**中国人寿保险（海外）股份有限公司**

**威胁与漏洞管理平台建设项目招标清单及技术指标**

**2023年10月**

**目 录**

[第一章 适用范围 5](#_Toc149258786)

[第二章 背景、目标及范围 5](#_Toc149258787)

[2.1 项目背景 5](#_Toc149258788)

[2.2 目标与范围 5](#_Toc149258789)

[2.2.1 总体目标 5](#_Toc149258790)

[2.2.2 项目范围 6](#_Toc149258791)

[2.3 技术需求明细 6](#_Toc149258792)

[2.3.1 基础功能 6](#_Toc149258793)

[2.3.2 场景功能 6](#_Toc149258794)

[2.4 非功能需求 9](#_Toc149258795)

[2.4.1 可用性要求 9](#_Toc149258796)

[2.4.2 安全性要求 9](#_Toc149258797)

[2.4.3 可维护性要求 10](#_Toc149258798)

[2.4.4 原厂综合实力要求 10](#_Toc149258799)

[第三章 项目实施说明 10](#_Toc149258800)

[3.1 现状调研与需求分析 10](#_Toc149258801)

[3.2 工具部署与调试 11](#_Toc149258802)

[3.3 定制化需求开发 11](#_Toc149258803)

[3.4 人员培训 11](#_Toc149258804)

[3.5 定期巡检和升级加固 12](#_Toc149258805)

[3.6 其他增值服务 12](#_Toc149258806)

[第四章 项目管理 13](#_Toc149258807)

[4.1 项目管理方法论 13](#_Toc149258808)

[4.2 项目实施组织 13](#_Toc149258809)

[4.3 项目人员要求 13](#_Toc149258810)

[4.4 项目实施计划 14](#_Toc149258811)

[4.5 项目质量管理 14](#_Toc149258812)

[第五章 供应商责任 14](#_Toc149258813)

[5.1 供应商组织要求 14](#_Toc149258814)

[5.2 供应商职责要求 15](#_Toc149258815)

[第六章 培训与知识转移 15](#_Toc149258816)

[6.1 培训要求 16](#_Toc149258817)

[6.2 培训预期效果 16](#_Toc149258818)

[第七章 项目交付与成果物 16](#_Toc149258819)

[7.1 项目成果交付 16](#_Toc149258820)

[7.2 售后服务 17](#_Toc149258821)

[第八章 验收 17](#_Toc149258822)

# 适用范围

本技术规范书明确中国人寿保险（海外）股份有限公司（以下简称：国寿海外）威胁与漏洞管理平台建设项目（以下简称：本项目）的基本需求，也是对供应商（以下简称：乙方）的基本要求。通过本文件规范供应商的服务方案设计、实施过程及成果验收交付。

本技术规范中所有内容和技术要求属于安全保密信息，所有参与相关商务投标的供应商不得扩散或者泄露任何相关内容。

# 背景、目标及范围

## 项目背景

为提升中国人寿保险（海外）股份有限公司（以下简称“国寿海外”）网络安全防护能力，加强漏洞管理，减少手工成本，实现漏洞全生命周期的可视、可控和可管，开展威胁与漏洞管理平台建设工作。

## 目标与范围

### 总体目标

根据行业监管、集团、海外公司漏洞管理要求，同时结合行业漏洞管理现状，本次引入威胁与漏洞管理平台，主要实现以下两个目标：一是提高漏洞检测、漏洞数据管理、漏洞运营多个环节的自动化程度，提高漏洞管理和运维工作效率；二是建立漏洞管理自动化流程，确保有效地跟踪资产的漏洞生命周期，及时感知漏洞态势，提高安全防护能力。

### 项目范围

结合国寿海外实际情况，本次项目建设范围主要包括但不限于如下：

1. 搭建一套针对资产安全视角，以漏洞优先级为核心，整合资产漏洞数据，提供漏洞全生命周期管理的威胁与漏洞管理平台。
2. 对接国寿海外已有的安全设备及运维平台，包括但不限于漏洞扫描器、SIEM、HIDS、CMDB、ITSM、OA、邮箱等系统，提高国寿海安全漏洞集中管理及运营处置能力。
3. 安全信息留存满足内地监管、集团要求的同时，达到香港、澳门等国寿海外业务涉及地区相关的监管审计要求。

## 技术需求明细

### 基础功能

注：标记为★的需求为必须满足项，标记为▲的需求为需截图证明项

|  |  |  |
| --- | --- | --- |
| 产品 | 数量 | 性能及参数 |
| 威胁与漏洞管理平台 | 1 | ★含五年维保及技术支持服务。 |

### 场景功能

|  |  |
| --- | --- |
| 漏洞管理 | 1. ★支持提供细颗粒度的漏洞信息检索页面，支持复合查询及筛选，筛选项可自定义添加或去除，同时支持保留历史搜索条件便于后期复用； 2. ▲漏洞列表排序支持自定义设置，提供默认的排序规则漏洞详情可查看漏洞描述、漏洞危害、影响范围、利用条件、CVSS评分、修复方案、参考资料等内容，同时支持浏览漏洞对应工单的流转动态； 3. ▲支持设置漏洞处置优先级，优先级高的工单可在工单列表置顶展示； 4. ★支持漏洞批量导入和筛选导出，导出格式包括word/pdf/Excel等； 5. ★支持通过自动和手动方式复测验证漏洞修复结果，可批量验证； 6. ★支持批量处置漏洞，包括批量催办、批量转单、批量生成工单、批量删除； 7. 支持通过手动、自动及根据策略条件生成漏洞工单，策略支持按照漏洞提交时间范围、漏洞等级、漏洞类型、漏洞名称、IP段、域名等参数进行设置； 8. ★支持漏洞聚合，可根据漏洞类型、漏洞主机IP、C段地址、漏洞等级、漏洞模板等方式进行聚合； 9. ★漏洞处置完毕后，可将漏洞详情信息，包括漏洞危害、漏洞修复方案等信息同步到知识库，完善企业漏洞修复知识库构建； 10. 支持对不同渠道的重复漏洞进行合并，也可手动解除重复。多源数据可根据URL、IP、CVE ID、漏洞标题、漏洞类型等参数进行排重，并可设置高置信度数据源的信息优先展示，来自其他数据源的重复漏洞折叠展示。 |
| 工单管理 | 1. ★支持区分待处理的工单、由我发起的工单、我经办的工单等，支持批量催办，批量处置工单； 2. ▲工单详情可查阅工单各个节点的流转过程、审批人信息、流转意见及工单流转流程图等； 3. ▲支持工单流程自定义：支持创建流程开始、结束、流程分支、操作、审核、延期处置、同意、驳回等操作； 4. 支持一键重置工单，返回初始状态和强制关闭工单等。 |
| 用户管理 | 1. ★支持创建、编辑、查询账号信息，以及账号绑定角色，账号导入导出； 2. ★支持手动构建组织架构，查看各层级组织下的人员、资产数据信息； 3. 用户认证支持接入统一身份认证管理，组织架构支持从统一身份认证同步； 4. ▲系统默认设置系统管理员、安全人员、资产负责人、研发人员等角色，角色权限包括操作权限和数据权限，操作权限可覆盖菜单和按钮级别。 |
| 日志审计 | 1. ▲支持根据账号、操作时间、IP等查询系统日志，支持日志导出； 2. ▲日志存储满足等保、行业法律法规及审计要求，支持对接至SIEM平台。 |
| 资产管理 | 1. ▲提供细颗粒度的资产信息检索页面，支持复合查询及筛选，筛选项可自定义添加或去除，同时支持保留历史搜索条件便于后期复用； 2. ★资产列表排序支持自定义设置，提供默认的排序规则，支持更换排序内容，或设置多字段综合排序； 3. ▲支持手动添加和批量导入资产信息； 4. ▲资产详情支持查看漏洞趋势分析和漏洞分布情况，主机资产支持以端口和服务维度查看； 5. 支持针对归属分配错误和无归属的资产，触发ITSM工单反馈，通过审核后，完成资产归属的正确变更； 6. 支持对接资产测绘平台； 7. ★支持对接CMDB、HIDS等渠道获取资产数据，针对下线资产，自动关闭资产关联的漏洞工单。 |
| 任务管理 | 1. ▲支持对接第三方漏洞扫描器进行任务下发； 2. 支持任务暂停、续扫、手动停止、重扫、删除、一键验证等操作； 3. ▲支持任务查询，包括名称、ID、目标、类型、状态、执行方式、开始时间、结束时间等字段的查询； 4. ★支持选择单个或者多个任务，进行任务统计分析，统计多个任务整体的风险情况，存活目标数、端口数、漏洞数等； 5. ▲支持针对单个或批量IP进行单个或批量漏洞扫描任务下发，根据扫描结果自动判断漏洞是否修复； 6. 支持导出任务报告，报告可自定义导出信息。 |
| 漏洞统计 | 1. ▲漏洞概览支持查看漏洞总数、已修复、已关闭、已忽略、待处置、处置中、延期修复、误报的漏洞数据及对应的占比，漏洞状态分布、漏洞等级分布、漏洞修复率排名、漏洞处理时长排名、漏洞数量等级趋势、超时漏洞、漏洞来源占比等维度内容； 2. ▲统计信息支持以个人用户视角查看个人待办/已办事项，以及以管理者视角查看全局漏洞概况； 3. ★个人概览支持时间周期的漏洞统计（如今日、本周、本月、半年、全部等）处理漏洞数及占比，待办工单数、超时工单数、超时占比、平均处理时长等统计信息； 4. 支持按照服务、应用归并漏洞修复建议，对于相同服务类型的给出影响资产数、漏洞数、建议操作等； |
| 漏洞情报 | 1. ★情报列表支持提供细颗粒度检索，情报详情包括漏洞名称、漏洞描述、漏洞危害、漏洞类型、漏洞等级、漏洞评分、影响范围、修复方案、POC/EXP、关联资产等维度信息； 2. ★支持针对情报下发风险排查工单，一个排查工单可包含多条情报信息并下发给多个经办人； 3. ▲支持利用资产数据指纹信息，结合权威漏洞库，自动判断和筛选出该资产匹配的漏洞信息，进行预警。 |

## 非功能需求

### 可用性要求

要求系统应具备较强的负载能力、较高的事务处理能力以及良好的响应时间，在大用户量同时发送并发请求服务时不会造成阻塞。且系统从底层数据库到业务逻辑功能层都应经过严格测试，能在不同的硬件环境中长期平稳运行。

### 安全性要求

保证网络安全、系统安全和数据安全，整个系统要配置和构建可靠实用的安全策略和机制。根据不同的业务要求和应用处理方式，设置不同的安全措施和环节，既满足业务管理、业务授权以及流程管理中的业务安全性要求。有完善易查的日志功能，便于进行审计跟踪非法操作，保证用户不受非正当侵害。项目实施过程会接触到甲方的安全漏洞、资产以及相关数据，要求乙方保证系统安全和数据安全，满足甲方和相关监管部门对安全和风险管理的要求。

1.仅授权用户可访问系统；

2.系统所有接口过TLS，保证数据传输的安全性；

3.系统若存在个人信息等敏感数据内容落库，存储至本地的数据应进行存储加密（满足国密加密基本要求）。

### 可维护性要求

在系统设计之初应已考虑具备一定的可维护性，充分考虑系统人员维护及运行管理的可行性；同时针对本系统涉及用户多、业务繁杂的特点，实现从整体上易于维护，便于管理，保证系统的维护运行顺利可行。

### 原厂综合实力要求

为了展示原厂自身综合实力：需提供原厂注册资金证明，漏洞管理平台国内市场占有率排名报告及原厂产品获得的评价证明（如无可不提交）；

为了更好的证明公司综合实力以及满足一些公共标准原厂尽可能具备例如（ISO9001 质量管理体系认证、IS027001信息安全管理体系认证、信息安全服务资质、CMMI 能力成熟度模型（3 级及以上）、业务连续性管理体系等同类资质）；

投标人认为还有其他需要提供的原厂实力证明资料。

# 项目实施说明

本项目包含不同技术服务，分别为现状调研与需求分析、设备部署与调试、定制化开发、人员培训、定期巡检与升级加固、其他增值服务等阶段。乙方在各任务阶段所执行的主要工作任务和内容包括但不限于如下：

## 现状调研与需求分析

* 项目启动会议，建立项目计划；
* 调研甲方网络安全运营及漏洞管理现状；
* 根据现状调研结果，设计和优化部署方案；

## 工具部署与调试

* 乙方工程师到甲方现场完成工具安装部署；
* 按照甲方流程进行调试；
* 根据甲方威胁与漏洞管理现状加强漏洞管理，实现甲方安全漏洞的可视、可控和可管，减少漏洞管理手工成本；
* 保证系统功能运行不影响甲方业务正常开展；

## 定制化需求开发

* 根据甲方实际需求，对接已有的安全设备及运维平台，包括但不限于漏洞扫描器、SIEM、HIDS、CMDB、ITSM、OA、邮箱、统一身份认证等系统；
* 漏洞报表导出支持定制（如增加总结性文字和变量）；
* 资产负责人支持由CMDB提供且支持与组织架构进行关联变动；
* 漏洞工单支持对接ITSM，支持工单派发人员错误或在处置过程中需要撤回时等场景下的工单撤回，支持一键撤回至初始状态且保留撤回记录；
* 主机资产配置及展示支持定制（如端口、服务等信息）；
* 对接漏洞扫描器发现的漏洞支持实现漏洞复测；
* 漏洞知识库支持手动导入修复方案(标记数据来源)，供研发作为修复方案参考；
* 支持重保场景下漏洞修复时效及通知的控制；
* 根据甲方实际情况，完成规则、流程的预置及优化；
* 甲方需求提出后，须12个工作日内上线；

## 人员培训

* 对甲方工程师进行基本工具使用方法培训，保证甲方人员能够正常使用工具开展工作；
* 对甲方工程师进行高级工具使用方法培训，包括但不限于规则调优、检索语法等；
* 对甲方一线人员进行威胁与漏洞处置培训，保证甲方一线人员能够对产品追踪到的安全漏洞完成处置；
* 提供7\*24小时技术支持服务；
* 提供用户手册；

## 定期巡检和升级加固

* 维保期间，产品7\*24小时维保，解决部署后出现的问题；
* 维保期间，产品7\*24小时电话咨询服务；
* 维保期间，产品现场安装部署及升级加固服务；
* 维保期间，产品技术培训服务；
* 维保期间，产品季度巡检服务；
* 维保期间，提供处理各种突发事件的应急预案；
* 维保期间，对本产品相关联的其他系统升级、例行维护、变更等提供相应的配合支持服务；
* 根据甲方具体需求，对相关产品的变更进行支持（如有）；
* 服务工程师要求为专家级，固定人员，相关专业领域10年及以上工作经验，持有专业证书。
* 服务响应时间要求为15分钟之内，工程师到场（深圳现场）时间要求为1小时之内。
* 系统可用率要求为99.99%，故障解决率要求为99%。

## 其他增值服务

* 根据甲方具体需求，实施网络安全防护水平提升等增值服务。具体服务项包括且不限于以下。
* 1.安全保障：

1）安全加固及版本升级。

2）提供按照专题归纳的漏洞情报数据，囊括主流操作系统、中间件、应用程序等软硬件漏洞，提供支持按照时间线或行业（如保险）的漏洞情报。

3）安全漏洞运营机制优化建议。

* 2.运行保障：

1）环境搭建、系统迁移、重大变更等支持服务。

2）备份恢复策略制定及测试，每年至少1次备份策略更新及测试。

3）监测运行数据分析，问题发现及定位解决闭环追踪。

4）特殊时期现场巡检及保障服务。

* 3.能力提升：

1）技术交流与培训：每季度至少一次专业技术交流与培训。

# 项目管理

## 项目管理方法论

乙方须依据自身的项目管理方法论，结合国寿海外项目实际情况，提出合理优化的适应本项目的项目管理方法论，并在项目实施过程中,包括项目启动、执行与控制、收尾等阶段贯彻执行。

## 项目实施组织

为保证威胁与漏洞管理平台建设项目的顺利开展，乙方须根据甲方实际需求，派驻足够的人员到甲方现场或远程提供服务支持。如需到甲方现场进行项目实施，则在现场期间须遵守甲方的工作纪律和要求。同时，甲方根据项目实施需要，组织相关人员参加此项目，与乙方人员紧密结合成项目实施小组。

乙方应提出详细的实施组织建议。项目实施组织的具体形式、人员组成及分工由双方在项目启动阶段根据项目实施需要协商决定，并报甲方批准执行。在具体项目实施各阶段，可根据需要，提出项目实施组织或/和人员组成变更申请，经甲方批准执行。

## 项目人员要求

投标方必须在投标文件中列出参与项目的项目总监、项目经理、主要顾问、专家的资历、投入本项目的时间及在本项目承担的职责。

中标方投入的项目主要成员必须和投标文件中建议的人员一致，未经招标方同意，不允许更换（人员离职或健康原因等特殊情况除外）。

项目总监应为投标方公司高级管理人员，拥有丰富的行业实践经验与项目管理经验。

## 项目实施计划

本项目中，乙方需要按照国寿海外要求的时间点安排实施计划，按时完成项目相应内容。

## 项目质量管理

质量控制队伍应该独立于项目组，作为项目成功的重要因素和保障，在项目执行过程中始终与项目组保持密切联系。从另一个角度观察和监督项目的开展，帮助项目组发现和解决项目执行中的问题，确保项目的成功。

在组织结构上，将设置质量控制小组，专门负责项目实施的质量控制。质量控制小组由项目双方项目经理、业务人员及双方领导组成，乙方专门指定一位高级经理作为质量总监。

质量管理小组将定期或不定期的举行检查会议，进行项目各阶段提交件的评审，听取项目经理及项目其他人员的汇报，对项目的进展和质量进行监督和控制，提出有关建议和意见。

质量管理小组的每次会议的内容，结论和决定，都将形成文字备忘录，为项目文档保存，并作为以后工作的依据，随时对项目的进展和质量进行修正。

# 供应商责任

供应商须确认并承诺能够完成本技术规范中所要求的需求内容以及按要求组织项目团队，确认并承诺承担本技术规范书中所要求供应商承担的所有责任。

招标人在发放中标通知书之前，可视情况设置测试验证环节，投标人需在规定时间内提供测试设备进行功能验证。

## 供应商组织要求

为保障项目以及产品落地成功，同时为了确保乙方提供的技术服务响应的及时性、有效性，要求乙方具备网络安全服务能力，拥有金融行业5年相关安全技术服务案例；要求乙方具备本地团队，提供本次项目团队主要成员简历；需提供乙方团队成员最近半年的社保缴纳证明。

## 供应商职责要求

供应商须对项目的全部内容进行应答，按照本技术规范要求提交全部资料，并对本技术规范各方面做出实质性响应。

1. 对本项目范围、内容、所承担的任务的理解与确认；
2. 本项目管理方案建议包括但不限于：

* 设计项目组织结构，明确双方职责和主要任务；
* 详细工作进度计划/策略，包括对工时、人力、费用等资源需求的预期；
* 拟提交成果清单及说明；
* 培训方案；
* 项目人员简历及资质证明；
* 项目实施经验；
* 项目实施组织、工作职责；
* 项目验收标准。

1. 项目实施阶段职责包括但不限于：

* 提供现状调研与需求分析、设备部署与调试、定制化开发、人员培训、定期巡检与升级加固、其他增值服务；
* 编制项目实施过程中的相关材料、会议纪要等；
* 项目实施完成总结。

# 培训与知识转移

在项目中，为确保项目的可持续性发展，保证从设计阶段到实施阶段和上线维护的平滑过渡，以及降低不同阶段过渡过程的不确定性和可能的执行偏差，通过多种方式提供项目技术培训。

知识转移是将专家的特定能力转移到项目组的客户成员，并最终转移到客户整个组织。根据本次项目总体内容和时间进度要求，乙方安排有关项目方法、项目成果等方面的培训,相关知识培训内容包括：

## 培训要求

1）在项目启动时，向项目组进行产品使用培训；

2）在项目实施过程中，通过技术培训、人员访谈、数据收集、分析整理、研讨会等形式向项目组进行知识转移；

3）在项目维保周期结束之前，根据甲方具体需求，向甲方技术人员进行安全技能培训；

4）应提供中文培训资料、讲义、模板等资料。

## 培训预期效果

1）甲方人员安全业务能力提升，对新型网络安全漏洞以及攻击手段能有一定的敏锐度，了解安全漏洞处置的技术流程。

2）甲方人员熟悉威胁与漏洞管理平台工具的使用，能够在乙方离场后独立使用设备实现相关功能。

3）甲方一线人员能够熟悉漏洞运营机制，懂得对应的漏洞处置方式，能够对平台上的安全漏洞完成闭环处置；

# 项目交付与成果物

## 项目成果交付

为了确保项目实施的成功，在项目中的各级交付文件非常重要，乙方需要按照双方约定的格式提交项目相关文档。

为确保项目按照项目预期的计划执行，在项目实施过程中，一些重要文件需要国寿海外项目经理或相关人员进行审批和确认。

在项目各阶段交付物内容与要求（包含但不限于以下内容）：

★系统交付

* 系统交付包括项目范围内所有系统、工具和模型，以及在测试中因需求变更而新增或修改的功能。

★文档交付

* 项目实施计划
* 项目实施方案
* 项目调研提纲及调研结果
* 产品部署方案
* 产品维保方案平台定制化需求开发记录
* 产品巡检记录
* 产品升级加固记录
* 产品变更记录（如有）
* 产品许可更新记录（如有）
* 产品更换记录（如有）
* 产品用户操作手册
* 培训计划及资料、讲义、模板
* 其他增值服务记录（如有）
* 项目总结报告
* 工作遗留项及关注事项

## 售后服务

乙方在项目验收后6个月内依据实际情况提供不少于5次的电话指导、邮件指导或远程支持，每次支持时间在半天以内。

在服务结束后一年内，将至少回访国寿海外2次，对国寿海外威胁与漏洞管理平台以及漏洞运营现状做了解和访谈，并提出针对性建议。

# 验收

本项目的验收标准为：

* 乙方完成威胁与漏洞管理平台的建设工作，完成场景功能以及定制化需求开发的实施，确保所建设的平台满足非功能要求，平台平稳运行，完成项目成果交付以及知识移交。
* 达到服务期限约定时间。

符合项目验收标准后，乙方须提前十四天用书面方式向国寿海外提出验收申请，由国寿海外组织项目验收小组对项目成果物进行验收，如验收通过，则由国寿海外出具最终验收证书。

上述各验收阶段均与付款直接相关，具体条款经甲乙双方商定后，体现在具体合同文本中。