UCloud 优刻得云服务平台

等保三级报告关键页

1、云上等保 2.0 安全合规解决方案

UCloud 已完成 2020 年度等保三级测评，采用等保 2.0 最新标准，分数为 95.06 分（满分 100 分），评级为“优”，并向云客户公开透明的呈现等保三级报告关键页（见附件）。

等保 2.0 提出，云平台与云客户安全责任共担，双方均必须完成等保合规工作。UCloud 在满足自身合规的基础上，助力云客户等保合规，推出等保 2.0 安全合规解决方案（官网地址：https://www.ucloud.cn/site/active/djbh2.0.html）。

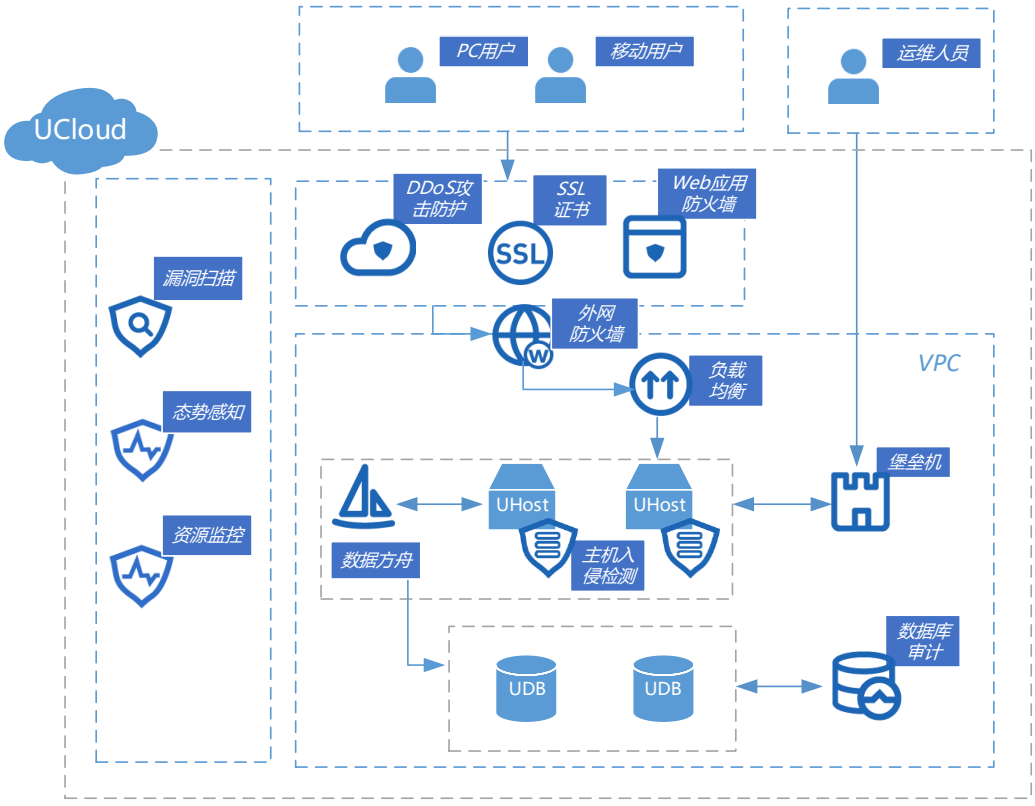
图：等保 2.0 安全合规解决方案架构

在解决方案中，UCloud 机房已满足安全物理环境要求。在技术层面，围绕等保 2.0“一个中心，三重防护”的基本要求，UCloud 为云客户提供满足等保三级/二级要求的安全产品。在管理层面，UCloud 合作全国多地的优质机构，为客户提供等保咨询及测评服务，从而帮助云客户一站式完成等保合规。

表：助力云客户建设等保 2.0“一个中心，三重防护”

一个中心 三重防护	安全产品服务	等保要求	二级 必选套餐	三级 必选套餐	三级 增强套餐
安全通信网络	外网防火墙+VPC	网络边界隔离，网络区域划分	√	√	√
	负载均衡	通信线路、关键网络设备冗余		√	√
安全区域边界	DDoS 攻击防护	应在关键网络节点处检测、防止或限制网络攻击行为			√
	WAF	应具有提供通信传输、边界防护、入侵防范等安全机制	√	√	√

一个中心 三重防护	安全产品服务	等保要求	二级 必选套餐	三级 必选套餐	三级 增强套餐
安全计算环境	Web 漏洞扫描	应能发现可能存在的已知漏洞			√
	SSL 证书	应保证数据传输完整性和保密性	√	√	√
	主机入侵检测	应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警	√	√	√
	堡垒机	应对用户进行身份鉴别、访问控制、安全审计		√	√
	数据库审计	应对数据库进行安全审计，对审计进程进行保护		√	√
	数据方舟	应提供重要数据的本地数据备份与恢复功能			√
安全管理中心	态势感知	应能对网络中发生的各类安全事件进行识别、报警和分析		√	√
	资源监控	应对设备的运行状况进行集中监测		√	√



图：UCloud 云安全产品架构图

2、UCloud 等保备案证及报告关键页

UCloud 云平台的等保备案证明由属地上海市公安局颁发，初次颁发为 2014 年，备案证长期有效。

信息系统安全等级保护

备案证明

依据《信息安全等级保护管理办法》的有关规定，优刻得科技股份有限公司单位的：

第三级云服务平台系统

予以备案。

证书编号：31001413020-00001

中华人民共和国公安部监制

备案公安机关公章

2014年06月05日

以下为 UCloud 云平台 2020 年等保测评报告关键页：

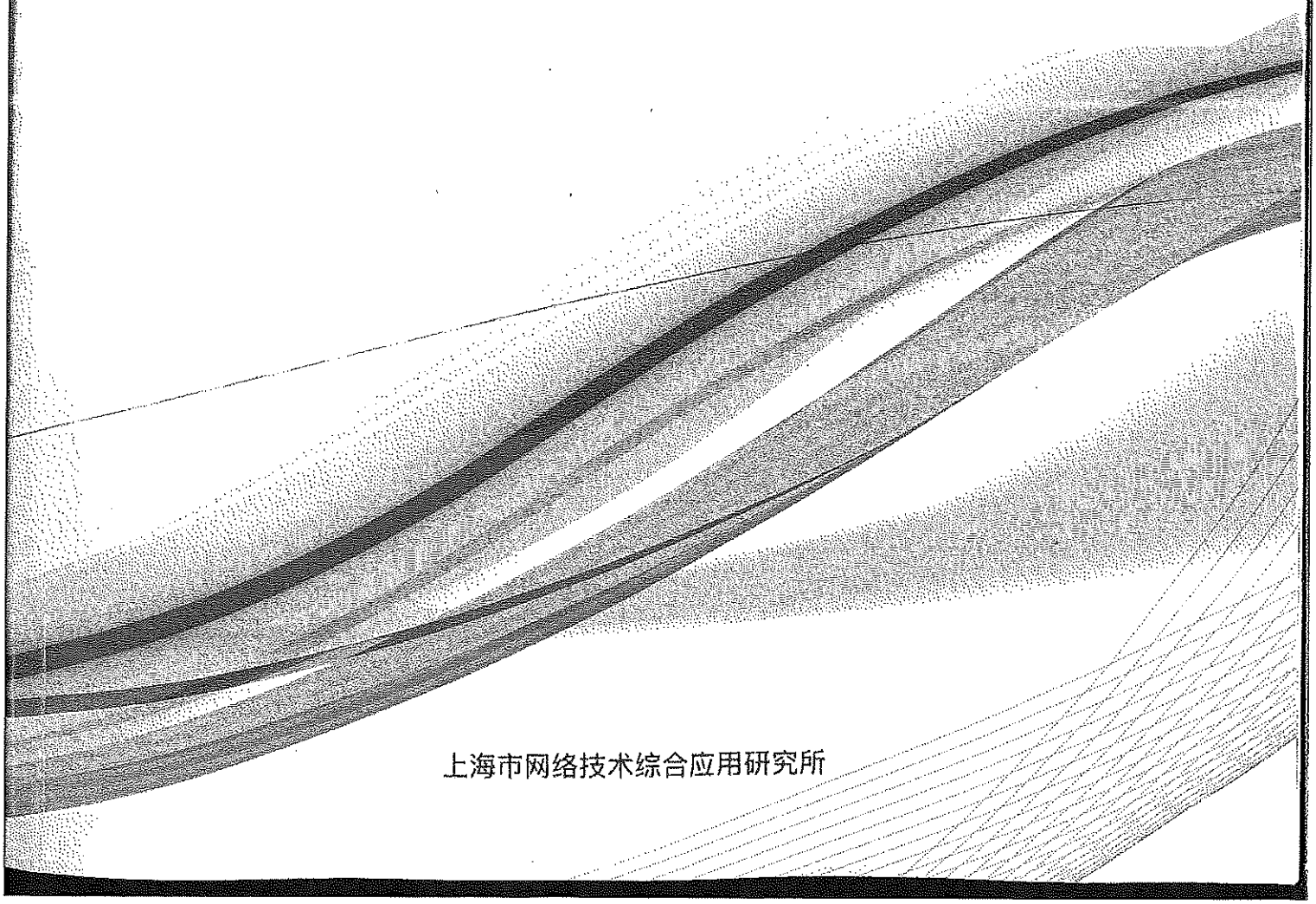
报告编号：31001413020-00001-20-310073-01

网络安全等级保护测评报告

系统名称：云服务平台

委托单位：优刻得科技股份有限公司

报告时间：2020年05月16日



上海市网络技术综合应用研究所

报告编号：31001413020-00001-20-310073-01

项目编号：SIANT-DB-20200210-082-01

网络安全等级保护
云服务平台等级测评报告

委托单位：优刻得科技股份有限公司

测评单位：上海市网络技术综合应用研究所

报告时间：2020 年 05 月 16 日

说明：

一、每个备案系统单独出具测评报告。

二、测评报告编号为四组数据。各组含义和编码规则如下：

第一组为系统备案表编号，由2段16位数字组成，可以从公安机关颁发的系统备案证明（或备案回执）上获得。第1段即备案证明编号的前11位（前6位为受理备案公安机关代码，后5位为受理备案的公安机关给出的备案单位的顺序编号）；第2段即备案证明编号的后5位（系统编号）。

第二组为年份，由2位数字组成。例如09代表2009年。

第三组为测评机构代码，由测评机构推荐证书编号最后六位数字组成。其中，前两位为省级行政区划数字代码的前两位或行业主管部门编号：00为公安部，11为北京，12为天津，13为河北，14为山西，15为内蒙古，21为辽宁，22为吉林，23为黑龙江，31为上海，32为江苏，33为浙江，34为安徽，35为福建，36为江西，37为山东，41为河南，42为湖北，43为湖南，44为广东，45为广西，46为海南，50为重庆，51为四川，52为贵州，53为云南，54为西藏，61为陕西，62为甘肃，63为青海，64为宁夏，65为新疆，66为新疆兵团。90为国防科工局，91为国家能源局，92为教育部。后四位为公安机关或行业主管部门推荐的测评机构顺序号。

第四组为本年度系统测评次数，由两位构成。例如02表示该系统本年度测评2次。

网络安全等级测评基本信息表

被测对象					
被测对象名称	云服务平台			安全保护等级	第三级（S3A3G3）
备案证明编号	31001413020-00001				
被测单位					
单位名称	优刻得科技股份有限公司				
单位地址	上海市杨浦区上海市杨浦区隆昌路 619 号 10 号楼 B 座			邮政编码	200090
联系人	姓名	杨丹	职务/职称	安全合规工程师	
	所属部门	安全中心	办公电话	021-55509888	
	移动电话	[redacted]	电子邮件	summer.yang@UCloud.cn	
测评单位					
单位名称	上海市网络技术综合应用研究所			机构代码	310073
单位地址	上海市长宁区虹桥路 2283 号君座 5 座			邮政编码	200336
联系人	姓名	江引子	职务/职称	项目经理	
	所属部门	测评部	办公电话	021-62192088	
	移动电话	[redacted]	电子邮件	jiangyinzi@siant.org	
审核批准	编制人	江引子	编制日期	2020.5.16	
	审核人	王世钦	审核日期	2020.5.16	
	批准人	王云飞	批准日期	2020.05.16.	

声明

本报告是云服务平台的等级测评报告。

本报告是对云服务平台的整体安全性进行检测分析，针对等级测评过程中发现的安全问题，结合风险分析，提出合理化建议。

本报告测评结论的有效性建立在被测评单位提供相关证据的真实性基础之上。

本报告中给出的测评结论仅对被测对象当时的安全状态有效。当测评工作完成后，由于被测对象发生变更而涉及到的系统构成组件（或子系统）都应重新进行等级测评，本报告不再适用。

本报告中给出的测评结论不能作为对被测对象内部部署的相关系统构成组件（或产品）的测评结论。

在任何情况下，若需引用本报告中的测评结果或结论都应保持其原有的意义，不得对相关内容擅自进行增加、修改和伪造或掩盖事实。

上海市网络技术综合应用研究所

（加盖单位公章）

2020 年 05 月 16 日

等级测评结论

测评结论和综合得分			
被测对象名称	云服务平台	安全保护等级	第三级（S3A3G3）
等级保护对象形态	☑传统 IT 系统 ☑云计算 ☐采用移动互联技术的系统 ☐物联网 ☐工业控制系统 ☐大数据 ☐其他系统		
被测对象描述	云服务平台主要承载的业务包括客户云计算资源用量、充值计费信息、网络流量信息和公司对外公开的信息等，主要是面向公众提供云计算信息技术基础架构服务。		
测评工作描述	受优刻得科技股份有限公司委托，上海市网络技术综合应用研究所于 2020 年 02 月 25 日至 2020 年 05 月 16 日对云服务平台进行了系统安全等级测评工作。本次安全测评的范围主要包括云服务平台的物理环境、主机、网络、业务应用系统、安全管理制度和人员等。安全测评通过静态评估、现场测试、综合评估等相关环节和阶段，从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等十个方面，对云服务平台进行综合测评。 本次等级测评分为四个过程：测评准备过程、方案编制过程、测评实施过程、分析与报告编制过程。其中，各阶段的时间安排如下： 1、2020 年 02 月 25 日～02 月 26 日，测评准备过程。 2、2020 年 02 月 27 日～02 月 28 日，方案编制过程。 3、2020 年 03 月 02 日～03 月 06 日，现场实施过程。 4、2020 年 03 月 27 日～05 月 16 日，分析与报告编制过程。 其中，2020 年 03 月 02 日召开了项目启动会议，确定了工作方案及项目人员名单；2020 年 03 月 06 召开了项目末次会议，确认了测评发现的问题；2020 年 03 月 26 日对系统的整改情况进行了复核确认。		
等级测评结论	优	综合得分	95.06 分

等级测评结论扩展表（云计算安全）

云计算安全等级测评结论扩展表			
云计算形态	☑云计算平台 ☐云服务客户业务应用系统（平台报告编号：N/A）		
运维所在地	上海	云服务模式	☑IaaS ☐PaaS ☐SaaS
云计算服务安全能力评价	云计算平台服务列表	云扩展要求项	符合性评价
	虚拟网络隔离服务	应实现不同云服务客户虚拟网络之间的隔离。	符合
	虚拟防火墙服务	应具有根据云服务客户业务需求提供通信传输，边界防护，入侵防范等安全机制的能力。	符合
	DDOS 攻击防护服务	应在检测到网络攻击行为、异常流量情况时进行告警。	符合
	主机入侵检测服务	应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。	符合
	数据存储位置查询服务	应提供查询云服务客户数据及备份存储位置的能力。	符合
	数据清除服务	云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除。	符合
	密钥管理服务	应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程。	符合
	服务水平协议（SLA）	应在服务水平协议中规定云服务的各项服务内容和具体技术指标。	符合
	供应链安全事件告知服务	应将供应链安全事件信息或安全威胁信息及时传达到云服务客户。	符合
	云计算迁移服务	应使用校验码或密码技术确保虚拟机迁移过程中重要数据的完整	符合

		性，并在检测到完整性受到破坏时采取必要的恢复措施。 应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。	
等级测评结论	优	综合得分	95.06 分

总体评价

通过对信息系统基本安全保护状态的分析，优刻得科技股份有限公司针对云服务平台面临的主要安全威胁采取了相应的安全机制，基本达到保护信息系统重要资产的作用。其中：

在安全物理环境方面，系统拥有分布在上海、北京、广州、杭州等地的 14 个机房，在物理位置的选择上符合要求，针对物理访问控制在机房大门和一楼大厅均有专人对来访人员进行登记鉴别和控制，设置视频监控报警系统，并拥有完备的防雷防火防水防潮防静电的手段，部署了精密空调设备，并建立了完善的电力供应系统，但是部分机房未提供电磁防护。

在安全通信网络方面，在数据中心内部按照 1:1 性能冗余设计，可以在 50%核心网络设备、线路异常时保证网络转发正常，并且在数据中心接入 Internet 以及 DCI 位置，考虑性价比，按照 N+1 冗余配置，通过天梁网络监控系统，检查各部分带宽使用情况，均不超过 60%，满足业务高峰期需求。机房划分多个区域进行管理，从外网到内网分为安全区、网关区、业务区等。在 POP 点部署安全区和网关区，将不信任区域的流量在安全区经过防 DDOS、WAF、防火墙设备的访问控制策略，然后到网关区做流量分发到数据中心内部，并且通过公司 IT 统一建设维护的 IPSec、SSLVPN 系统拨入公司内网保证了通信传输的保密性和完整性，不足之处在于无相关可信机制对通信设备的系统引导程序、系统程序进行可信验证。

在安全计算环境方面，网络设备具有完善的身份鉴别机制，通过 SSH 进行远程登录交换机，能够保证数据在传输过程中的保密性和完整性。登录交换机需

要进行账号+密码登录，身份标识唯一，同时采用 H3CiMC 作为 AAA 认证服务。同时已启用严格的访问控制策略，用户登录依据职能和使用功能的不同划分的账号和权限，并且交换机开启日志审计功能，审计范围涉及到所有用户，对重要操作、命令等进行记录，审计进程得到保护。不足之处在于网络设备登录时未采用双因素认证方式登录。安全设备均具有专门的登录模块，完善的身份鉴别机制和访问控制，同时开启了安全审计功能。操作系统通过堡垒机登录服务器，采用用户名、静态口令结合动态口令方式进行鉴别，身份标识唯一，服务器均已采用了可靠的身份鉴别措施，安全审计进程受到保护，记录内容详细且能够对操作系统用户进行审计，覆盖到每个操作系统用户，剩余信息保护措施到位；通过部署 HIDS 能够检测到对重要服务器进行入侵的行为。不足之处在于未对重要信息资源设置敏感标记和运维终端未采用双因素认证登录。在应用安全方面，系统具有完善的身份鉴别机制和访问控制，并通过 UCloud 云服务平台前台为云租户提供云服务，但是仅对交易信息提供审计功能。系统使用 https 进行传输，保证了数据在传输过程中的完整性和保密性，并且所有数据本地机房备三个副本，异地机房备一个副本。存在不足之处在于未采用双因素认证登录。

在安全管理中心方面，内部的态势感知系统及 DDOS 攻击防护系统、web 应用防火墙系统等共同构成安全管理中心（SOC），均采用 SSO 统一登录 Web 管理界面，严格划分人员权限，并且 DDOS 攻击防护系统保留操作日志。SOC 系统的安全管理员对 SOC 中的各类安全策略进行配置，但未配置可信验证策略。在网络拓扑中，机房划分特定的安全区，包括 web、抗 DDOS 系统、入侵检测系统，共同构成安全管理中心。统一部署并且由 web 应用防火墙、抗 DDOS 系

统、态势感知系统共同组成的 SOC 系统含安全策略、漏洞补丁、攻击流量等安全相关事项的集中管理。

在安全管理制度方面，对网络、计算机、机房、系统和相应的人员操作规程和岗位职责做出了相关规定。建立了覆盖从网络到运维管理，和系统资源管理等各类内容的管理制度。并制定了《ISMS_A01_信息安全管理手册 V1.2》包括信息安全工作的方针、策略，具有操作规程和规范，形成信息安全管理制度体系。由安全中心负责安全管理制度的制定，通过邮件进行发布，并定期对安全管理制度进行修订和评审。

在安全管理机构方面，已建立安全中心，设立安全主管、开发负责人、运维负责人、数据库主管等负责人岗位，关键岗位已配备 2 名以上的工作人员。通过 OA 系统进行授权审批操作，具有完善的审批流程，并定期对审批事项进行审查。制定了《审计与检查管理制度》明确规定定期进行安全检查，并提供了相关检查记录。

在安全管理人员方面，对入职岗位人员进行背景调查并记录，已提供人员签署保密协议和背景调查记录，人员离岗流程完善，严格执行离职过程，并制定了《年度信息安全培训计划》对安全培训计划进行规划，提供了《信息安全培训方案》、《培训签到表》，同时明确了奖惩措施。制定了《第三方管理程序》，对外部人员允许访问的区域、系统、设备、信息等内容进行了规定，存在不足之处在于未与获得系统访问授权的外部人员签署保密协议。

在安全建设管理方面，系统为自主研发，建立了较好的安全方案设计和完善的产品采购使用流程，运维部门负责系统交付相关的工作，确定安全服务商为上海谐润网络信息技术有限公司，并由技术部负责人负责工程实施过程的管理，并

制定了《工程实施方案》对实施过程进行有效的记录，由第三方安全机构对系统进行安全性测评，并提供了安全性测评报告。存在不足之处在于未定期评审和审核供应商提供的服务。

在安全运维管理方面，由机房管理员定期维护机房设施，并制定了《机房安全管理制度》。在《ISMS - B11_物理和环境安全管理程序 V1.1》中对人员调离、外来人员出入办公区域进行了详细的规定，同时制定了完备的资产管理制度，并提供了资产清单。指定设备管理部门对各种信息系统相关的设备进行管理，在信息安全事件处理方面，依据《ISMS-B16_信息安全事件管理程序 V1.1》对信息安全事件分级处理，对安全事件报告、事件处置等做出了明确要求。在《ISMS-B17_业务连续性管理程序 V1.1》第 2.4 中对应急预案做出了符合要求的描述。应急预案框架包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容，并且由安全中心对应急预案进行定期的审查更新，已提供《应急预案审查记录》。存在不足之处在于未定期进行应急预案培训。

主要安全问题及整改建议

1、安全物理环境

1）低风险 机房未采取电磁屏蔽措施。

建议为关键设备和磁介质实施电磁屏蔽。

2、安全通信网络

1）低风险 无相关可信机制对通信设备的系统引导程序、系统程序进行可信验证。

建议对通信设备的系统引导程序、系统程序进行可信验证。

3、安全区域边界

1）低风险 在网络边界处部署边界 H3C 防火墙，具有部分防病毒功能，能够对部分恶意代码进行检测和清除；

建议采取措施对所有服务器的恶意代码感染情况进行统一管理。

2）低风险 无可信根和可信验证程序进行可信验证。

建议采用可信根和可信验证程序进行可信验证。

4、安全计算环境

1）低风险 未采用两种或两种以上组合的鉴别技术；

建议对系统采用两种或两种以上组合的鉴别技术实现用户身份鉴别，如数字证书、令牌等。

2）低风险 未提供设置敏感标记功能；

建议对系统重要资源增加敏感标记的功能，并控制用户对已标记的敏感信息的操作。

3）低风险 操作终端未安装入侵检检测设备；

建议采取入侵检测措施，根据需要安装第三方入侵检测软件。

4）低风险 无相关恶意代码检测措施；

建议采取措施对所有服务器的恶意代码感染情况进行统一管理。

5）低风险 未采用密码技术进行通信完整性验证；

建议对重要数据采用经国家密码管理局认可的密码技术保证通信过程中数据的完整性。

6）低风险 操作终端未对重要数据进行备份；

建议对数据每天至少完全备份一次，并将备份介质场外存放，此外，还应定期对备份文件进行恢复测试，确保备份文件有效。

7）低风险 未实现热冗余，机房仅部署一台；

建议 H3C 防火墙采用热冗。

8）低风险 天梁、天眼系统无用户无操作超时退出响应机制；

建议对超时退出采取必要的安全措施，如超时 60s 自动退出等。

9）低风险 未限制终端接入地址；

建议限制可登录数据库的管理终端地址，仅允许特定的地址访问。

10）低风险 操作终端未提供异地实时备份机制；

建议利用通信网络将关键数据定时批量传送至备用场地，实现异地数据异地备份。

11）低风险 日志审计功能不完善；

建议开发安全审计分析功能，覆盖到每一个用户。

12）低风险 无可信根和可信计算设备对交换机系统和硬件进行可信验证。

建议采用可信根和可信计算设备对交换机系统和硬件进行可信验证。

5、安全管理中心

1）低风险 SOC 系统的安全管理员对 SOC 中的各类安全策略进行配置，但未配置可信验证策略。

建议配置可信验证策略。

6、安全管理人员

1）低风险 未与获得系统访问授权的外部人员签署保密协议。

建议与获得系统访问授权的外部人员签署保密协议。

7、安全建设管理

1）低风险 未组织相关部门和有关安全专家对安全整体规划及配套文件进行合理的论证评审；

建议组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施。

2）低风险 未通过第三方工程监理控制项目的实施过程；

建议通过第三方工程监理控制项目的实施过程。

3）低风险 测试验收不完善。

补充在系统验收阶段需委托第三方测试单位对系统进行安全性测试的相关规定，保证今后在系统建设验收阶段委托第三方进行安全测试。

8、安全运维管理

1）低风险 未记录和保存基本配置信息；

建议定期记录和保存基本配置信息。

2）低风险 未将基本配置信息纳入变更范畴；

建议及时更新基本配置信息库。

3) 低风险 未按照规定的周期进行恢复性验证；

建议按规定周期对备份数据进行恢复性验证。

4) 低风险 未对应急预案进行培训；

建议对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次。

5) 低风险 未定期对介质进行盘点。

建议定期对介质进行盘点。

8	物理攻击	通过物理的接触造成对软件、硬件、数据的破坏
9	泄密	信息泄露给不应了解的他人
10	篡改	非法修改信息，破坏信息的完整性使系统的安全性降低或信息不可用
11	抵赖	不承认收到的信息和所作的操作和交易
12	资源不足	系统重要设备负载较高，不满足业务需求，一旦设备因负载较高而出现故障将影响业务连续性
13	敏感信息泄漏	敏感信息包括用户信息、 公民信息、地理信息，数量级 0~1 万、1~10 万、10~100 万、100 万以上
14	网页篡改	针对连接互联网的网站面临被篡改的可能性较大

附录H　云服务商针对云平台测评问题及整改情况

问题 1：UCloud 云服务平台前台缺少日志集中管理和分析功能。

答复：目前正在对云平台的该功能进行优化改造。

问题 2：UCloud 云服务平台的登录超时默认时长过长。

答复：目前正在对云平台的该功能进行优化改造。

问题 3：网络设备、计算设备均未实现基于可信根的可信验证。

答复：目前正在关键节点对该功能要求进行设计优化。