**中国人寿保险（海外）股份有限公司**

**2023-2025常规网络安全技术服务框架采购项目招标清单及技术指标**

**2023年3月**

**目 录**

[第一章 适用范围 4](#_Toc18268)

[第二章 背景、目标及范围 4](#_Toc26571)

[2.1 项目背景 4](#_Toc27721)

[2.2 目标与范围 4](#_Toc7840)

[2.2.1 总体目标 4](#_Toc13465)

[2.2.2 范围与需求 4](#_Toc26210)

[2.2.3 非功能需求 5](#_Toc17883)

[第三章 项目实施说明 6](#_Toc6430)

[3.1 重要时期保障驻场服务 6](#_Toc6591)

[3.2 渗透测试服务 6](#_Toc31312)

[3.3 应急响应服务 7](#_Toc31788)

[3.4 风险评估服务 7](#_Toc27421)

[3.5 网站监控服务 7](#_Toc25385)

[3.6 应急演练服务 7](#_Toc1307)

[3.7 漏洞预警服务 7](#_Toc14071)

[3.8 安全培训服务 8](#_Toc30844)

[第四章 项目管理 8](#_Toc5133)

[4.1 项目管理方法论 8](#_Toc12459)

[4.2 项目实施组织 8](#_Toc7632)

[4.3 项目人员要求 8](#_Toc6797)

[4.4 项目实施计划 8](#_Toc28742)

[4.5 项目质量管理 9](#_Toc514)

[第五章 供应商责任 9](#_Toc28682)

[5.1 供应商组织要求 9](#_Toc26729)

[5.2 供应商职责要求 9](#_Toc29526)

[第六章 培训与知识转移 10](#_Toc1063)

[6.1 培训要求 10](#_Toc21464)

[第七章 项目交付与成果物 11](#_Toc22918)

[7.1 项目成果交付 11](#_Toc14507)

[7.2 售后服务 11](#_Toc8035)

[第八章 验收 12](#_Toc8370)

# 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）2023-2025常规网络安全技术服务框架采购项目（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”）网络安全防御能力，更好地配合集团检查、满足监管要求以及确保网络安全重要保障等重点工作正常开展，在保证现有标准服务的基础之上，尽可能提高供应商的综合服务水平和国寿海外网络安全防护水平。

## 目标与范围

### 总体目标

通过本项目采购，完成国寿海外常规网络安全技术服务保障工作，安全服务保障期限不超过三年。

### 范围与需求

针对下表列出的网络安全技术服务，服务期限不超过三年。

|  |  |
| --- | --- |
| 产品 | 需求数量 |
| 重要时期保障驻场服务 | 每年180人天 |
| 渗透测试服务 | 每年65个 |
| 应急响应服务 | 每年5次 |
| 风险评估服务 | 每年10个系统 |
| 网站监控服务 | 每年20个网站 |
| 应急演练服务 | 每年3次 |
| 漏洞预警服务 | 不限 |
| 安全培训服务 | 面向技术人员、全员各3次 |

### 非功能需求

国产化要求

为响应国产化的建设方针及目标，要求乙方在实施过程，如需引入工具提升工作效率，需符合中国国情及海外当地法律法规和企业运作的实际情况。

安全性要求

项目实施过程会接触到甲方的网络安全监测评估系统以及相关数据，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。

时效性要求

项目实施过程会遇到突发安全事件，要求乙方能够及时响应，验证并评估风险和影响范围，按照甲方实际需求进驻甲方深圳、香港现场或提供远程服务支持进行应急处置，使安全风险可知、可管、可控，尽可能减小不良影响和损失。

专业性要求

为保证服务质量，保障国寿海外网络安全防御底线，对服务团队专业素养提出较高要求，每项服务均要求有专业资质、专业技能过硬的成员参与，人员资质要求内容按合同约定执行。

# 项目实施说明

本项目包含不同技术服务，分别为重要时期保障驻场服务、渗透测试服务、应急响应服务、风险评估服务、网站监控服务、应急演练服务、漏洞管理服务、安全培训服务等任务。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：

## 重要时期保障驻场服务

* 调研甲方重要时期联防联控需求；
* 调研甲方网络安全防御设备以及系统架构现状；
* 根据现状调研结果，设计和优化安全值守方案；
* 重要保障时期7\*24小时于甲方现场完成安全值守任务；
* 重要保障后进行总结；
* 服务工程师要求为有至少一名专家级，固定人员，相关专业领域5年及以上工作经验，持有专业证书；
* 重要时期保障驻场服务至少每年180人天，服务期限不超过三年。

## 渗透测试服务

* 调研甲方渗透测试需求；
* 对甲方互联网网站以及应用系统（包括手机APP、微信公众号、小程序等）进行渗透测试；
* 输出渗透测试报告；
* 渗透测试服务能够覆盖至少每年65个网站或系统应用，服务期限不超过三年。

## 应急响应服务

* 重要时期突发事件应急处置；
* 日常常态化监控安全事件应急处置；
* 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；根据甲方实际需求，如需工程师到香港现场，原则上时间要求在2小时以内。
* 服务工程师要求为有至少一名专家级，固定人员，相关专业领域5年及以上工作经验，持有专业证书；
* 应急响应服务共计15次，服务期限不超过三年。

## 风险评估服务

* 根据甲方具体需求开展风险评估工作，包括但不限于以下情况：

1.集团自查自检要求；

2.新系统上线前检查；

3.审计要求；

4.分支机构需求。

* 服务工程师要求为有至少一名专家级，固定人员，相关专业领域5年及以上工作经验，持有专业证书；
* 服务能够覆盖至少每年10个系统，期限不超过三年。

## 网站监控服务

* 对官网及指定的网站进行“7\*24”的页面资源与指纹信息的分析，通过监测技术对各类安全事件进行全面分析感知，包括篡改、暗链、黑页、挂马、后门等；
* 结合威胁情报，对接入网站安全监测的网站域名和服务器IP进行碰撞，发现挖矿、僵尸网络等失陷主机，弥补远程透明监测短板问题；
* 发现问题第一时间向相关部门和人员进行安全通报；
* 如发现中高危安全漏洞或网站被DDoS攻击、被篡改等重大安全事件，安全专家团队第一时间应急响应，对事件进行验证并评估风险和影响范围，协助进行应急处置，使安全风险可知、可管、可控，减小不良影响和损失。
* 服务能够覆盖至少每年20个网站，期限不超过三年。

## 应急演练服务

* 调研甲方信息科技风险应急演练工作要求以及信息化建设现状；
* 根据调研结果选取适合的场景开展应急演练工作；
* 进行应急演练方案设计；
* 应急演练实施；
* 应急演练结束后进行工作总结；
* 服务工程师要求为有至少一名专家级，固定人员，相关专业领域5年及以上工作经验，持有专业证书；
* 应急演练服务至少每年3次，不超过三年。

## 漏洞预警服务

* 通过多种方式（电话、邮件、短信等）及时对互联网爆发的新型漏洞进行预警；
* 对重大安全事件进行通告；
* 提供最新外部安全环境和最新的漏洞信息，以及时规避新安全漏洞带来的风险。
* 本项服务要求作为增值服务，不参与报价

## 安全培训服务

* 面向技术人员的专业技能培训，培训讲师要求具有专业资质，有5年及以上相关领域工作经验；
* 面向全员的安全意识培训；
* 巩固安全意识培训成果，在安全意识培训后基于培训内容开展测验；
* 三年内，提供面向专业人员和全体员工的培训各3次。
* 本项服务要求作为增值服务，不参与报价

# 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

为保证网络安全技术服务的顺利开展，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。

## 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；
* 项目人员简历及资质证明；
* 详细工作进度计划/策略；
* 成果清单及说明；
* 项目验收标准。

1. 项目实施阶段职责包括但不限于：

* 提供重要时期保障驻场、渗透测试、应急响应、风险评估、网站监控、应急演练、漏洞预警、安全培训等服务；
* 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）基于面向全员的安全意识培训内容，给出安全意识测验方案以及试题内容，在培训结束后检验培训成果（如钓鱼邮件测试等）；

5）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，了解安全事件处理的技术流程。

2）甲方整体安全意识加强，具有一定的攻击（包括但不限于社工、钓鱼邮件等）鉴别与防范意识。

# 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）：

* 项目实施计划
* 项目实施方案
* 项目调研提纲及调研结果
* 重要时期保障驻场调研报告
* 重要时期保障驻场实施方案
* 重要时期保障驻场工作总结
* 渗透测试报告
* 应急响应措施以及优化意见
* 风险评估报告
* 安全事件验证报告（如有）
* 安全事件评估（如有）
* 应急演练方案
* 应急演练总结
* 重大安全事件通报
* 培训计划及资料、讲义、模板
* 安全意识测验方案以及试题内容
* 项目总结报告
* 工作遗留项及关注事项

## 售后服务

在每项服务结束后一周内，基于当前服务事项对国寿海外网络安全防御架构现状做整体总结，复盘本次服务实施过程中遇到的问题以及解决方案，并提出相应的建议。

# 验收

* 本项目的验收标准为：按照甲方实际需求完成所有项目成果交付以及达到服务期限约定时间。
* 各项服务完成标准为：服务结束以及产出内容提交并达到甲方要求。

每项服务达到服务完成标准后，甲方针对当次服务从不同维度进行评分，计算服务考核得分。

在所有服务项均完成且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。