第四部分　采购需求说明书

能力清单		数量
服务项目	内容	
互联网资产测绘	**互联网资产识别及风险暴露面排查：** 对互联网资产的操作系统、端口与服务、Web 应用、资产组件、登录页面、端口服务等情况进行自动识别、风险暴露面排查，形成资产台账，并定期更新和审核。具体包括： 1.操作系统识别，对互联网应用进行操作系统识别。 2.端口与服务发现，对目标进行 65535 全端口扫描，并整理出服务的端口、应用类型、版本等。 3.Web 应用识别，对 Web 应用系统进行深度识别，包括其使用的开发语言、开发框架、Web 服务器类型、页面 Tittle、首页页面数据。 4.资产组件识别，对 http 系统所使用 web 组件识别。5.登录页面自动识别，通过搜索引擎、页面数据自动识别主域名下的所有登录页面。 6.识别判断端口的开放与关闭情况，整理出清单。	12 次（每月 1 次）
	影子资产排查： 根据关键词标识出互联网上归属中国银行广东省分行的互联网“影子资产”，持续监测及发现外部机构在互联网渠道上挂中国银行广东省分行信息的情况。具体包括： 1.提供平台化的模糊资产发现功能，根据中国银行广东省分行提供的业务相关关键词，搜索互联网上存活 IP，标识出归属中国银行广东省分行的互联网“影子资产”。 2.持续监测及发现外部机构(中国银行广东省分行合作公司、其它不相关机构等）在互联网渠道（包括但不限于网页、微信公众号、小程序等）上挂中国银行广东省分行信息(包括但不限于可被识别成中国银行广东省分行的相关文字、图片 Logo 等）的情况，及时书面通报甲方。	
	敏感信息泄露排查： 互对互联网侧的信息泄漏进行排查，包括：项目文档泄漏、代码泄漏、人员信息泄漏、敏感信息泄漏、社工库泄漏查询等，具体包括以下内容： 1.在流行的开源社区（如 Github、码云等）搜索相关信息，涵盖但不仅限于项目配置文档、API 接口密钥、敏感文档、项目源代码、设计文档、通讯录、账号密码等信息。 2.对互联网网盘（如百度网盘、腾讯微云等）的共享文档进行搜索，搜索范围涵盖但不限于表格、文档、pdf、图片等文件。 3.对国内主流的各大文库站点进行检索，发现跟中国银行广东省分行相关的敏感信息和文件。包括但不限于：豆丁、道客巴巴、百度文库、简书等互联网文库。 4.对暗网交易情报监控，识别主流的暗网交易平台中与中国银行广东省分行相关的交易情报和贩卖信息。	
	微信公众号和小程序排查： 根据关键词进行全面发现识别，识别其类型、状态、认证主体等信息，解析识别其功能菜单资产及变化情况（如所属微信号，AppID，服务状态）。	
渗透测试	广东中行的所有互联网应用系统（约 200 个 URL）	2 次（每半年 1 次）
	全辖网点提供客户使用的互联网设备（含网关等，需在广州地区及 21 个地市分行现场测试）	