通信网络安全防护符合性检测表—经营分析系统

填写说明	1、本表为通信网络安全防护达标检查表经营分析系统部分，适用于经营分析系统相关安全防护定级对象的企业安全自查，及主管部门或其他机构开展的安全达标评测。 2、本表相关检查内容依据《YD/T 3800-2020 电信网和互联网经营分析系统 安全防护要求》、《YD/T 4057-2022 电信网和互联网经营分析系统 安全防护检测要求》及《YD/T 2669 第三方安全服务能力评定准则》制定。 3、本表由相关定级对象的所属单位填写，每个定级对象填写一份。 4、本表填写状态及达标情况部分相关内容为自动生成，当"未完成项数量"数值不为0时，表示本表中还有检查项目未完成。 5、本表检查项目部分"检查结果"应根据各检查点内容及要求，按照定级对象相关实际情况下拉选择相应的选项（是、否、不适用），需对相关情况补充说明的可在检查结果选项下方的对话框中填写说明信息。

检查项目

序号	适用范围	检查类型	检查内容	适用网络属性	检查点	备注	答案	答案说明
1.1.1	第1级及以上	经营分析系统 -物理安	应满足YD/T 1754中的要求	经营分析系统	是否满足YD/T 1754中的要求？		是	
1.2.1	第1级及以上	经营分析系统 -网络安全	应经制与当前运行情况相符的网络拓扑结构图	经营分析系统	是否经制与当前运行情况相符的网络拓扑结构图？		是	见附件
1.2.2			应实现网络安全域划分，经营分析系统 与外部系统之间使用防火墙进行隔离和访问控制	经营分析系统	是否实现网络安全域划分，经营分析系统 与外部系统之间使用防火墙进行隔离和访问控制？		是	见附件
1.2.3	第2级及以上		应定期对网络进行安全检查和审计	经营分析系统	是否定期对网络进行安全检查和审计？		是	见附件
1.2.4			应及时修补漏洞，杜绝弱口令	经营分析系统	是否及时修补漏洞，杜绝弱口令？		是	见附件
1.2.5			应对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新	经营分析系统	是否对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新？		是	见附件
1.2.6			应监视是否对经营分析系统 存在以下攻击行为：端口扫描、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等。	经营分析系统	是否监视是否对经营分析系统 存在以下攻击行为：端口扫描、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等？		是	见附件
1.3.1	第1级及以上	经营分析系统 -主机安全	应对登录操作系统的用户进行身份标识和鉴别	经营分析系统	是否对登录操作系统的用户进行身份标识和鉴别？		是	见附件
1.3.2			操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序	经营分析系统	操作系统是否遵循最小安装的原则，仅安装需要的组件和应用程序？		是	见附件
1.3.3			应关闭不必要的端口，保持端口服务最小化	经营分析系统	是否关闭不必要的端口，保持端口服务最小化？		是	见附件
1.3.4			应安装防恶意代码软件，并定期进行升级和更新防恶意代码库	经营分析系统	是否安装防恶意代码软件，并定期进行升级和更新防恶意代码库？		是	见附件
1.3.5	第2级及以上		应定期（至少每月1次）进行漏洞扫描（重大变更与系统升级后也需进行），以及时发现所使用的操作系统、中间件、数据库以及程序本身的安全漏洞，及时修补发现的安全漏洞以及配置不符合项	经营分析系统	是否定期（至少每月1次）进行漏洞扫描（重大变更与系统升级后也需进行），以及时发现所使用的操作系统、中间件、数据库以及程序本身的安全漏洞，及时修补发现的安全漏洞以及配置不符合项？		是	见附件
1.3.6			应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间	经营分析系统	是否能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间？		是	见附件
1.4.1	第1级及以上	经营分析系统 -云平台安全	应支持虚拟机之间、虚拟机与宿主机之间的隔离	经营分析系统	是否支持虚拟机之间、虚拟机与宿主机之间的隔离？		不适用	经营分析系统没有云服
1.4.2			应在虚拟化网络边界部署访问控制机制，以实现网络的安全隔离	经营分析系统	是否在虚拟化网络边界部署访问控制机制，以实现网络的安全隔离？		不适用	经营分析系统没有云服务器
1.4.3	第2级及以上		应支持虚拟机部署防病毒软件	经营分析系统	是否支持虚拟机部署防病毒软件？		不适用	经营分析系统没有云服务器
1.4.4			应支持对虚拟机脆弱性进行检测的能力	经营分析系统	是否支持对虚拟机脆弱性进行检测的能力？		不适用	经营分析系统没有云服务器
1.4.5			应部署一定的访问控制安全策略，以实现虚拟机之间、虚拟机与虚拟机管理平台之间、虚拟机与外部网络之间的安全访问控制	经营分析系统	是否部署一定的访问控制安全策略，以实现虚拟机之间、虚拟机与虚拟机管理平台之间、虚拟机与外部网络之间的安全访问控制？		不适用	经营分析系统没有云服务器
1.4.6			应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量	经营分析系统	是否能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量？		不适用	经营分析系统没有云服务器
2.1.1	第1级及以上	经营分析系统 -身份管理	应建立内部管理人员、租户、应用、组件等经营分析系统 用户的身份标识与鉴别机制	经营分析系统	是否建立内部管理人员、租户、应用、组件等经营分析系统 用户的身份标识与鉴别机制？		是	管理员通过4A创建用户经营分析系统 从账号，用户从账号作为系统唯一标识（见截图）
2.1.2			应支持身份标识唯一性检查功能，保证系统中不存在重复用户身份标识	经营分析系统	是否支持身份标识唯一性检查功能，保证系统中不存在重复用户身份标识？		是	重复账号不满足唯一性校验，无法创建（见截图）
2.1.3			应支持身份鉴别信息复杂度检查	经营分析系统	是否支持身份鉴别信息复杂度检查？		是	用户从账号作为唯一标识，4A支持身份用户从账号复杂度检查（见截图）
2.1.4			应划分不同的管理员角色，明确各个角色的责任和权限	经营分析系统	是否划分不同的管理员角色，明确各个角色的责任和权限？		是	分配不同的管理角色（见截图）
2.1.5	第2级及以上		当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听	经营分析系统	当进行远程管理时，是否采取必要措施防止鉴别信息在网络传输过程中被窃听？		是	所有设备主机、数据库、应用由4A统一管控，无需远程管理（见截图）
2.2.1	第1级及以上	经营分析系统 -账号管理	帐号的分配应经过审批	经营分析系统	帐号的分配是否经过审批？		是	见相关文档
2.2.2			应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制	经营分析系统	是否指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制？		是	统一有管理员进行账号管理（见截图）
2.2.3			应及时删除或停用多余的、过期的帐号	经营分析系统	是否及时删除或停用多余的、过期的帐号？		是	对过期账号进行加锁和删除（见截图）
2.2.4	第2级及以上		对于涉及敏感客户信息（例如客户详单等）操作的帐号，应禁止多人共享帐号	经营分析系统	对于涉及敏感客户信息（例如客户详单等）操作的帐号，是否禁止多人共享帐号？		是	无多人共享账号，对从账号进行细粒度授权，日志由4A统一管控（见截图）
2.2.5			系统维护交接时，需对开发、建设过程中设置的帐号进行检查，删除不必要的帐号，需要继续使用的帐号，均应重新设置口令	经营分析系统	系统维护交接时，是否对开发、建设过程中设置的帐号进行检查，删除不必要的帐号，需要继续使用的帐号，均应重新设置口令？		是	系统系统维护交接，将以前账号授权为失效状态（见截图）
2.2.6			员工离职需要回收帐号，员工转岗需要修改账号角色	经营分析系统	员工离职是否回收帐号，员工转岗是否修改账号角色？		是	回收人员账号进行加锁（见截图）
2.3.1	第1级及以上		口令长度不得少于8位，至少由数字、字母混合组成，至少每90天进行更新，且不得使用最近5次以内重复的密码，重复尝试3次以后应将该帐号锁定，在一定时间段暂停该帐号登录	经营分析系统	口令长度不得少于8位，至少由数字、字母混合组成，至少每90天进行更新，且不得使用最近5次以内重复的密码，重复尝试3次以后是否将该帐号锁定，在一定时间段暂停该帐号登录？		是	密码长度8位，大小写符号等组成，90天更换密码，密码输入失败5次 60秒后才能重新输入（见截图）
2.3.2			应避免使用默认口令	经营分析系统	是否避免使用默认口令？		是	默认账户已被锁定，（见截图）
2.3.3	第2级及以上	经营分析系统 -口令管理	管理员为各用户分配的初始口令应不同	经营分析系统	管理员为各用户分配的初始口令是否不同？		是	经分系统已全部纳入4A管理，口令规则由4A统一管控，个人用户不涉及默认口令，详细见4A账号密码管理规范。（见文档）
2.3.4			应确保帐号口令在系统内网络传输或者保存时不得使用明文	经营分析系统	是否确保帐号口令在系统内网络传输或者保存时不得使用明文？		是	经分系统已全部纳入4A管理，4A单点登录系统
2.3.5			帐号口令保存在文件中时，应改为不可读文件、并控制文件只能是对应程序访问	经营分析系统	帐号口令保存在文件中时，是否改为不可读文件、并控制文件只能是对应程序访问？		是	经分系统已全部纳入4A管理，不存储明文密码
2.4.1	第1级及以上	经营分析系统 -访问控制	应对经营分析系统 用户（内部管理人员、租户、应用等）进行认证，避免未授权访问	经营分析系统	是否对经营分析系统 用户（内部管理人员、租户、应用等）进行认证，避免未授权访问？		是	通过4A单点登录，见附件
2.4.2	第2级及以上		权限分配应支持最小授权原则	经营分析系统	权限分配是否支持最小授权原则？		是	构建角色权限矩阵，见附件
2.4.3			应支持对角色进行分级，不同级别的角色分配不同范围的权限	经营分析系统	是否支持对角色进行分级，不同级别的角色分配不同范围的权限？		是	构建角色权限矩阵，见附件
2.5.1	第1级及以上	经营分析系统 -接口安全	应对接口实施安全控制措施，如身份鉴别、访问控制、签名、时间戳和安全协议	经营分析系统	是否对接口实施安全控制措施，如身份鉴别、访问控制、签名、时间戳和安全协议？		是	见相关附件
2.5.2	第2级及以上		明确每类接口的使用安全限制并进行管控，如远程连接等被限制使用的功能和权限、可操作的资源范围等	经营分析系统	是否明确每类接口的使用安全限制并进行管控，如远程连接等被限制使用的功能和权限、可操作的资源范围等？		是	见相关附件
2.6.1	第1级及以上	经营分析系统 -多租户管理	应支持租户间大数据服务隔离和数据隔离	经营分析系统	是否支持租户间大数据服务隔离和数据隔离？		是	离和数据隔离（见截图）
2.6.2			应支持租户间计算资源隔离，限制超配额的使用计算资源，并限制未授权访问	经营分析系统	是否支持租户间计算资源隔离，限制超配额的使用计算资源，并限制未授权访问？		是	租户间计算资源隔离，进行并发数限制
2.6.3	第2级及以上		应支持租户数据剩余信息保护及租户数据物理清除，确保租户数据存储的文件/对象删除后，租户数据无法恢复	经营分析系统	是否支持租户数据剩余信息保护及租户数据物理清除，确保租户数据存储的文件/对象删除后，租户数据无法恢复？		是	见截图
3.1.1	第1级及以上		应定义采集数据目的和用途，明确数据采集源和采集数据范围	经营分析系统	是否定义采集数据目的和用途，明确数据采集源和采集数据范围？		是	采集数据目的和用途，明确数据采集源和采集数据范围见接口规范（见相关文档）
3.1.2			应确保数据采集是与其大数据服务相关，且只采集满足业务所需的最小数据集	经营分析系统	是否确保数据采集是与其大数据服务相关，且只采集满足业务所需的最小数据集？		是	通过建立最小权度逻辑模型，物化到物理模型，通过加工作业采集入库（见截图）
3.1.3			应根据数据分类分级策略，进行数据分类分级标识	经营分析系统	是否根据数据分类分级策略，进行数据分类分级标识？		是	见相关文档
3.1.4			应制定数据清洗和转换过程中敏感数据安全管理规范	经营分析系统	是否制定数据清洗和转换过程中敏感数据安全管理规范？		是	见相关附件

3.1.5	第2级及以上	经营分析系统 -数据采集	采集个人信息过程中应获得本人的授权	经营分析系统	采集个人信息过程中是否获得本人的授权?		是	经分系统采集流量数据需通过ftp进行身份验证，验证通过后访问授权目录（见截图）
3.1.6			应采取加密、脱敏等防护措施对采集过程中的敏感数据进行保护	经营分析系统	是否采取加密、脱敏等防护措施对采集过程中的敏感数据进行保护?		是	采集过程中的敏感数据进行加密处理（见截图）
3.1.7			应采取必要的技术手段，对采集到的数据进行完整性和一致性校验	经营分析系统	是否采取必要的技术手段，对采集到的数据进行完整性和一致性校验?		是	采集到的数据进行校验处理，保障数据完整性及一致性（见截图）
3.1.8			应按照数据分类分级策略对收集数据进行分类分级标识	经营分析系统	是否按照数据分类分级策略对收集数据进行分类分级标识?		是	见相关文档
3.1.9			应记录并保存数据清洗和转换过程中敏感数据的操作过程	经营分析系统	是否记录并保存数据清洗和转换过程中敏感数据的操作过程?		是	加工敏感数据技术手段及加工过程日志（见截图）
3.1.10			应建立不同数据源和不同安全域之间数据加载安全策略、加载方式和授权规范	经营分析系统	是否建立不同数据源和不同安全域之间数据加载安全策略、加载方式和授权规范?		是	建立不同数据源，根据租户分配不同的资源权限（见截图）
3.2.1	第1级及以上	经营分析系统 -数据传输	应依据安全域内、安全域间、跨境传输等不同的数据传输场景建立相应的安全控制措施，保证数据传输的机密性和完整性	经营分析系统	是否依据安全域内、安全域间、跨境传输等不同的数据传输场景建立相应的安全控制措施，保证数据传输的机密性和完整性?		是	见附件3.1.1 接口规范
3.2.2	第2级及以上		建立数据传输的安全技术管控措施，并对密钥使用、通道安全配置、密码算法选择、传输协议开级等技术管控措施进行审批及记录	经营分析系统	是否建立数据传输的安全技术管控措施，并对密钥使用、通道安全配置、密码算法选择、传输协议开级等技术管控措施进行审批及记录?		是	见附件接口传输部分
3.2.3			应在构建传输通道前对两端主体身份进行鉴别，并定期进行重新认证	经营分析系统	是否在构建传输通道前对两端主体身份进行鉴别，并定期进行重新认证?		是	见附件3.1.1 接口规范
3.3.1	第1级及以上	经营分析系统 -数据存储	应提供配置数据、用户信息等数据的本地数据备份与恢复功能	经营分析系统	应提供配置数据、用户信息等数据的本地数据备份与恢复功能		是	见附件
3.3.2	第2级及以上		采用必要的技术或管控措施保证数据存储完整性和多副本一致性	经营分析系统	采用必要的技术或管控措施保证数据存储完整性和多副本一致性		是	经营分析系统 采用分布式存储进行保证数据存储完整性和多副本一致性（见截图）
3.3.3			应具备数据分布式存储安全管理能力，满足数据存储完整性和机密性保护要求	经营分析系统	是否具备数据分布式存储安全管理能力，满足数据存储完整性和机密性保护要求?		是	数据采用分布式存储，满足数据存储完整性和机密性保护要求（见截图）
3.4.1	第1级及以上	经营分析系统 -数据共享	应提供共享组件的双向身份认证机制	经营分析系统	是否提供共享组件的双向身份认证机制?		不适用	经分系统不涉及数据共享
3.4.2	第2级及以上		应提供最小化共享数据集	经营分析系统	是否提供最小化共享数据集?		不适用	经分系统不涉及数据共享

3.5.1	第1级及以上	经营分析系统 -数据归档与销毁	应提供数据销毁机制，明确销毁方式和销毁要求	经营分析系统	是否提供数据销毁机制，明确销毁方式和销毁要求?		是	根据大数据建设规范生命周期管理，详单类留
3.5.2	第2级及以上		依据介质存储内容的重要性确定销毁要求，建立磁介质、光介质和半导体介质的销毁处理方法和机制	经营分析系统	是否依据介质存储内容的重要性确定销毁要求，建立磁介质、光介质和半导体介质的销毁处理方法和机制?		是	经分系统服务器由系统至统一管理，不涉及介质销毁
3.5.3			对用户访问归档数据的权限进行控制，确保归档数据安全	经营分析系统	是否对用户访问归档数据的权限进行控制，确保归档数据安全?		是	集群下线将人员权限设置为已失效状态（见截图）
3.5.4			数据整体迁移的过程中，应杜绝数据残留	经营分析系统	数据整体迁移的过程中，是否杜绝数据残留?		是	数据整体迁移后，填写申请单进行库表清除
3.6.1	第1级及以上	经营分析系统 -数据分类分级	应根据数据类型或重要性等原则制定数据分类分级策略或规程	经营分析系统	是否根据数据类型或重要性等原则制定数据分类分级策略或规程?		是	见相关文档
3.6.2			应根据数据分类分级情况，建立数据资源清单	经营分析系统	是否根据数据分类分级情况，建立数据资源清单?		是	见相关文档
3.6.3			应根据数据分类分级情况，制定数据安全管理策略	经营分析系统	是否根据数据分类分级情况，制定数据安全管理策略?		是	见相关附件
3.7.1	第1级及以上	经营分析系统 -数据脱敏	应建立数据脱敏规范和制度，明确需要使用脱敏处理的场景，并依据场景确定数据脱敏规则、脱敏方法等内容	经营分析系统	是否建立数据脱敏规范和制度，明确需要使用脱敏处理的场景，并依据场景确定数据脱敏规则、脱敏方法等内容?		是	见相关附件
3.7.2	第2级及以上		应采用动态脱敏等技术措施对数据处理过程中的敏感数据进行保护	经营分析系统	是否采用动态脱敏等技术措施对数据处理过程中的敏感数据进行保护?		是	对于涉敏报表，采用金库模式这种动态脱敏进行法网（见截图）
3.7.3			应能对数据进行静态脱敏和去标识化处理	经营分析系统	是否能对数据进行静态脱敏和去标识化处理?		是	对数据进行静态脱敏和去标识化处理（见截
3.7.4			应能针对不同用户和不同敏感数据根据需求设置不同的脱敏算法	经营分析系统	是否能针对不同用户和不同敏感数据根据需求设置不同的脱敏算法?		是	见相关文档
3.8.1	第1级及以上	经营分析系统 -数据导入导出	应对请求导入数据的终端、用户或导入服务组件进行身份鉴别	经营分析系统	是否对请求导入数据的终端、用户或导入服务组件进行身份鉴别?		是	经营分析系统 统一纳入4A管控，导入操作需登录接口机通过4A金库
3.8.2			对请求导出数据的终端、用户或导出服务组件进行身份鉴别	经营分析系统	是否对请求导出数据的终端、用户或导出服务组件进行身份鉴别?		是	经营分析系统 统一纳入4A管控，导出操作需
3.8.3	第2级及以上		应采用数据通道加密等技术措施，保证数据安全导入	经营分析系统	是否采用数据通道加密等技术措施，保证数据安全导入?		是	接口文件在主机进行入库操作（见截图）
3.8.4			数据导出通道应具备数据加密等数据安全保护能力	经营分析系统	数据导出通道是否具备数据加密等数据安全保护能力?		是	接口文件在主机进行库操作（见截图）
3.8.5			应能验证导出数据的完整性和可用性，并在使用结束后销毁导出缓冲区中的数据	经营分析系统	是否能验证导出数据的完整性和可用性，并在使用结束后销毁导出缓冲区中的数据?		是	经营分析系统 为分布式数据库，无缓存数据（见截图）
3.9.1	第2级及以上	经营分析系统 -元数据管理	应对元数据的访问、修改及删除等操作设置权限管理	经营分析系统	是否对元数据的访问、修改及删除等操作设置权限管理?		是	使用集团产品对元数据进行管理维护，分角色设置管理权限
4.1.1	第1级及以上	经营分析系统 -安全管理制度	应建立覆盖数据采集、传输、存储、处理、共享、销毁全生命周期的数据安全管理制度	经营分析系统	是否建立覆盖数据采集、传输、存储、处理、共享、销毁全生命周期的数据安全管理制度?		是	见相关文档

4.2.1	第1级及以上	经营分析系统 -安全管理机构和人员	应设立数据安全管理机构和人员，并定义机构和岗位职责	经营分析系统	是否设立数据安全管理机构和人员，并定义机构和岗位职责?		是	见截图
4.2.2	第2级及以上		制定大数据服务安全岗位人员的安全培训计划	经营分析系统	是否制定大数据服务安全岗位人员的安全培训计划?		是	见截图
4.2.3			按计划对相关人员开展安全培训，包括政策、法律、法规、标准等合规性培训，并对培训结果进行评价、记录和归档	经营分析系统	是否按计划对相关人员开展安全培训，包括政策、法律、法规、标准等合规性培训，并对培训结果进行评价、记录和归档?		是	见截图
4.3.1	第1级及以上	经营分析系统 -系统建设管理	应与选定的服务供应商签订与安全相关的协议，明确整个服务供应链各方需履行的网络安全相关义务	经营分析系统	是否与选定的服务供应商签订与安全相关的协议，明确整个服务供应链各方需履行的网络安全相关义务?		是	见附件
4.3.2	第2级及以上		经营分析系统 应开放接口，允许第三方安全产品接入，支持异构方式对经营分析系统 的网络、主机、应用、数据层的安全措施进行实施	经营分析系统	经营分析系统 是否开放接口，允许第三方安全产品接入，支持异构方式对经营分析系统 的网络、主机、应用、数据层的安全措施进行实施?		不适用	经营分析系统 主机、数据库由集团统一管控
4.3.3			在测试验收阶段，应验证或评估经营分析系统 所提供的安全措施的有效性	经营分析系统	在测试验收阶段，应验证或评估经营分析系统 所提供的安全措施的有效性		是	测试检查项，验证经营分析系统 所提供的安全措施的有效性（见相关文档）
4.3.4			应根据经营分析系统 的安全保护等级选择能够提供相应安全等级保护能力的服务商	经营分析系统	应根据经营分析系统 的安全保护等级选择能够提供相应安全等级保护能力的服务商		是	见大数据安全保护部分（见相关附件）
4.3.5			应以书面方式约定经营分析系统 的各项服务内容和具体技术指标	经营分析系统	应以书面方式约定经营分析系统 的各项服务内容和具体技术指标		是	见相关文档
4.4.1	第1级及以上	经营分析系统 -安全运维管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补	经营分析系统	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补		是	见相关文档
4.4.2	第2级及以上		应将经营分析系统 系统、设备等纳入资产管理	经营分析系统	应将经营分析系统 系统、设备等纳入资产管理		是	经分经营分析系统 已纳入4A管理（见截图）
4.4.3			应制定并实施系统配置管理规程，建立系统配置管理组织结构，明确配置管理人员的角色和职责	经营分析系统	应制定并实施系统配置管理规程，建立系统配置管理组织结构，明确配置管理人员的角色和职责		是	见截图
4.4.4			制定日常配置检查内容清单，并按照最小特权原则对经营分析系统 进行安全配置	经营分析系统	制定日常配置检查内容清单，并按照最小特权原则对经营分析系统 进行安全配置		是	见相关文档
4.4.5			应建立补丁管理规程，至包括下载、测试、分析、分发、安装、归档等流程和内容，确保系统补丁的规范化管理	经营分析系统	应建立补丁管理规程，至包括下载、测试、分析、分发、安装、归档等流程和内容，确保系统补丁的规范化管理		是	见相关文档
4.4.6			应对用户访问经营分析系统 的关键操作进行日志记录	经营分析系统	应对用户访问经营分析系统 的关键操作进行日志记录		是	同重要报表进行操作日志记录（见截图）
4.4.7			日志记录的具体内容应包括，操作时间、操作账号、客户端 IP、服务器 IP、操作类型、操作名称、操作内容、操作结果等信息	经营分析系统	日志记录的具体内容应包括，操作时间、操作账号、客户端 IP、服务器 IP、操作类型、操作名称、操作内容、操作结果等信息		是	见截图
4.4.8			应制定安全审计策略，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计	经营分析系统	应制定安全审计策略，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计		是	安全审计策略见审计报告（见相关文档）
4.4.9			审计记录应包括事件的日期和时间、用户、事件类型、事件结果及其他与审计相关的信息	经营分析系统	审计记录应包括事件的日期和时间、用户、事件类型、事件结果及其他与审计相关的信息		是	审计记录见审计报告(见相关文档)
4.5.1	第1级及以上	经营分析系统 -安全事件管理	应建立并实施安全事件预警通报制度，及时向大数据服务安全管理部门报告相关安全事件，并根据预案实施应急措施	经营分析系统	应建立并实施安全事件预警通报制度，及时向大数据服务安全管理部门报告相关安全事件，并根据预案实施应急措施		是	见相关文档
4.5.2			应建立专门负责应急响应的组织，负责收集安全事件相关信息，并传递给相应的团队进行处理	经营分析系统	应建立专门负责应急响应的组织，负责收集安全事件相关信息，并传递给相应的团队进行处理		是	故障诀策小组通过微信群进行应急沟通（见截图）
4.5.3	第2级及以上		建立安全事件预警和应急处置规程，确保安全事件预警预防、应急保障准备、应急响应和跟踪总结	经营分析系统	建立安全事件预警和应急处置规程，确保安全事件预警预防、应急保障准备、应急响应和跟踪总结		是	见相关文档
5.1.1	第1级及以上	经营分析系统 -第三方服务提供安全	应确保安全服务商的选择符合国家的有关规定；	经营分析系统	是否将通过中国通信企业协会通信网络安全服务能力评定列为外部安全服务提供商招标条件之一?		是	满足