馆信息系统及其相关主机、网络安全设备及应用。

2、服务时间

信息系统安全运维周期为合同签订后12个月。

二、服务内容

1、风险评估服务

1）信息资产调研

投标人须对IT资产进行充分调研，并进行分类识别，并建立资产配置库。

服务级别：全服务周期。

服务成果：《IT资产清单》、网络拓扑图、资产配置库等。

2）技术评估服务

投标人须提供一次技术评估服务，参照GB/T 20984-2007《信息安全技术 信息安全风险评估规范》国家标准，应用系统的总体运行情况进行综合评估分析。

服务级别：1次。

服务成果：《安全评估报告》。

3）渗透测试服务

投标人须模拟黑客的漏洞发现技术和攻击手段，每半年一次对目标系统的安全性作深入的探测，发现系统最脆弱的环节。

服务级别：1次/半年。

服务成果：《渗透测试报告》。

4）差距分析服务

投标人须提供一次差距分析服务，新馆系统正式上线前根据等级保护三级基本要求，从安全技术和安全管理两个方面分析系统现有的安全措施和安全要求之间的差距，根据差距提出整改建议。

服务级别：1次。

服务成果：《差距分析报告》。

2、安全运维服务

1）漏洞检测服务

* 网站漏洞检测

投标人须每月一次对互联网网站进行交叉检测，发现漏洞及时告知并协助修复，保证网站的运行安全。

* 主机漏洞检测

投标人须每季度一次对主机进行漏洞检测，并联合厂商、集成商、开发商、网络服务商等及时对漏洞进行修复。

服务级别：1次/季度。

服务成果：《网站漏洞扫描报告》、《主机漏洞检测报告》。

2）安全巡检服务

* 网站恶意代码检测

投标人须每季度一次，通过人工及检测工具，发现可疑网站木马文件、webshell等可疑代码或文件，通过分析进行确认、溯源，最后协助进行清理和加固。

服务级别：1次/季度。

* 设备安全巡检

投标人须每月一次对网络及安全设备运行状态、软件及库信息进行检查，发现问题并协助解决。

服务级别：1次/月。

服务成果：设备巡检记录。

* 安全隐患分析

投标人须每月一次对威胁监控、安全网关等安全设备的日志进行分析。发现信息系统存在的安全隐患，并及时处置。

服务级别：1次/月。

服务成果：日志分析记录。

3）安全监测服务

投标人须采用第三方专业网站监控平台，7\*24小时对互联网系统系统进行可用性、完整性和漏洞监控，出现异常及时告警。

4）优化加固服务

* 基线规范维护

投标人须协助甲方建立专属于甲方信息系统的基本安全技术要求及规范。根据信息安全标准，建立专属《Linux主机系统安全基线文档》和《windows主机系统安全基线文档》，采用配置加固、策略调整、补丁安装等方式，协助实施加固。

* 策略优化加固

投标人须对信息系统的安全防护策略进行针对性的调整，实现动态防护，提升信息系统的整体防护水平。

服务级别：1次/月。

服务成果：《策略变更记录》、《Linux主机系统安全基线文档》、《windows主机系统安全基线文档》。

5）APT远程值守

投标人须通过远程的方式提供针对威胁监控设备的日常值守服务，对网内存在的安全隐患做到及时发现。

3、应急保障服务

1）应急响应服务

投标人须根据不同的安全级别需求，提供相应的应急响应支持服务，提供5\*8小时的远程技术支持和7\*24小时的紧急现场救援，15分钟远程响应，必要时赶到客户现场。

2）节点保障服务

* 节假日、重大会议活动

投标人须强化重大节假日、国家及地方重大会议或活动期间的值班保障，建立7\*24小时双人值班制度，并落实在线值班监控。

服务级别：2次/年。

服务成果：《安全保障方案》、《安全保障总结报告》。

* 重大演练活动

投标人须在重大演练活动间安全保障，提供专项的安保障工作，对内外网进行风险检测、加固，对外网进行重保前的渗透，同时安排专人现场值守。

服务级别：10人天。

服务成果：值守记录。

3）应急预案咨询

投标人须提供一次应急预案咨询，根据信息系统的实际需求，结合当前系统的网络环境及政策法规要求，协助采购方制定或修订应急预案。

4）应急演练服务

投标人须提供一次应急演练服务，通过制定应急演练方案，并协助采购方对信息系统进行不同主题的应急模拟演练，并对演练中发现的问题进行总结并整改。

4、其他安全服务

1）安全培训服务

投标人须提供一次信息安全培训服务，包括信息安全形势、意识、技术或管理培训。

2）合规维护服务

投标人须深层次解读各种政策法规，帮助采购方做好风险管理与规避，包括监管部门历年的迎检准备工作，协助采购方顺利完成检查。

3）安全防护框架符合性咨询

投标人须提供一次安全防护框架符合性咨询服务，针对相关信息系统安全技术防护架构是否满足等保要求提供咨询服务。

4）管理制度及流程合规性咨询

投标人须提供一次管理制度及流程合规性咨询，协助建立符合等保要求的信息安全管理制度及流程。

5）风险跟踪管理

投标人须在运维期间内，对来自各类技术检测、评估、通报等来源的风险点进行跟踪管理，提出符合实际情况的修复建议，与修复责任人确认修复完成时间，并按时跟踪修复情况。

三、服务要求

服务人员需要严格按照采购人要求的相关安全服务规范开展工作，包括制定服务计划、编写方案、执行安全评估并提交相关报告、协助安全加固等，具体要求如下：

1、要求提供详细的安全服务技术方案，方案中应包含对服务对象的详细调研报告，包括网站及应用系统清单、主机操作系统情况、网络拓扑及安全设备情况等。项目实施方案中要体现各项服务内容实施方法、服务工具及人员配置、风险控制方案、项目进度安排、服务成果输出等。负责本项目的技术团队中要求具有2个及以上CISP证书中国网络安全审查技术与认证中心（CCRC）颁发的信息安全运维服务资质。

2、要求规范提供检测报告、事件报告及其他相关服务报告，方案中须明确各阶段交付的报告清单、报告模板。

3、本项目要求提供对服务工具的详细说明，服务工具要求如下：

（1）主机漏洞扫描器：必须提供两种以上主流品牌扫描器，用于主机漏洞交叉检测，要求不限制扫描地址；

（2）应用漏洞扫描器：必须提供两种以上主流品牌扫描器，用于应用漏洞交叉检测，要求不限制扫描地址；

（3）主机安全巡检工具：用户主机安全巡检，要求能够对windows和linux主机进行安全检查；

4、针对应急响应服务，要求提供详细的应急响应服务机制，包括事件定级、应急流程、事件升级和扩大应急流程等。

5、服务方及人员须对本次安全服务项目实施过程的数据和结果数据严格保密、未经授权，不得泄露给任何其他单位和个人，同时应在项目结束之后销毁所有和本项目相关的数据和文档。

6、合同签定后，因中标人服务响应不及时或服务内容、工具、人员不符合采购要求，经采购方提醒后仍拒不整改，采购方有权终止合同，且不支付任何款项。

7、因中标人原因造成信息安全责任事故产生重大损失或不良影响的，采购方有权随时终止合同，不支付任何合同款并保留追偿权。

8、本项目不允许分包或转包。

**投标人在投标前需进行现场查勘，以确保对服务对象、服务范围及工作量的准确评估。如未踏勘，不具备中标条件。**