通信网络安全	护符合性過	例表-经营分析	系统					
	1、本表为通信网络	8安全防护达标检查表经:	苦分析系统 部分,适用于经普分析系统 相关安全防护定级对象的	9企业安全自查,及主管部门或其他机构	为开展的安全达标评测。			•
填写说明	2。未是根灰在青净转载(VOT 3600-2020 电信仰电互照例还分析系统 安全指护更求)、(VOT 4687-2022 电信列和互联网经符分析系统 安全辩护检测更求)及(VOT 2689 第三方安全服务能力评 定期》 转定。 3、未食曲机定应对参阅所属单位对"、特个定数对常和等一份。 4、未是相求成金达法情况服分租农净有效与适比。当"未定规项程"数值不为4时,表示未来中压有位查项目未完成。							
	4、本表填写状态及 5、本表检查项目音	及达标情况部分相关内容; 邓分"检查结果"应根据各样						
检查项目	e.							
序号 1.1.1	超用推開 第1級及以上	检查类型 经营分析系统 -物理安	検査内容 应満足YD/T 1754中的要求	近用网络属性 经营分析系统 の動へに変統	検査点 是否満足YD/T 1754中的要求?	备注	答案 是	答案说明
1.2.1	第1级及以上		应绘制与当前运行情况相符的网络拓扑结构图 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	经营分析系统 经营分析系统	是否绘制与当前运行情况相符的网络拓扑结构图? 是否实现网络安全域划分,经营分析系统 与外部系统之		北	児附件 児附件
1.2.3			火墙进行隔离和访问控制 应定期对网络进行安全检查和审计	经营分析系统	同使用防火墙进行隔离和访问控制? 是否定期对网络进行安全检查和审计?		是	光附件 見附件
1.2.4		经营分析系统 -网络安 全	应及时修补漏洞, 杜绝弱口令 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开	经营分析系统	是否及时修补漏洞, 杜绝别口令? 是否对恶意代码进行检测和清除, 并维护恶意代码防护机		是	見附件
1.2.5	第2级及以上	-	銀 和 明 報	经营分析系统	海的升级和更新?		是	見附件
1.2.6			底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	是否監視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?		北	見附件
1.3.1			应对登录操作系统的用户进行身份标识和鉴别 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	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? 操作系统是否遵循最小安装的原则, 仅安装需要的组件和		是	见附件
1.3.2	第1級及以上		序	经营分析系统	应用程序?		是	見附件
1.3.4			应关闭不必要的端口,保持端口服务最小化 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 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? 是否安装防恶意代码软件,并定期进行升级和更新防恶意		是	見附件 見附件
		经背分析系统 -主机安 全	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		代码库? 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			
1.3.5	第2级及以上		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 不符合項	经营分析系统	同件、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	見附件
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?		北	見附件
1.4.1	第1級及以上		应支持虚拟机之间、虚拟机与宿主机之间的隔离 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	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? 是否在虚拟化网络边界部署访问控制机制,以实现网络的		不适用	经营分析系统没有云服 经营分析系统没有云服
1.4.2	30.0000742		商	经营分析系统	安全隔离?		不适用	务器
1.4.3		www.reser -w.c.	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		经营分析系统 -云平台 安全	应支持对虚拟机能器性进行检测的能力	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	经普分析系统没有云服 务器
1.4.5	第2级及以上		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	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		不适用	经营分析系统没有云服 务器
1.4.6			制 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	安全访问控制? 是否能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异		不适用	经营分析系统没有云服
1.4.0			放送的なのの世界は10人の一般では、10人が10人の10人が10人の10人が10人の10人が10人の10人が10人が10人が10人が10人が10人が10人が10人が10人が10人が	经具力机 MANG	常流量?		小油用	务器
2.1.1			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(见裁图)
2.1.2	第1级及以上	終皆分析系统 -身份管 理	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?		北	重复账号不满足唯一性 校验,无法创建(兇截 图) 用户从账号作为唯一
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	/// / / / / / / / / / / / / / / / / /
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	当进行过程管理时,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,无需逃程管理(见 截图)
2.2.1			帐号的分配应经过审批 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	经营分析系统 经营分析系统	帐号的分配是否经过审批? 是否指定专门的部门或人员进行账户管理。对申请账户、		是	見相关文档 统一有管理员进行账
2.2.3	第1级及以上		户、删除账户等进行控制 应及时删除或停用多余的、过期的帐号	经营分析系统	建立账户、删除账户等进行控制? 是否及时删除或停用多余的、过期的帐号?		是	号管理(见截图) 对过期账号进行 加锁和删除(见截
2.2.0		经营分析系统 - 账号管 理	125.0X 10 20 20 40 17 17 20 20 17 17 20 20 20 20 20 20 20 20 20 20 20 20 20	STEEN ALVON	SELECTION OF STATES AND ASSESSMENT OF STATES ASSESSMENT ASSESSMENT ASSESSMENT ASSESSMENT ASSE		/L	图) 无多人共享账号,对
2.2.4			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	从账号进行细粒度 授权,日志由4A统一 管拉(见截图)
2.2.5	第2级及以上		系统维护交接时, 嵩对开发、建设过程中设置的帐号进行检查, 删除不必要的帐号, 嵩要继续使用的帐号, 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,员工转尚需要修改账号角色	经营分析系统	员工离职是否回收帐号,员工转尚是否修改账号角色?		北	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,在一定时间数暂停该帐号登录	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		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
2.3.2				经营分析系统	哲停该帐号登录?		n	入(見載图) 默认账户已被锁定。
2.5.2			应避免使用默认口令	SE具力例 SEND	是否避免使用默认口令?		龙	(见截图)
		经营分析系统 -口令管						经分系统已全部纳入4A
2.3.3	第2級及以上	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	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
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 明立?		是	文档》 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	经营分析系统	明文? 帐号口令保存在文件中时,是否改为不可读文件、并控制 立此口维基型层阅读设备?		A.	官理,4A平点登录系统 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		能是对应程序访问 应对经营分析系统 用户(内部管理人员、租户、应用等) 进行	经营分析系统	文件只能是对应程序访问? 是否对经营分析系统 用户(内部管理人员、租户、应用 (数) 进行证证 例如主题和证证证		是	管理。本存储明文密码 通过4A单点登录,见附
2.4.2	第2級及以上	经营分析系统 -访问控 制	认证,避免未授权访问 权限分配应支持最小授权原则	经营分析系统	等) 进行认证,避免未授权访问? 权限分配是否支持最小授权原则?		是	构建角色权限矩阵,见
2.4.3		411		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		是	附件 构建角色权限矩阵,见
2.5.1	第1级及以上	经营分析系统 -接口安	应对接口实施安全控制措施,如身份鉴别、访问控制、签名、	经营分析系统	的权限? 是否对接口实施安全控制措施,如身份鉴别、访问控制、 签名 财间额和宏介地位?		是	附件 見相关附件
	第2级及以上	经营分析系统 -接口安 全	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	经营分析系统	签名、时间戳和安全协议? 是否明确每类接口的使用安全限制并进行管控,如远程连 体体被阻制使用的系统和规则。可操作的系统使用等。		是	見相关附件
2.6.1			制使用的功能和权限、可操作的资源范围等 应支持租户间大数据服务隔离和数据隔离	经营分析系统	接等被限制使用的功能和权限、可操作的资源范围等? 是否支持租户间大数据服务隔离和数据隔离?		A.	高和数据隔离(见截
2.6.2	第1级及以上	经营分析系统 -多租户 管理	应支持租户同计算资源隔离,限制超配额的使用计算资源,并	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		g.	图) 租户间计算资源隔
2.6.3	第2級及以上		限制未授权访问 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	源,并限制未授权访问? 具否支持和户数据剩金信息保护及和户数据物理洁路、确		是	高,进行并发数限制 见截图
3.1.1	2010年以下1		数据存储的文件/对象删除后,租户数据无法恢复 施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	保租户数据存储的文件对象删除后。租户数据无法恢复? 是否定义采集数据目的和用途,明确数据采集源和采集数 振荡闻?		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
	第1級及以上		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	COMMUNICATION OF	是否确保数据采集是与其大数据服务相关,且只采集满足			口 規 憨 ( 見 相 美 文 档) 通过建立最小粒度逻辑 模型,物化到物理模
3.1.2			需的最小数据集 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 经营分析系统	业务所需的最小数据集? 是否根据数据分类分级策略,进行数据分类分级标识?		是是	模型,物化到物理模型,通过加工作业采集 入库(见截图) 见相关文档
3.1.4			应制定数据消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	見相关附件

3.1.5 3.1.6 3.1.7 \$\text{\$\tint{\$\text{\$\exititt{\$\text{\$\text{\$\text{\$\text{\$\}}}}\$\text{\$\texitt{\$\text{\$\text{\$\text{\$\text{\$\text{\$\text{\$\text{\$\text{\$\text{\$\	上 经款分析系统 数据传输 数据传输		经置分析系统 经置分析系统 经置分析系统 经置分析系统 经置分析系统 经置分析系统	采集个人信息过程中提高获得本人的授权? 最后等规则感,脱脓等防护指统对某型过程中的散磨数据 进行保护? 是占等规必要的技术手段,对采集制的数据进行完整性和一致性检验? 是占防阀数据分类分级集局对收集数据进行分类分级标 行行。 是占防阀数据分类分级集局对条数据进行分类分级标 行行。 是市场不同被服务和不同安全域之间数据加载安全策略 力能为实在规模规范。 是市场的发展形成,对于原场的现在 对于原场的发展的发展,对于原场的现在 或据的发展的发展,对于原场的现在 或据的发展的发展,对于原场的现在 或据的发展的发展,对于原场的现在 或据的发展的发展,对于原场的现在 或据的发展的发展,对于原场的发展的	是 是 是	於分系於來集流量 指新過程作到 行身的學述。樂記通 行身的學述。樂記通 行身的學述。樂記通 (见魏四 (明朝) 東東東 (明明) 東東 (明明) 東東 (明明) 東東 (明明) 東東 (明明) 東東 (明明) 東東 (明明) 東東 (明明) 東東 (東東 (明明) 東東 (東東 (東東 (東東 (東東 (東東 (東東 (東東 (東東 (東東
3.1.7 第2級3 3.1.8 3.1.9 3.1.10 第1級35 3.2.1 第1級35 3.2.2 第2級3 3.3.1 第1級35 3.3.2 第2級3	生 经票分析系统 数据传输 数据传输 数据传统 数据传统 数据传统 数据传统 数据传统 数据传统 医二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十	戶 应平配必要的技术手段,对果集制的数据进行完整性和一截性 转接 应该期数据分类分级策略对收集数据进行分类分级标识 他记录并保存数据器体和转换过程中或感数据的操作过程 由建立不同感阻器和不同安全域之间使跟印度全全策略。 加极 方式巩膜吸滤器 建立体器综合全线和,安全线面。跨域的全体等处全线和,加坡 之实现象的操作,保收数据的编的现在和实现转 建立就器件编的安全技术整约服务,并对密则使用,通路安全 危度。在时间还是有效的	经查分析系统 经查分析系统 经查分析系统 经查分析系统 经查分析系统	語行場內?  思古等單必能的技术手段,对采集例的被提出行完整性和 更性的验?  是古版制数据分类分级结整对或集数部进行分类分级标识? 是古记录并保存数据流和转线过程中帧频数据的操作过程?  思古说不可被照婚和不同安全域之间数据加载安全策略,加载方式和假权规据?  是古能力或组织的安全性规制度。库证数据的编码地位特别的概念性,在完整定量值的安全性规制度。在数据的编码地位并完整度是是一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一	是是	采集过程中的敏感型 级超别 数别 实验处理。保障数据进行校 等处理。保障数据处 图) 见相关之间 见相关之间 (见截阳) 数据进行之报 (见数阳) 数据进行之报 (见数阳) 数据测,根 使 近立不同数据测,根 数据性产分配不同的资 数据使一分配不同的资 数据使一分配不同的资
3.1.8 3.1.9 3.1.10 3.2.1 第1度以 3.2.2 第2度 3.2.3 3.3.1 第1度及 3.3.2	上 经款分析系统 数据传输 数据传输	於論 直接網數据分类分單角層对收集數据进行分类分類标识 並记述并保存數据高為和核他过程中物應數据的操作过程 底建立不同數据認和不同安全域之间数据加键安全策略。加载 方式加度级認 症核接安全域用,安全域间,跨域将破碎不同的数据传输码 建立能高的安全分型相振。保定数据的编码则是常和完整性 地立能器符略的全点扩展等组制。并对数据使用,黑路全全 强度。常等描法速度,传输协议计划等使用,黑路全 发起。常等描法速度,传输协议计划等使用,黑路全 在在标准传输通循环对概主往身带进行需别,并交取进行重 就以正 加程中	经查分析系统 经查分析系统 经查分析系统 经查分析系统	一效性給2 是击距离数据分类分级重整对效重数逐进行分类分级标 1572 是书记与并保存效整着汽车机构过程中物质数据的操作过 程2 是告建立不同数据源和不同安全域之间数据则联安全策略 从据接方式间接规则2 是各线数金金线。交全域间,跨域价值等不同的数据价 输场器单位组织的安全控制器。保证数据价值的现象性 和完整在2 是否整效数据价值的安全技术管控组像,并对密则使用, 是否整数数据价值的安全技术管控组像,并对密则使用, 是否整数数据价值的安全技术管控组像,并对密则使用。	是是	来集到的數据进行校 發效理,保障數据提 數性及一致性(见截 图) 见相关较越据技术手 (及及加工过程日志 (足裁图) 建立不同数据源。根 被担价的资 源权限(見截图)
3.1.9 3.1.10 3.2.1 第1級法 3.2.2 第2級 3.2.3 3.3.1 第1级法 3.3.2	经营分析系统。数据传输 数据传输 经营分析系统。数据传输	能记录并保存数据源块和转换设理中或感数据的操作过程 相宜以不用感性服务和平向安全域之间被据的接受全情感。加税 方式和膜收规范 直线接受金梯机。安全域间、跨槽均缘等不同的复数性结构器 建立施的综合全线相信。保收数据等的编序则是有机构等 建立就图计编码的全线性器,保收数据等的编序则是有机构等 建立就图计编的安全技术整约图像,并对密钥使用、通路安全 配置、密等确定组织、传输的公开吸导技术探控指施进行审批 互汇规 定在环境等通道解对两端主体身份进行图例,开发驱进行国 然记证 加强的人工程等。	经置分析系统 经置分析系统 经置分析系统	197 是否记录并保存数据高机和体验过程中物质数据的操作过程。 即否能 2 不可被据源和不同安全域之间数据加载安全策略 10%方式和假安规范? 是否能要安全域内,安全域间。跨峰传输等不同的数据传 输给理查对组织的安全控制器值。海运数据传输的规定 和示规程? 是否主义数据传输分全专术常控组版,将运数据传输的规定 是否主义数据传输分全专术《管控组版,并对密明使用, 测量全金混用。密码等法选择、传统协议开始等本有管	是是	图) 见相关文档 加工敏感数据技术手 段及加工过程日志 (见载图) 建立不同数据源。根 据租户分配不同的资 源权限(见载图)
3.1.10 3.2.1 第1模型: 3.2.2 第2模型 3.2.3 3.3.1 第1模型: 3.3.2 第2模型	经营分析系统。数据传输 数据传输 经营分析系统。数据传输	超建以不测能提展外不同分全域之间数据机器安全策略。 加坡 方式机理收规范 应依据安全域列,安全域间,跨域价值等的运作地场梯 建立组配价分全位物组施。但或数据价值的现在针机完格 建立就配价值的安全技术整控组施,并对您明使用,通道安全 配置,就可能无效率。传输的公开吸令技术就对指地还行命机 及正规 加速的发展,传输的公开吸令技术就对指地还行命机 是正规程序的通道解对两线主体身份进行虚例,开观现近行重 就以 加速存在规模的对象。	经营分析系统 经营分析系统 经营分析系统	是否证明并保存效率流流和转换过程;中帧频数据的编作过程? 程? 显示建立不同数据原和不同安全域之间数据的联安全策略, 加坡五方式组接处规范? 显示核键安全组织。安全城间,跨峰标编等不同的数据传 编场理业馆组的安全的明确值。保证数据传输的规定 报示整理? 思古建立数据传输的安全技术管控组版,并对密则使用, 是随坐全台流,是可解决进程,传统的又对接受技术管理	足	段及加工过程日志 (见截图) 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模以 3.2.2 第2模 3.2.3 3.3.1 第1模以 3.3.2 第2模以	经营分析系统。数据传输 数据传输 经营分析系统。数据传输	方式加度规范 直接联合合体,安全接向、跨域物等不同的数据性构态度 建立指面的安全技术器性用。 (学数据价值的规定性和完整性 建立截据代值的安全技术器控措施,并对您的使用、温面安全 危期、常等制法型。 (特别及订单等技术器控措施进行审批 及正式物准性物通道的对构理主体身份进行重加,开定则进行重 新见证 加度的最重点。用户信息等数据的本地数据备的与恢复功能	经實分析系统 经實分析系统	显击维义不同数据源和不同安全域之间数据加较安全策略 ,加载方式和报权规范? 是否核赛安全城内、安全城间、跨域价值等不同的数据价 纳尔曼维立机脉的安全控制阻衡,保证数据价值的制度性 和完整性? 是否维立效据价值的安全技术管控阻衡,并对密明使用, 通避全会混浑。密明解法选择、作场协议开级等技术管位		(见截图) 建立不同数据源,根据租户分配不同的资源权限(见截图)
32.1 第1度以 32.2 第2度 32.3 33.1 第1度及 33.2 第2度J	经营分析系统。数据传输 数据传输 经营分析系统。数据传输	方式加度规范 直接联合合体,安全接向、跨域物等不同的数据性构态度 建立指面的安全技术器性用。 (学数据价值的规定性和完整性 建立截据代值的安全技术器控措施,并对您的使用、温面安全 危期、常等制法型。 (特别及订单等技术器控措施进行审批 及正式物准性物通道的对构理主体身份进行重加,开定则进行重 新见证 加度的最重点。用户信息等数据的本地数据备的与恢复功能	经實分析系统 经實分析系统	是否依据安全域内、安全域间、跨域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。 通道安全能宜、密码算法选择、传输协议升级等技术管控		源权限 (見截图)
3.2.2 第2級 3.2.3 3.3.1 第1級以 3.3.2 第2級 3.2.0 第2級 3.3.2	经营分析系统。数据传输 数据传输 经营分析系统。数据传输	建立性病形含全种物组织。保全数据价值的现实也沉淀物件 建立数据价值的安全技术整例细胞。并对您则使用、通路安全 充强、密等调法进程、价值的公开模型技术整例细胞进行组织 及记录 应在分量价值通明对构建主体身份进行鉴别,开定输进行重 新以证 起程仍在图数据、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	输场侧建立相应的安全控制措施,保证数据传输的制定性 和完整性? 是否建立数据传输的安全技术管控措施,并对密钥使用、 通道安全加度、密码算法选择、传输协议升级等技术管控	是	DI DYLOLO A A TONIO DE TE
第2級3 第2級3 第1級3以 第1級3以 第1級3以 第2級3	上 经营分析系统 - 数据存	配置。密切轉送起導、停輸协议升級等技术管控開施进行审批 及记录 应在构建传输通道前对两端主体身份进行强别,并定哪进行重 新认证 起提供在置数据、用户信息等数据的本地数据备份与恢复功能		通道安全配置、密码算法选择、传输协议升级等技术管控		元nift3.1.1 按口规范
3.3.1 第1级及3	经营分析系统 数据存	新认证 或提供配置数据、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	是否在构建传输诵道前对两端主体身份进行鉴别,并定期	是	见附件接口传输部分
3.3.2 第2級	经营分析系统 数据存		A CONTRACTOR OF THE CONTRACTOR	进行重新认证? 应提供配置数据、用户信息等数据的本地数据备份与恢复	是	见附件3.1.1 接口规范
第2級)	22		经营分析系统	功能	足	见附件 经营分析系统 采用分
		采用必要的技术或管控措施保证数据存储完整性和多	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	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)
		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	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	alg	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	E	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	是否提供数据销级机制,明确销级方式和销级要求?	足	根据大数据建设规范生 命周期管理,详单类留
3.5.2	经营分析系统 - 数据归	依据介质存储内容的重要性确定销级要求,建立磁介质、光介质和半导体介质的销级处理方法和机制	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级处理方法和机制?	足	经分系统服务器由系统 室统一管理,不涉及介
3.5.3 第2级2	pure-room	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
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	図) 数据整体迁移后,填写 申请单进行库表清除
3.6.1		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	見相关文档
3.6.2 第1級7	松丁 经营分析系统 - 数据分 类分级	应根据数据分类分级情况,建立数据资清单	经营分析系统	是否根据数据分类分级情况,建立数据资清单?	<b>원</b>	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級及以	Ŀ	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	经营分析系统 -数据脱	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
3.7.3 第2级》	WLL 敏	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	行法(2) (日 於四) 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?	足	見相关文档
3.8.1 第1級]	NUL	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?	R	经营分析系统 统一纳 入4A管拉,导入操作需 登录接口机通过4A金库
3.8.2	经营分析系统 -数据导	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	经官分析系统 统一纲 入4A管控,导出操作需
3.8.3	入号出	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 第2級]	RIXE	数据导出通道应具备数据加密等数据安全保护能力 应能验证导出数据的完整性和可用性,并在使用结束后销级导	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? 是否能验证导出数据的完整性和可用性,并在使用结束后	是	接口文件在主机进行库 操作(见截图) 经营分析系统 为分布
3.8.5		出缓冲区中的数据	经营分析系统	報题导出缓冲区中的数据?	是	式数据库,无缓存数据 (甲基因) 使用集团产品对元数据
3.9.1 第2級及以	M-7E	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)	と以上 经普分析系统 -安全管 理制度	应建立覆盖数据采集、传输、存储、处理、共享、销级全生命 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、销股 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級	EU.E	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 土。	是	见截图
4.2.2		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? 是否按计划对相关人员开展安全培训,包括政策、法律	足	见截图
4.2.3 第2級	ED.E.	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	、 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	k以上	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 应开放接口,允许第三方安全产品接入,支持异	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		构方式对经营分析系统 的网络、主机、应用、数据层的安全指 施进行实施		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 测试检查项,验证经营
4. 3. 3 第2级	经营分析系统 -系统建 设管理	施的有效性		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	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 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		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 应以书面方式约定经营分析系统 的各项服务内容和具体	是	见大数据安全保护部分 (见相关附件)
4.3.5	IN L	标 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	经营分析系统 经营分析系统	技术指标 应采取必要的措施识别安全漏洞和障患,对发现的安全漏	是	見相关文档
4.4.1 第1級7	GAT	隐患及时进行修补 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	洞和隐患及时进行修补 应将经营分析系统 系统、设备等纳入资产管理	是非	见相关文档 经分经普分析系统 己
4.4.3		应制少并完整系统影響使用提供 建立系统影響使用组织件	经营分析系统	应加少比少数系统影響的相提的 电立系统影響的相称和	AL.	納入4A管理(児蔵图) 児蔵图
4.4.4		构,明确配置管理人员的角色和职责 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	结构,明确配置管理人员的角色和职责 制定日常配置检查内容的单、并按照最小特权原则对经营 分析系统 排行完全配置	AL.	見相美文档
4.4.5	经营分析系统 -安全运	NOT ALLEY THE ME	经营分析系统	分析系统 进行安全配置 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	A.	見相美文楷
4.4.6 第2級	kU.L. 维管理	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	何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 IF、服务器 IP、操作类型、操作名称、操作内容、操作结果等信	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	是	见截图
4.4.8		息 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 外面要要公本事件并行业;	经营分析系统	作结果等信息 应制定安全审计策略,审计概差到每个用户,对重要的用	是	安全审计策略见审计报
4.4.9		为和重要安全事件进行审计 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	户行为和重要安全事件进行审计 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	告(見相关文格) 审计记录见审计报告(见 相关文档)
4.5.1		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	经营分析系统	市场来及共轭与平市和大的市局 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	足	和大文档) 見相关文档
第1級〕	及以上 经营分析系统 -安全事 件管理	曾理部门报告相关安全事件,并根据预案实施应急清施 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、并传递给相应的组队进行处理	经营分析系统	施 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	故障決策小组通过微信 群进行应急沟通(见截
4.5.3 第2級及以	.E	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、	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	是	图) 見相美文档
5.1.1 第1級及以	STANCHER WAS AN AN AN AN	应急保障准备、应急响应和跟踪总结 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	防、应急保障准备、应急响应和跟踪总结 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	満足