

附表一 服务清单

## 1. 安全运维

序号	项目名称	主要内容描述	频率
—	统计局安全运维服务		
1	安全应急响应	根据事件类别，通过远程和现场支持的形式协助对遇到的突发性安全事件进行紧急分析和处理。主要工作内容包括：突发事件相关信息的收集、事件的分析、报告提交、问题解决建议等。	随机
2	漏洞扫描	对网络设备、主机服务器、操作系统、数据库和应用服务等中存在的安全漏洞进行扫描，并提供漏洞评估报告和漏洞修复解决方案。	月度
3	安全加固	针对安全漏洞和安全配置评估中发现的安全漏洞和配置缺陷，提供加固意见和方案，配合客户完成配置修复	季度
4	安全巡检	定期对IT系统、网络、安全设备等进行特定内容安全检查。一般包括设备健康性检查，以此发现客户日常IT运维的安全隐患，解决并规避安全风险。	季度
5	渗透测试	通过人工黑盒的测试方式，发现网络和业务系统中网络和系统存在的安全缺陷，提供渗透测试报告和改进建议。	月度
6	日志审计分析	每月对安全设备、服务器和系统的日志进行审计分析，提供报告。	季度
7	安全应急演练	根据实际环境，提供专项预案，准备演练场景，以模拟演练的方式检验应急预案和应急流程是否完	随机

		善，提高应急处理能力	
8	重要时期安全保障	重要时期协助甲方进行网络安全保障。包括但不限于制定保障方案，7*24小时值守，开展安全隐患排查和加强防护，对保障工作进行总结等工作。	随机
9	配置评估	使用安全配置核查工具或人工方式，对系统网络设备、操作系统、数据库和应用服务器的配置进行安全检查，并提供安全配置评估报告和解决方案。	季度
10	安全培训	对技术负责人、管理员、操作人员、系统维护员及其他相关人员进行现场培训和统一集中培训	随机
11	恶意样本分析	通过现场分析的方法对客户的主机操作系统和应用运行环境的恶意代码排查，主要包括可疑文件、可疑服务、可疑进程、可疑端口、可疑的网络连接、网站WebShell后门等一系列内容的深入检查和分析，并提供安全分析报告和清除方法。	随机
二	国资委安全运维服务		
1	安全应急响应	在安全服务期间为甲方提供24小时应急响应服务，远程或现场（1小时之内到达现场），在最短时间内协助甲方响应和处理安全事件，并提供详细的解决方案。对安全事件应急响应的全过程形成记录，并提供对系统加固、加强保护的可行方案。	随机
2	漏洞扫描	使用多厂商漏洞评估产品，远程和现场检测的方式，检测网络设备、操作系统、数据库和应用服务中存在的安全漏洞，提供漏洞评估报告和修复建议，并协助甲方对漏洞进行修复。每月提供漏洞检测和评估报告，并对漏洞修复情况进行记录。	月度
3	安全加固	为用户定期提供信息系统、服务器、网络设备、安全设备等风险排查及修复、策略优化，并形成记录。	季度

4	安全巡检	定期对网络、安全设备等进行特定内容安全检查。一般包括设备健康性检查，以此发现客户日常IT运维的安全隐患，解决并规避安全风险。	月度
5	渗透测试	每季开展一次渗透测试，发现网络和系统中存在的安全缺陷，提供渗透测试报告和改进建议，并协助整改。	季度
6	日志审计分析	每月对安全设备、服务器和系统的日志进行审计分析，提供报告。	月度
7	安全应急演练	根据用户系统实际情况，协助用户每年开展一次应急演练，包括制定应急演练方案，组织演练，撰写应急演练报告等。	随机
8	重要时期安全保障	重要时期协助甲方进行网络安全保障。包括但不限于制定保障方案，7*24小时值守，开展安全隐患排查和加强防护，对保障工作进行总结等工作。	随机
9	安全检测服务	每季度为用户提供对服务器恶意代码检测服务，发现问题立即处理。每月提供恶意代码检测报告，并对恶意代码处理情况进行记录。 每季度为用户提供定期网络性能和网络安全测试服务，并提供测试报告。	季度
10	风险评估	每年至少对用户网络及系统做一次安全风险评估，出具报告并提供解决方案，协助整改。	年度
三	内蒙古自治区粮食和物资储备局安全运维服务		
1	安全应急响应	根据事件类别，通过远程和现场支持的形式协助对遇到的突发性安全事件进行紧急分析和处理。主要工作内容包括：突发事件相关信息的收集、事件的分析、报告提交、问题解决建议等。	随机
2	安全加固	对加固目标的安全漏洞进行修复、配置隐患进行优化的过程。加固内容包括但不限于漏洞补丁、防火墙、防病毒、危险服务、文件共享、自动播放、密码安全	季度

		。	
3	安全巡检	每季度对托管设备及应用系统安全进行巡检与分析，对托管设备配置需要更新的重新进行配置，并做好备份。巡检采用远程登录和本地检查的方式进行，并提供巡检报告。	月度
4	渗透测试	通过人工黑盒的测试方式，发现网络和业务系统中网络和系统存在的安全缺陷，提供渗透测试报告和改进建议。	季度
5	漏洞扫描	对网络设备、主机服务器、操作系统、数据库和应用服务等存在的安全漏洞进行扫描，并提供漏洞评估报告和漏洞修复解决方案。	月度
6	日志审计分析	每月对托管设备、应用系统服务器和系统的日志进行审计分析，提供报告。	季度
7	安全应急演练	根据用户系统实际情况，协助用户每年开展一次应急演练，包括制定应急演练方案，组织演练，撰写应急演练报告等。	随机
8	重要时期安全保障	重保期间、系统网络割接后或其它任何可能对业务运营产生重大影响时刻，提供7*24小时重保安全现场服务，并提供服务方案、应急预案、服务日报、故障总结等书面材料。	随机
9	配置评估	使用安全配置核查工具或人工方式，对系统托管设备、操作系统、数据库和应用服务器的配置进行安全检测，并提供安全配置评估报告和解决方案。	季度