珠海机场网络信息安全服务项目

采购需求

珠海市珠港机场管理有限公司

2023 年 3 月

目录

1. 项目概述

1.1. 项目背景

随着信息技术的发展,特别是云计算、大数据、物联网等新技术的出现，使得网络信息安全形势更加严峻。根据《网络安全法》第三十二条及第三十三条中明确要求负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作，建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

近年来，珠海机场网络信息安全管理通过持续发展，并根据国家、民航局的网络信息安全相关的要求，确保了珠海机场在网络安全防护、安全值守保障、网络安全制度等工作的落实执行，特别在各项重大活动民航网络安全保障了本场网络及信息系统运行安全稳定。但目前珠海机场在网络信息安全管理仍在发展阶段，相应网络信息安全体系建设仍需持续完善，并通过梳理优化各个安全节点流程及技术管控手段,以应对外部以及内部的网络信息安全风险。

为了更好和持续支撑珠海机场的公司信息化发展战略、完善网络信息安全管理，提高公司网络信息安全保障能力，以满足等级保护、网络安全法、数据安全法以及民用航空网络与信息安全管理规范等法律法规等相关合规的要求，因此需要延续网络信息安全服务项目，系统性、全面性地开展网络信息安全管理工作。

1.2. 项目目标

通过实施信息安全管理体系(ISMS)建设项目，全面、准确地了解珠海机场的信息安全现状，对公司目前所拥有的信息资产进行梳理，分析存在的信息安全风险，根据监管部门要求，结合行业、国内和国际的最佳实践经验，规划珠海机场信息安全建设发展的蓝图，按照《网络安全法》、等级保护标准和民用航空网络与信息安全管理规范的要求编写有关安全策略和体系文件，推动珠海机场 ISMS 体系的建设，切实从管理、技术、运维、开发及合规等方面提高珠海机场的信息安全水平,以保护企业的业务持续运行,满足法律法规和监管部门要求。

具体项目目标如下：

1）全面、准确地了解珠海机场的信息安全现状，对标明确差距，对公司目前所拥有的

信息资产、体系文件、安全策略、安全运维管理等进行梳理，分析存在的信息安全风险。

2) 规划珠海机场信息安全建设发展的蓝图，建立符合珠海机场管理模式的信息安全管理体系（ISMS）框架。

3）按照《网络安全法》、《数据安全法》、等级保护标准、民用航空网络与信息安全管理规范和监管合规要求制定安全策略、体系文件及管理流程，初步建成珠海机场信息安全管理体系，为后续该体系全面落实打下良好基础。

4）年度安全服务，持续发掘企业信息系统存在的安全漏洞，并推动整改。根据最新的合规性要求优化管理文档，规范技术、运维、开发等流程，提高企业信息安全防护能力。

1.3. 项目内容

乙方须按照本项目采购需求提供24个月的网络信息安全服务及平台，从合同签订之日起计算，服务内容包括但不限于以下要求：

1) 提供信息安全体系落地服务，全面、准确地了解珠海机场的信息安全现状，从管理、技术对珠海机场现存的信息安全问题和需求进行调研和梳理,按照信息安全规划的实施计划，按甲方要求建立完善珠海机场网络信息安全制度，并按照制度落实的信息安全控制措施，分批次逐步落实；

2) 提供安全服务团队为珠海机场提供驻场服务和安全服务等。乙方需定期对生产环境中的重要系统进行安全技术评估，包括安全扫描、渗透测试、人工检查和架构评估，发现存在的技术威胁或漏洞，提出改进建议并完成整改工作，促进珠海机场信息安全体系持续改进和完善。

3) 提供网络信息安全运维服务，对珠海机场全网信息系统、终端、应用和数据库等设备和行为建立长效安全监测机制，同时对珠海机场网络与信息安全类系统、平台等设施设备开展运维及保养工作。

4) 按要求完成珠海机场信息安全专项工作，包括但不限于完成法定自查、民航专项检查、等级保护、攻防演练和网络安全竞赛等专项工作。特别在重大活动保障期间，配合完成重大活动保障前隐患排查工作，并提供信息安全技术人员现场全天候驻守，提供服务详细报告，确保珠海机场网络信息安全专项工作保质保量完成。

5) 提供网络安全态势感知服务，以实现全公司网络系统的自动化集中安全管理、安全监测

和通报预警。监测手段不限信息系统监测预警、布点监测、重要系统日志集中分析和存储、流量检测、资产普查等方式。

6) 提供信息安全通告及培训宣传教育服务，对于安全攻击手段和系统安全漏洞的不断发现和利用，乙方应每周向珠海机场提供实时安全动态和安全提示并根据甲方需求，提供网络信息安全培训服务，同时按甲方要求配合开展网络信息安全相关宣传及活动。

7) 提供网络信息安全咨询及规划服务，向珠海机场持续提供信息安全专家服务，规划珠海机场信息安全建设发展的蓝图，包括但不限于网络安全建设、数据安全建设、等级保护建设、蓝队体系建设、混合云安全规划等，制定以上建设规划方针，建立年度安全服务工作计划，经甲方确认的规划方案，并按计划落实相关服务工作。

2. 服务需求

2.1. 安全体系建设服务

乙方要按照信息安全规划的实施计划，将需要落实的信息安全控制措施，分批次逐步落实。

根据珠海机场现有的信息安全管理体系文件，乙方的信息安全团队应在体系运行实施期间，通过实施体系文件，充分发挥体系本身的各项功能，及时发现体系策划和信息安全控制本身存在的问题，找出问题根源，采取纠正措施，纠正各种不符合，并按照更改控制程序要求对体系予以更改，以达到进一步完善信息安全管理体系的目的。

根据运行分阶段的原则，计划主要完成如下领域的落实工作（以下仅为示例，具体领域和内容在项目再确定）：

域	重点落实的安全措施（示例）
信息安全组织架构	成立运行组织，确定人员、落实各团队的安全管理员，制定、完善网络安全管理规章制度，内容应涵盖人员、资产、采购、外包、系统建设与运维、备份、应急等方面，须符合民航网络信息安全法定自查的要求。
人员安全管理	1、定期修订网络安全与保密协议，明确网络安全与保密要求和责任。 2、制定人员离岗离职网络安全管理规定，人员离岗离职时应终止信息系统访问权限，收回各种软硬件设备及身份证件、门禁卡等。

	3、制定网络安全教育计划，每年开展面向全体人员的网络安全教育。
信息资产管理	1、建立信息资产管理制度，编制资产清单，明确资产管理责任部门，明确每项资产的管理责任人及其职责。信息资产应当包括信息系统相关的硬件资产、软件资产、数据资产、人员资产及第三方服务资产。 2、定期对照资产清单对信息资产进行一致性检查，保证账物相符，保留检查记录。 3、对计算机及相关设备维修、报废销毁情况进行登记。
信息技术外包服务安全管理	1、对系统开发、运维、安全建设、定级测评、灾难备份等方面的外包服务建立安全管理制度。 2、审核外包服务公司资质，确保符合合同及国家相关资质要求。 3、落实外包服务信息安全管控和保密条款，安全责任明晰。 4、当外包服务采取远程服务，需对远程在线服务记录，并采取书面审批、访问控制、在线监测、日志审计等管控措施。
物理和环境安全	机房来访登记、线缆梳理推动、机房风火水电等改进项整改推动。
网络防护	1、网络分区分域管理落实推动，确保生产网与互联网、办公网安全隔离，根据承载业务的重要性对网络进行分区分域管理。 2、对网络边界访问控制（如防火墙）、入侵检测、安全审计以及非法外联检测、病毒防护等的安全设备，定期进行防病毒策略优化、安全策略优化。 3、对旅客的互联网接入，采取身份认证、上网行为审计等安全技术措施，同时保证公共网络区域与民航内部网络安全隔离。 4、对网络设备登录制定口令策略，规定口令强度和更新频率，并对更新予以记录；对网络设备管理员登录地址进行限制；对网络设备进行远程管理时，采取有效的身份鉴别信息保密措施。
网络安全等级保护和风险评估	1、按照国家要求开展信息系统定级工作并按要求备案。定级备案结果同时报送所在地民航行政管理机构。 2、根据安全保护等级对信息系统进行相应的安全建设，提供安全

	方案，安全方案描述的安全措施与安全等级的要求相一致。 3、定期开展信息系统等级测评和风险评估。
网站与显示大屏防护	1、建立并完善网站信息发布审核制度。 2、落实公共区域显示大屏的网络安全管理责任，采取有效的安全防护措施，确保大屏显示内容安全。
互联网电子邮件系统防护	1、规范电子邮箱的注册和变更管理，原则上只限于本单位工作人员注册使用，注销“僵尸”账户。 2、使用技术措施控制和管理单位邮箱口令，口令强度符合要求并定期更新。
终端防护	1、采取有效管理措施，对计算机终端进行集中统一管理。 2、对终端账户口令强度有统一要求，并强制定期更新。 3、严格管理接入互联网的终端，采取有效的接入认证和追踪溯源措施。
移动存储设备管理	对移动存储设备采取集中安全管理措施，制定移动存储设备的分发、注册、使用、存放、送修、报废等管理制度。
访问控制	系统访问权限管理、重要系统帐户和权限清理、日志审计。
业务连续性管理	业务影响分析(BIA)、业务连续性计划和灾难恢复计划(BCP/DRP)制订和演练。
系统运维管理	1、对信息系统上线前进行安全评估，上线后定期进行漏洞扫描、病毒木马检测。 2、信息系统运维管理体系完善度，如制度、实施记录和巡检过程的记录。 3、确保信息系统均安装防恶意代码软件，定期更新恶意代码库。 4、对网络设备、操作系统和数据库系统的补丁程序经过测试后，及时安装，更新系统。 5、定期进行系统运行日志、监控记录和报警信息等分析处理工作。
应急管理	1、建立网络安全信息通报制度,明确需要通报的内容和范围，落实负责人员。

	2、按照民航网络安全事件应急预案，制定网络安全及专项应急预案。 3、组织相关人员针对演练方案进行培训；制定演练计划，定期开展应急演练，根据应急演练情况完善网络安全信息通报制度及络安全事件应急预案。
数据安全	通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

乙方应具备信息安全制度体系建设及规划能力，根据民航局、公安机关和公司等上级单位关于网络信息安全相关的法律法规及政策要求,结合珠海机场信息化建设及运营的真实情况和具体需求，完成相关规章制度制定及工作落实，内容应涵盖人员、资产、采购、外包、系统建设与运维、备份、应急等方面，确保满足相关法律法规及政策要求。

2.2. 服务团队工作标准

2.2.1. 服务团队

为甲方提供一个不少于 4 人的信息安全服务团队(含 1 名项目经理和 1 名驻场服务工程师)；

- 项目经理要求 8 年或以上信息安全服务项目经验，具备 PMP 和 CISSP。以协助珠海机场信息安全管理体系持续优化和改进;
- 其他服务团队成员（含驻场服务工程师）要求 3 年以上信息安全相关经验，具备 CISA、CISP 任一证书；。

2.2.2. 服务工作标准

乙方对珠海机场的信息系统、终端设备和安全设备等信息设备的漏洞和风险进行安全加固，同时需要对存在漏洞的信息系统、终端设备和安全设备等信息设备重新进行全面安全风险评估。

乙方对珠海机场信息安全管理体系制度文档存在的问题及时采取纠正措施,纠正各种不符合，并按照更改控制程序要求对体系予以更改，以达到合规及甲方要求。

不发生因乙方责任原因的重大信息安全事件，包括但不限于如因乙方补丁更新、安全加

固等工作时疏忽导致入侵、信息资料泄露等安全事件发生。

建立服务团队。专人负责，建立期房信息安全工作的档案及工作记录，并按月提供信息安全工作、人员计划、工作计划等报告（含日常工作、计划实施情况、信息安全态势分析、重大事件活动记录、整改措施）。

项目实施过程中，如出现技术障碍、系统运行故障等问题，供应商有义务和责任组织、协调相关各方尽快对问题进行解决。

本项目中因应履行服务工作所需具备的系统、设备、工具等由乙方自行配备，并在服务内容中包含提供甲方使用，不再另行产生支付任何费用。

2.3. 安全日常服务支持

2.3.1. 安全设备运维服务

对现有机房物理环境、安全设备、服务器系统、应用和终端进行安全日常检查，出具信息安全检查报告，检查内容包括但不限于设备、系统的资源使用情况、安全状况和存在的安全风险等。定期检测上述设备是否存在安全漏洞，如发现漏洞应第一时间进行漏洞修复，并对病毒库、漏洞库、规则库、系统版本等定期进行升级以提高防护能力。

结合网络安全态势感知平台,对接入的资产系统所存在、可能存在的风险进行跟踪定位，并对存在的安全告警进行逐一分析、判定和处置。

信息安全服务团队对信息安全相关设备和系统进行日常监控运维，包括但不限于防火墙、入侵检测设备、入侵防御设备、运维审计设备、数据库审计设备、网络综合审计设备、防病毒网关、隔离网闸、Web 应用安全网关等涉及信息安全的设备和系统，每日不少于一次，主要工作内容如下：

- 巡检监控、日常运维和跟踪分析记录，并根据工作环境和需求，开展相关培训工作。
- 根据巡检评估等分析结果，为安全设备、网络设备和服务器系统配置合理的安全策略，定期优化安全策略，定期升级安全设备事件库、漏洞库和规则库。
- 定期（每周/月/季度/年）分析安全设备的日志并进行总结，形成安全设备综合分析报告。
- 对各安全设备安全规则和策略进行梳理，达到最大化利用安全设备防护能力和监测能力。
- 结合网络安全态势感知平台对信息系统所产生的安全事件、告警和风险等进行分析定

位，并对高危事件进行深度验证（以便确认是有效攻击还是无效攻击）；对风险较高的信息系统和区域，进行综合分析，并提出解决加固方案。

乙方应提供安全防护系统策略梳理服务， 针对珠海机场现有的安全防护系统策略开展梳理工作，包括不限于以下要求：

- 日志分析：通过对安全设备进行日志分析能够识别网络攻击、发现潜在风险、及时进行策略调整和优化等。
- 策略分析：通过相关产品工具，对珠海机场全网安全防护系统策略进行分析和梳理，策略分析主要用于安全防护系统运行阶段的策略问题分析，包括不限于冗余策略、冲突策略、交叉策略、宽泛策略、any 策略、可合并策略、策略使用情况分析、隐蔽流量情况分析。
- 策略梳理：通过策略梳理帮助珠海机场查看每条策略的关联流量，并按照源 IP、目的 IP 等方式进行归并，完成珠海机场宽泛策略细化，另外结合流量分析功能完成安全防护系统策略梳理工作。

2.3.2. 系统漏洞扫描服务

乙方应具备网络扫描工具，定期检查珠海机场网络设备、应用服务器、主机系统、数据库、中间件和防火墙等系统的弱点，从而识别能被入侵者用来非法进入网络的漏洞。生成网络扫描评估报告，提交检测到的漏洞信息，提供漏洞等不符合项的整改方式，包括位置和详细命令描述，该项工作每季度不少于一次。

扫描内容包含但不限于以下：

- 是否能够获得目标系统的指纹信息；
- 系统开放的端口号；
- 系统中存在的安全漏洞；
- 是否存在弱口令；
- 系统不规范配置。

2.3.3. 系统渗透测试服务

渗透测试工作每季度不少于一次，同时测试内容至少包括网络层、系统层、应用层三方面：

- 网络层安全

乙方对珠海机场的信息系统所在网络层进行网络拓扑的探测、路由测试、防火墙规则试探、规避测试、入侵检测规则试探、规避测试、无线网安全、不同网段 Vlan 之间的渗透、端口扫描等存在漏洞的发现，通过漏洞利用来验证此种威胁可能带来的危害，并提供避免或防范此类威胁、风险或漏洞的具体加固措施，乙方在甲方同意情况下实施加固措施；

- 系统层安全

乙方通过采用适当的测试手段，发现测试目标在系统识别、服务识别、身份认证、数据库接口模块、系统漏洞检测以及验证等方面存在的安全隐患，并给出该种隐患可能带来的损失或后果，并提供避免或防范此类威胁、风险或漏洞的具体改进或加固措施，乙方在甲方同意情况下实施加固措施。

- 应用层安全

乙方通过采用适当测试手段，发现测试目标在信息系统认证及授权、代码审查、被信任系统的测试、文件接口模块报警响应等方面存在的安全漏洞,并现场演示再现利用该漏洞可能造成的客户资金损失，并提供避免或防范此类威胁、风险或漏洞的具体改进或加固措施，乙方在甲方同意情况下实施加固措施。

2.3.4. 移动 APP 安全检测

乙方应配合珠海机场检测移动终端 APP 的安全，保证用户个人信息的机密性、完整性。

为了达到以上安全目的，乙方应围绕珠海机场业务系统的移动终端的系统参数、系统数据、用户数据、秘钥信息、证书、应用程序等进行检测。并提供相对应的安全策略，包括但不限于以下：

- 提供措施对系统程序、应用程序、终端关键器件进行一致性检验服务；
- 对 APP 提供的受控和受限的资源及对象的访问、操作权限进行检测；
- 检测 app 对秘钥、证书、系统参数、用户数据等的安全管理，保证存储数据的机密性、完整性、可靠性；
- 检测 APP 记录安全相关事件的方式；
- 检测 APP 中的关键器件是否具备抵抗防篡改等物理攻击的能力；
- 检测 APP 操作权限管理能力；
- 检测接入网络的安全性；

- 检测与智能卡安全的进行信息交互。
- 该项工作每季度不少于一次

2.3.5. 代码安全审计服务

乙方应具备代码审计能力，对珠海机场当前现存的应用系统的源代码对其审计，从应用系统结构方面检查其各模块和功能之间的功能、权限验证等内容；从安全性方面，检查其脆弱性和缺陷，提供代码审计报告，代码审计报告应包含整改详细步骤，该项工作每季度不少于一次。

乙方提供的源代码审计工作应依据的国家颁发的编程规范和标准，针对应用程序源代码，从结构以及脆弱性和缺陷方面做审查工作，以发现应用程序中存在的安全缺陷以及代码的规范性缺陷。

源代码审计工作主要突出代码编写的缺陷和脆弱性，以 OWASP TOP 10 为检查依据，针对 OWASP 统计的问题作重点检查。

检查方法

通过灰盒（模糊测试）+白盒的方式检查应用系统的安全性，白盒测试所采用的方法是工具扫描+人工确认+人工抽取代码检查，依照 OWASP 2013 TOP 10 所披露的脆弱性，根据业务流信息检查目标系统的脆弱性和缺陷以及结构上的问题。

2.3.6. 信息安全应急服务

乙方应结合珠海机场环境，定期进行网络信息安全演练，采用实战与模拟相结合的演练方式，提高珠海机场与各协作单位的协同合作能力，并通过演练总结，完善应急预案，改进应急操作及流程，全面提高珠海机场预防和控制网络安全突发事件的能力。

2.3.6.1. 应急服务要求

乙方应提供 7*24 小时的电话支持信息安全服务,重大安全事件发生时应 10 分钟内响应且 1 小时内到达现场。

珠海机场根据网络管理员和系统管理员的初步判断认为和安全事件相关,信息安全服务团队驻场工程师应在 10 分钟内响应，并在 1 小时内到达现场支持，必要时安排信息安全专

家到场，乙方需根据我方安全事件级别进行应急响应。同时，应对上级或行业监管部门的检查也在应急响应的服务范围之内。

2.3.6.2. 应急响应内容

紧急事件主要包括但不限于以下：

- 病毒和蠕虫事件
- 黑客入侵事件
- 误操作或设备故障事件

根据安全威胁事件的影响程度来分类：

- 单点损害：
- 只造成独立个体的不可用，安全威胁事件影响弱。
- 局部损害：造成某一系统或一个局部网络不可使用，安全威胁事件影响较高。
- 整体损害：造成整个网络系统的不可使用，安全威胁事件影响高。

当入侵或者破坏发生时，对应的处理方法主要的原则是首先保护或恢复计算机、网络服务的正常工作；然后再对入侵者进行追查。因此对于紧急事件响应服务主要包括准备、识别事件（判定安全事件类型）、抑制（缩小事件的影响范围）、解决问题、恢复以及后续跟踪。

2.3.6.3. 应急响应等级要求

乙方根据安全事件分类或故障分类级别来提供应急响应的等级，同时建立信息安全的应急策略和应急措施，当出现重大事件时能能按照应急程序进行应急处理，消除或降低信息安全事件的影响，同时乙方须提供资产扫描工具、安全应急溯源工具等工具。服务标准不低于以下要求；

事件分类	事件描述	威胁级别	支持方式
紧急事件	甲方业务系统由于安全问题崩溃、系统性能严重下降，已无法提供正常服务。出口路由由于网络安全原因非正常中断，严重影响用户使用。公众服务由于安全原因停止服务或者造成恶劣影响的。	高危险	现场支持

严重事件	甲方内部的业务支持系统由于安全事件出现问题，导致不能运转正常不稳定。部分服务由于安全原因中断，影响正常使用。	中危险	现场支持
一般事件	由于安全原因导致系统出现故障，但不影响用户正常使用。甲方提出安全技术处置、索取安全技术资料、技术支持等。	低危险	远程支持或现场支持

2.4. 安全专项工作支持

2.4.1. 重大节日安全保障服务

乙方应提供重大活动信息安全保障服务，在重大活动保障前，按照上级单位民航及公安的相关要求进行专项安全检查工作，在重大活动保障期间，提供信息安全专家现场全天候驻守，并提供服务报告：

时间	检查和保障内容	服务交付物
活动前一星期	系统应用服务器、数据服务器和其他服务器的木马、蠕虫病毒和漏洞等检查(不限云端检测与现场主机检测）； 应用系统扫描等；	《木马、后门、蠕虫、病毒、病毒检查报告》 《漏洞扫描报告》等
活动期间	现场安全值守：安全状况监控（包含广告大屏内容监测）、安全预警信发布、现场应急响应	《安全值守日志》
活动后一星期内	信息安全情况总结	《总结报告》

2.4.2. 合规性专项检查服务

乙方应依据民航局、公安机关和公司等上级单位下发的关于行业信息安全技术指引及上级监管单位的工作要求，完成甲方的信息系统专项检查及整改工作。检查涉及的配置合规性，

网络及信息系统的安全风险等工作内容，对相关资产进行实施前调查、实施过程记录、检查结果分析、系统运作情况进行汇总、分类与分级，并最终输出相关安全调查、实施过程与建议报告。

乙方应具备资深的安全检测与安全防护的经验积累，丰富的安全服务项目实施经验，可根据外部机构如民航局、等保测评机构和公安机关等合规性检查要求，提供以下服务支持：

- 完成珠海机场在外部机构检查前进行信息系统安全自查，提出整改方案并完成整改，直至通过合规性检查。
- 在外部机构（包括不限于民航、公安机关和测评机构等机构）检查过程中配合检查，提供相关技术支持。

针对检查结果，编写信息安全检查汇总分析报告或审计报告。

2.4.3. 攻防对抗及竞赛服务

乙方应根据甲方要求完成国家级、省级、市级等不同级别的攻防演练活动，必要时派遣专家团队参与。同时配合珠海机场完成各项网络信息安全竞赛，提供相应网络信息安全竞赛培训资料、练习靶场等，必要时提供相关的技术支持。

2.5. 信息安全培训及宣传服务

乙方应配合珠海机场开展各项网络信息安全培训及宣传活动，形式包括但不限于：月度安全工作坊培训、雷锋月网络信息安全意识宣传、国家网络安全宣传周培训等，根据培训、活动内容制作相应培训课件，提供宣传平台、宣传刊物（含制作、耗材等费用）等，并且每年面向珠海机场全体人员的网络安全教育不少于两次，同时乙方对珠海机场网络信息安全技术人员提供信息安全技术类培训。

网络安全教育培训内容包括但不限于以下：

- 个人信息保护意识；
- 木马病毒与恶意代码防范；
- 账号密码安全；
- 电子邮箱安全；
- 远程办公安全。

信息安全技术类培训包括但不限于以下：

- 操作系统安全防护；

- web 系统安全防护
- 系统应急事件处理；
- 安全系统运维管理；

2.6. 安全咨询及规划服务

提供网络信息安全咨询及规划服务，向珠海机场持续提供信息安全专家服务，规划珠海机场信息安全建设发展的蓝图，包括但不限于网络安全建设、数据安全建设、等级保护建设、蓝队体系建设、混合云安全规划等，制定以上建设规划方针，建立年度安全服务工作计划，经甲方确认的规划方案，并按计划落实相关服务工作。。

2.6.1. 安全专家服务

本项目中，乙方提供信息安全专家向珠海机场持续提供信息安全专家服务，规划及落实珠海机场信息安全管理体系持续优化和改进。

服务内容包括但不限于以下：

- 信息安全管理及技术培训；
- 系统建设信息安全方案评审；
- 重大信息安全建设项目实施建议；
- 安全系统运维优化建议；
- 信息安全疑难问题诊断和专家建议；
- 信息安全前瞻性技术和方案建议。
- 信息安全体系制度优化和修订

信息安全专家应定期对网络信息安全工作进行复盘总结，并规划下一步工作计划，结合自身及珠海机场的网络信息安全工作成果，按照月度、季度、半年度、年度的形式，输出相应网络信息安全工作总结报告、网络信息安全刊物等。

2.6.2. 数据安全规划建设

乙方应具备数据安全规划与建设能力，按照甲方要求完成数据安全体系建设，建立健全数据分级分类管理、数据安全风险评估、数据安全监测预警、数据安全应急处置和数据安全审查等数据安全基本制度，逐步推进数据全生命周期各阶段的安全运营，满足数据安全技术要求。

包括但不限于以下：

- 数据安全总体规划方案及路径:现场访谈、调研、查阅组织级战略规划文件，进行数据安全总体规划设计，并构建数据安全建设路径图，规划设计组织级数据安全管理体系文档框架，为后续数据安全执行落地提供有力依据；
- 数据安全组织架构规划:规划设计完善组织级数据安全组织架构及数据安全角色职责，为数据安全责任落实提供有力保障；
- 数据分类分级规划：梳理珠海机场的数据类别和级别，包括敏感数据及重要数据，对数据进行分类分级，并形成指引及分类分级样例表，指导珠海机场的数据分类分级落地，并建立数据分类、数据分级、用户分级清单，梳理标记组织内数据类别及级别，为数据安全管控提供依据；
- 数据安全合规差距分析服务：根据国家法律法规、民航局、公安机关和公司等上级单位政策制度要求，通过对标合规性体系差距分析（如 DSMM、DSG 等体系），分析评价组织级数据安全能力成熟差距；

2.7. 网络安全态势感知服务

通过网络安全态势感知服务，对甲方信息系统、终端设备、安全设备和数据库等设备的行为建立长效安全监测机制，以实现全公司网络系统的自动化集中安全管理、安全监测和通报预警。监测手段不限信息系统监测预警、布点监测、重要系统日志集中分析和存储、流量检测、资产普查等方式。

网络安全态势感知平台应能对珠海机场内网络空间安全态势提供数据支撑,并集合大数据的有效信息提供分析展示平台，从多个维度，提供大数据分析结果，为研判、决策及日常运维管理的网络安全保障工作提供有效支撑。同时包含态势感知平台日常运维、故障维修、产品升级、配置变更等。

本平台乙方以服务的方式提供给我方，要求如下：

网络安全态势感知系统		
产品名称	**描述**	**数量**
网络安全态势感知平台	1、 提供软硬一体化设备，以便于更好的适应网络环境部署需求。 2、 网络安全态势感知平台支持对网络流量及安全设备数据的采集、展示、检索、分析、溯源和响应处置，结合威胁情报可实现对威胁的快速精准判定，满足客户对传统态势感知场景的需求。 3、 包含大数据平台处理模块支持数据采集、解析、标准化、	1 套

	丰富化、存储、检索、计算等;基础分析模块支持情报分析、关联分析、威胁行为分析、攻击检测等；安全运营基础模块支持安全态势、安全事件管理、可视化 BI 分析、智能仪表盘、自动化报告、资产风险评估、安全信息库、预案可视化编排和自动化响应、指挥调度等。 4、 硬件规格要求：机架式服务器，CPU*2（不少于 10 核心 20 线程），内存不少于 128G，SSD 硬盘不少于 960G， 企业级 SATA 硬盘不少于 32T，支持冗余电源，千兆电口不少于 4 个，万兆光口不少于 2 个。	
态势感知前端数据采集器		
全流量采集器	1、 硬件要求： 应用层吞吐量不低于 1Gbps 须满足数据存储高可用，磁盘不少于 1T 提供千兆电口不少于 6 个,千兆光口不少于 2 个	1 台
	2、 支持基于网络关键节点的全流量审计、协议识别、重组还原，内置威胁检测能力，可提供攻击检测、攻击成功检测、威胁情报检测等多种维度的威胁检测; 3、 可将本地分析后的数据实时传递到态势感知平台，进行关联分析和大屏展示。	

2.7.1. 平台技术参数要求

功能项	功能子项	功能具体要求
数据接入	采集种类	支持业内通用标准数据获取方式，获取方式不少于 15 种，包括 Syslog、SFTP、文件、Kafka、HDFS、主机终端(win/linux)Agent、DB2、Mysql、Oracle、Sqlserver、Postgrel、SNMP、Netflow、WMI、ES、AWS 等。 可接入各类硬件设备和应用系统，包含但不限于主机、防火墙、IPS/IDS、WAF、网络设备、安全设备、数据库、应用系统、中间件、存储。设备、虚拟化设备、机房设备、云平台（AWS）等多种设备和系统的日志接入方式。
XDR 分析	XDR 模型	支持内置 500+XDR 规则模型，并支持模型的启用与停止配置。
		支持查看 XDR 模型对应的典型攻击场景，理解典型的攻击过程，辅助告警分析研判。
	AI 模型	支持孤立森林算法、ARIMA 时间序列算法、自研关联分析算法、向量机模型、长短期记忆网络、卷积神经网络、word2vec 模型、神经网络模型、多层人工神经网络、预训练语言模型等算法模型检测暴力破解、个人行为异常、群组行为异常、账号共享预判、DGA 域名、DNS 隐蔽隧道、SQL 注入等网络攻击。
SIEM 数据预处理	数据解析	数据解析规则支持规则嵌套和逻辑组合方式,能够对一组事件进行多层规则解析处理，添加、删除、重命名、合并、拆分与裁剪现有字段，对范式化后字段再解析处理。支持多种数据解析，包含精准匹配、包含再解析、正则匹配后从数据头、尾进行二次解析等处理 。

		支持解析字段可以通过映射关系进行别名显示，映射方式有：文本、时间、URI 解码、IP 解码、重定义、正则、映射表等。同时还可以对某个或某些字段进行加密，无对应权限的用户不能显示该字段，但其他字段不影响。
		支持字段解析的自动化智能推荐，根据该日志数据的特点自动推荐匹配优先的对象类型，同时在字段映射时自动推荐靠前的字段类型。系统用不同的颜色提示推荐字段的匹配程度，减少人为选择的错误并提高效率。
SIEM 关联分析规则	关联场景和方式	关联分析系统的模型配置支持图形化配置和管理，有助于根据场景运营，支持修改所有预置关联分析规则，支持新建关联分析规则，关联分析规则修改、新建，不接受后台代码化实现方式。
		支持关联规则根据数据标准进行规则编写的自动化推荐，系统根据事件类型自动推荐其所属的对象。
		支持关联规则在配置时评估该策略运行所使用的资源情况，在线显示该规则的性能指标，分为优、良、差多个级别。
	时序关联分析	支持 A 事件后发生 B 事件，事件 A 发生后关联产生 B 事件，如检测到 webshell 连接后疑似通过 mysql 提权。事件前置条件是 webshell 连接成功，连接成功后通过 mysql 有提权操作，这两件事 30 分钟内先后发生。
		支持至少 M 次 A 事件之后发生了 B 事件，事件 B 的发生是因为事件 A 导致（事件 A 不限数量），如特定账号 5 分钟内进行暴力破解的次数大于或等于 10 次后，登录成功。
	预案联动	关联分析规则支持通过配置调用 SOAR 预案形成自动触发场景，支持触发周期、责任人的配置。支持设置告警抑制参数来将相同告警聚合并静默进而减少告警数量，抑制指标包括静默期（分钟、小时），静默条件（如根据源地址、结果、账号等）。支持指定告警阶段、告警级别和该告警使用的 ATT&CK 技战术。
安全态势	综合态势大屏	通过综合计算，展示当前网络的风险指数，支持展示主机、服务、网站、域名等资产数量；支持展示合并告警、告警、安全事件、失陷资产、资产脆弱性数量；支持展示待处置与已处置安全事件数、资产总数、风险资产数量、高风险资产 TOP5、威胁类型分布 TOP10、高危安全事件排行 TOP5、热点情报等。
	大数据中心大屏	支持轮播展示接入数据源数据分类地图，如接入 EDR 数据后展示文件操作、注册表行为、进程行为、其他等相关分类统计； 支持展示数据流向图，展示接入数据源各类型日志数量统计到系统后转换的各类型告警数量统计。
	威胁攻击态势	将具体的安全事件以 3D/2D 的形式展示出攻击源、攻击路径和攻击目标，通过地理位置直观掌握宏观攻击概况。通过攻击源国家的排名了解攻击者，通过受害 IP 和攻击阶段、攻击时间分布图了解攻击的严重程度和攻击面，最严重事件的排名指引关注危害最高的威胁。
	安全事件态势	安全事件态势根据提醒、告警、严重、紧急等 4 个等级各级事件总量、攻击成功和未成功的数量，展示待处置事件的总数、比例和环比变化，同时对高危待处置事件 TOP 进行排名，展示事件名称、等级、事件和责任人信息；

		对安全事件运营过程进行管理，展示事件变化趋势以及根据不同分类（如探测扫描、恶意程序、网站攻击等）统计新增、在处理和完结的事件数量，用来快速审视运营情况；
	威胁情报态势	威胁情报态势包含威胁情报告警类型分布，包含 APT、僵尸网络、窃密木马、黑客工具、挖矿、黑灰产等 16 类，支持显示具体分类的情报数量、命中告警数量。
		支持威胁情报告警摘要，命中情报家族团伙、情报告警趋势、威胁情报告警信息、命中威胁情报资产分布情况、命中威胁情报安全事件级别分布等统计。
	运营态势	支持查看情报引擎、数据平台、采集引擎、安全编排引擎等模块 CPU、内存、状态展示。
		支持数据接入情况统计，包含数据源名称、日志接收速度等；支持平台运营模块健康状态监控、数据存储占比监控。
	攻击者态势	支持攻击者数量、出发告警数、情报告警数、已处置数等统计，且支持攻击者阶段分布、攻击类型、告警 TOP10、受害资产 TOP10、攻击源 IP TOP10、攻击源国家 TOP5 等统计信息。
	安全成果态势	通过该态势掌握各类安全事件的检测和产生分类，直观了解威胁情况。包含从原始日志、安全告警、安全事件多个层级描述安全建设实现的效果，体现整体安全事件的收敛；支持展示安全事件级别分布、安全事件处置情况、告警降噪情况、合并告警类型分布 TOP5、规则触发情况、触发规则数量分布、数据接入情况、最近 24 小时接入日志趋势等。
	XDR 运行态势	支持查看 XDR 套件的接入与响应态势，可查看套件的 IP、版本、型号及相关安全事件。
告警分析	告警详情	告警详细支持展示基础信息、原始告警、历史经验、同类告警； 基础信息包含攻击者、受害者、告警次数、攻击结果、威胁信息、HTTP 请求/响应、事件、关联实体、命中告警 payload 高亮显示等信息； 原始告警包含的关联原始日志信息，并可以对其关联流量 pcap 包进行下载；历史经验提供同类告警的历史处理经验；同类告警中展示想同类型的告警列表。
	处置建议	对告警进行处置时提供 ATT&CK 缓解措施建议、ATT&CK 检测建议，并且在平台能够连接互联网的情况下，支持查看云端富化处置建议与云端攻击案例，云端攻击案例包含杀伤链资产视角图示、杀伤链攻击过程、杀伤链技战术等。
安全事件分析	安全事件总览	支持以 XDR 引擎自动聚合告警形成安全事件，并通过时间、标题、攻击 IP、风险资产、事件分类、事件等级、处置状态、责任人进行搜索过滤。
	安全事件分析	自动聚合相关告警，并以发生时间顺序展现，并支持关系图模式与溯源模式两种展示方式，能对汇聚的告警进行单独确认或者批量确认，并支持关联预案进行手动联动处置，预案包括封禁 ip、隔离主机等。
		支持基于恶意行为分析告警生成 UEBA 安全事件。
		具备网络数据的安全检测能力。
		告警事件支持 ATT&CK 攻击技术识别与详细说明展示，包括攻击技术的说明，攻击技术的数据源等信息辅助分析。

攻击者分析	攻击者分析	以攻击者视角自动聚合相关告警，支持从地理位置、情报风险等级、情报标签、侵害资产数量、攻击阶段、最近攻击时间等对每个攻击源进行统计分析。
		具备网络攻击取证能力。
		支持对单个攻击源进行深入分析，包含该攻击者关联告警类型分布、告警趋势统计、杀伤链统计及相关告警列表，告警列表同样支持下钻查看详情，并支持对单个告警进行处置预案联动。
云地一体化分析	云地一体化分析	支持告警上传云端进行自动化判定并将研判结果返回态势平台，以提高告警精准度。
多维场景化分析	多维场景化分析	支持安全场景包括不限于：Webshell、通用 web 攻击、漏洞利用、弱口令、爆破攻击、邮件威胁、隐蔽隧道、威胁情报、勒索病毒、挖矿木马，并支持在场景化分析界面调用处置预案进行快速处置。
UEBA	恶意行为分析	支持基于浏览器日志进行异常行为发现，并内置对应行为分析模型。
		支持展示恶意行为的用户列表，可查看资产详情包含资产分类、ID、负责人、Email、电话、恶意行为数量、可疑行为数量等。
		具备识别程序的网络行为是否异常的能力。
		支持查看资产恶意行为详情，包含用户画像和行为时间轴，用户画像包含恶意行为总分、所属部门行为平均分、恶意行为倾向统计、画像标签、告警数量排名前五的用户常用 IP/资产、7 天 24 小时可疑行为热力图、可疑行为数量趋势等，行为时间轴中展示的恶意行为可标记处置状态。
实体分析	实体分析	支持对实体的网络连接关系进行图谱绘制，对图谱的手动操作包含删除、返回、前进、居中显示、固定显示等操作，对实体的分析操作包含按关系分类拓线、复制、固定节点、删除、预案执行、多源查询等操作。
云端沙箱分析	云端沙箱分析	支持将流量探针还原的文件自动上传云端沙箱进行威胁判断，并自动拉取扫描结果。
联动处置（SOAR）	可视化编排	支持 SOAR 预案可视化编排，根据不同安全策略的需求，通过拖拽预案动作的方式自定义安全预案，实现安全流程的自动化处置。
		支持多级子预案嵌套形成复杂的预案，并且预案可以复用。
	自动处置策略	支持手动添加自动处置策略，并支持禁用、启用操作。
		自动处置策略可配置策略名称、生效时间、状态、处置来源、策略条件、关联预案等内容。
资产管理	资产主动识别	支持从对接的资漏探针自动获取资产与安全相关字段信息，也可以使用导入模板，导入资产信息。支持添加资产自定义标签，支持标识为重要资产，且支持查看资产详情，包括资产组信息、服务信息、网站信息、域名信息等
	漏洞报告导入	支持绿盟 RSASV6.0、360 鸿光企业版等漏扫产品 excel 格式扫描报告导入。
日志检索分析	交互检索查询	支持检索一键切换 BI 分析，通过可视化 BI 图表自定义展示与分析，图表展示包括直方图、折线图、面积图、饼图、表格、统计值、同比、

		环比等多种类型，多维度快速展现数据的价值，在分析过程中支持设定周期自动刷新。 支持仪表盘和报表模板对 BI 分析结果的直接引用，BI 分析所用的查询条件和 BI 图例一起保存和发布。
		支持研判分析过程中在线解码，无需使用其他工具即可实现 BASE64\HEX\URL\JSON 等常见编码和解码转换功能，提高分析效率。
仪表板	仪表分析	仪表盘的图形位置和大小可自由拖拽，同时支持丰富下钻功能，可下钻至具体事件、告警、安全事件，也可跳转到自定义的其它仪表盘，实现仪表的嵌套，方便安全人员定制化的快速分析。
	可视化 BI 数据分析	提供强大的数据分析功能，可以多维度快速展现数据的价值。数据结果通过可视化 BI 图表自定义展示与分析，图表展示包括直方图、折线图、面积图、饼图、表格、统计值、同比、环比等多种类型。
		满足将查询条件保存并发布与设定周期自动刷新，支持选择查询条件和/或 BI 图例一起保存和发布。
系统管理	运营场景	支持 WEB 页面配置精准运营模式，通过该模式对平台告警进行降噪以满足不同的运营场景。
	用户管理	支持用户功能分权和数据分权管理，功能分权可以将平台的每个功能进行独立指定不可见、只读和读写权限；数据分权能与组织机构进行映射，通过类 SQL 结构化检索语言定义日志、告警的字段、字段组合进行数据分权范围。
等保电子化管理	等保电子化管理	支持等级保护工作电子流程化管理，按基础信息录入、定级、备案、差距分析、整改、测评、监督检查等流程化管理电子文档，并支持等保知识库管理功能。
安全工单	工单内容	支持设置工单标题，优先级，截止时间，受理人，是否需要审批，审批人，工单内容、工单附件；工单内容支持在线富文本编辑，包括文字、表格、图表等；工单附件支持文件类型包括：rar、zip、gz、doc、docx、pdf、txt、ppt、pptx、xlsx、xls、csv、jpg、jpeg、png；支持保存工单至草稿箱，便于后续编辑。
	工单调用	支持在合并告警、安全事件、脆弱性界面一键发起对应类型的工单，并根据所选择的合并告警、安全事件、脆弱性内容，自动设置工单标题、优先级、自动填入工单内容；支持选择多个合并告警、安全事件、脆弱性发起批量工单；支持通过响应预案模块自动化发起工单；支持手动发起通用工单。
	指挥调度	重保任务场景下提供安全工单任务的规划、分解、分配，可设置任务的各类属性，比如优先级、负责人、状态、进度、到期日、风险等；提供安全任务的跟踪调度功能，提供任务的信息交互，催办等功能；提供方便的任务状态与更新方式，可以用平台账号登录查看与更新。
产品资质	产品资质	产品须具备公安部颁发的《计算机信息系统安全专用产品销售许可证》。

全流量采集器	流量还原	提供对网络流量中主流协议进行识别、解析还原并记录，用于取证分析、威胁发现，支持协议包括：HTTP、DNS、SMTP、POP3、IMAP、Mysql、Postgresql、DB2、Oracle、Mongodb、Resp、SMB、NFS、FTP、RIP、Netflow、DHCP、BGP、ICMP、OSPF、Radius、RIP、VNC、NTP、RDP、Rlogin、RSH、Idap、SSH、Oicq、Telnet 等，还原内容包括：TCP 会话、行为日志、登录行为等；
		提供对网络流量中的文件进行识别和还原，支持可执行文件（exe、dll、msi 等）、文档类文件（docx、pptx、xls、pdf 等）、压缩文件（rar、zip 等）、移动应用 apk 等
	攻击检测	具备攻击结果判断能力
		具 0day 漏洞识别能力。
		支持检测 web 漏洞，例如 PHP 代码执行、扫描器漏洞探测、XSS 跨站脚本、PYTHON 代码执行、SQL 注入攻击等。
		具备未知文件样本安全性鉴定的能力。
		提供常规渗透入侵、内网横向渗透，提供精细化规则 65 条，例如读取/etc/passwd 文件、执行 ipconfig 命令、执行 netstat 命令等，提供 web 木马类型 300+种，木马隧道 5 种，挖矿页面 6 种等各类黑客攻击和恶意流量进行实时精准入侵动作识别及报警，并能够检测出系统中受控的服务器，定位出当前企业受影响的业务模块。
		攻击检测覆盖：Web 攻击、恶意软件、二进制攻击、网络钓鱼、信息探测、异常行为、网络攻击、横向移动、暴力破解、服务攻击、域内渗透攻击、SHELL 命令执行、异常通信等攻击场景
		支持基于特征库检测钓鱼欺诈网页能力。
		支持基于人工智能模型检测各种变种漏洞，如 Struts2 系列漏洞、SQL 注入漏洞、Java 反序列化漏洞、CMS 类型漏洞等；
	威胁情报	支持基于威胁情报的威胁检测，检测类型包含僵尸网络、勒索软件、流氓推广、网络蠕虫、远控木马、黑市工具、其他恶意软件等

3. 服务评分方法和标准

对乙方的年度安全运维服务每半年度进行一次综合考核评分，根据评分情况支付安全服务外包费用。

总的考核计分方法如下：考核结果（百分制）=服务综合考核得分+网络安全事件处理实效考评得分+安全运维服务工作质量得分

3.1. 服务综合得分

考核部门:珠港机场管理有限公司（以下简称珠港机场公司）资讯科技部。

以半年度为单位，对乙方的工作情况(如遵章守纪、工作规范、安全运维及安全事件处

理情况、巡检等记录是否及时完整、用户满意度等综合情况)进行考核，权重 40 分。

扣分标准：

1) 对有违反服务标准、服务流程、管理制度的行为按次数进行扣分，每次 2 分；

2) 没有提前提交月报会议材料，扣 1 分；

3) 没有按时交会议纪要，扣 2 分；

4) 在维护过程中与报障者产生冲突影响极坏的，本考核为 0 分。

3.2. 网络信息安全事件处理实效得分

考核部门：珠港机场公司资讯科技部

以半年度为单位，在安全事件处置服务过程中进行事件处理质量的考评，权重 30 分。分数评定因素可参考故障响应时间、故障处理时间、故障处理结果的用户满意度等。

扣分标准：

1) 未在按规定时间做出响应的情况，一次扣 2 分；

2) 安全事件（隐患）处理时间过长，按照实际情况扣 2 至 5 分；

3) 故障处理结果甲方不满意的，按照实际情况扣 2 至 5 分；

4) 甲方有要求而未能及时提供咨询建议或采取措 施导致发生信息安全事件的,扣 50 分；

3.3. 安全运维服务工作质量得分

考核部门：珠港机场公司资讯科技部

以半年度为单位，权重 30 分，按照乙方承诺的服务内容及要求的执行情况及工作质量得分。如无违规操作，能按要求进行定期巡检、制定有效的安全策略、日常检查记录清析完整等考评因素。

扣分标准：

1） 如发现巡检记录不真实的，一次扣 5 分；

2） 如没有满足本需求提出的服务要求的，一次扣 5 分；

3） 未进行事前方案评审、事中执行监督、事后评估跟进的每次扣 2 分；

4） 对专项 安全任务交付质量差导致其他负面影响，每次扣 6 分；

5） 其他资料质量和服务效果不理想的，每次扣 3 分；

6） 人力资源保障未能到位的，每次扣 3 分；

7） 咨询人员管理不到位，每次扣 3 分；

3.4. 对服务承包商的考核评分

半年度考核评分表：

服务承包商半年度**考核评分表（202__年__半年度）**

<table>
<tr><td colspan="6"><u>珠海机场安全规划及服务项目</u>考核评分</td></tr>
<tr><td>考评项目</td><td>分项总分</td><td>分项得分</td><td colspan="2">扣分</td><td>最后得分</td></tr>
<tr><td>综合服务考核得分</td><td>40</td><td></td><td colspan="2"></td><td></td></tr>
<tr><td>故障处理实效考评得分</td><td>30</td><td></td><td colspan="2"></td><td></td></tr>
<tr><td>维护工作质量考核评分</td><td>30</td><td></td><td colspan="2"></td><td></td></tr>
<tr><td>服务考核总得分</td><td colspan="5"></td></tr>
<tr><td>服务承包商</td><td colspan="2"></td><td>考评单位</td><td></td><td>考评时间</td><td></td></tr>
<tr><td>考评人</td><td colspan="2"></td><td>考评成绩</td><td colspan="2">得分： ☐优秀 ☐良好 ☐合格 ☐不合格</td></tr>
<tr><td colspan="6"></td></tr>
<tr><td>服务商签名</td><td colspan="2">年 月 日</td><td>经理签名</td><td colspan="2">年 月 日</td></tr>
</table>

考评成绩及服务费用支付：

A. **优秀得分范围：90～100 分　　支付 100%的服务费。**

B. **良好得分范围：80～<90 分　　支付 95%的服务费。**

C. **合格得分范围：70～<80 分　　支付 80%的服务费。**

D. **不合格得分范围：70 分以下支付 50%的服务费。**

考评原则：考评结果为 D，即 70 分以下，中标方需立即针对考评不合格的原因进行分析，并立即整改，如在下一半年度考评依旧不合格者，甲方有权解除合同而不给予服务承包商任何赔偿。如对机场运行保障造成严重影响，中标方需赔偿机场方经济损失。

4. 服务验收标准

验收范围主要为：交付物验收

验收标准为：供应商应负责在项目验收时将全部有关输出文件、阶段性交付物成果、日常安全运维报告、验收报告以及相关培训文档等汇集成册交付用户，交付物需符合监管部门法律、法规和民航规定的合规要求，并由双方项目组评审通过，双方签字生效。

项目交付物：

信息安全现状分析报告（包括但不限于）：

信息安全体系成熟度评估、安全漏洞扫描报告、安全渗透性测试报告、IT 设备人工安全检查报告、信息系统安全检测报告、系统架构安全评估报告（包括网络架构部分）、信息资产风险评估报告、IT 流程风险评估报告、信息安全管理体系制度文件等。

- 信息安全体系实施规划报告
- 信息安全体系实施规划报告及规划图表
- 安全策略（审批稿）
- 安全策略细化系列文档
- 运行部门有关安全管理制度文档
- 安全控制措施落实方案
- 安全控制措施落实记录
- 优化后的文件制度
- 安全运维日常工作报告
- 应急响应报告
- 安全加固报告
- 重大活动安保服务报告等
- 应急演练和攻防演练报告

5. 付款方式

乙方须按照本项目采购需求提供 24 个月的网络信息安全服务及平台，甲方按半年度支付乙方年度安全服务费用，每半年度支付本合同约定年度安全服务费的 50%，实际支付按第 3 章条款约定对乙方在服务期间进行考核及评分的得分情况进行结算。乙方须于每半年度首月 15 日内向甲方递交上半年度的服务费结算申请，并提供结算资料及等额合法增值税专用（包括发票联及抵扣联）发票（税率为 6%）后 60 个工作日，甲方核实后付款。

乙方在甲方支付款项前，应按甲方应支付的数额向甲方提供合法、有效的增值税专用发票及 付款申请书等付款资料，该付款资料应经甲方审核通过。不按本协议约定提供或不及时提供该付款资料的，甲方有权不予支付或延迟支付相应款项且不承担任何违约责任，乙方的各项协议义务仍应按本协议约定继续履行。乙方开户银行名称或账号等信息有变更，应在本协议规定的相关付款期限前 30 个工作日以书面形式通知甲方，否则甲方不承担因此导致的违约责任。

6. 资格要求

序号	内　容	说 明 与 要 求
1.	资格要求	1. 具备中国网络安全审查技术与认证中心颁发的信息安全服务资质认证证书。 2. 具备中国信息安全测评中心颁发的信息安全服务资质认证证书。 备注：以上资质须在有效期内并出具复印件证明加盖单位公章。