ICS 35.020
CCS L 70

T/GDEIIA

团　体　标　准

T/GDEIIA xx—2023

能源区块链系统评估要求

Energy Blockchain System Evaluation Requirements

（征求意见稿）

2023－xx－xx 发布　　2023－xx－xx 实施

广东省电子信息行业协会　　发布

目 次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件不涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由广东电网有限责任公司提出。

本文件由广东省电子信息行业协会归口。

本文件起草单位：广东电网有限责任公司、南方电网数字企业科技（广东）有限公司、湖南天河国云科技有限公司、南方电网人工智能科技有限公司、广东天河国云科技有限公司

本文件主要起草人：陈军、裴求根、伍江瑶、郑灶贤、吴欣欣、尹海波、姚昱旻、孔曼、杨能、杨伟、徐驰、肖晶、欧阳昌忠、魏来

本文件为首次发布。

能源区块链系统评估要求

1 范围

本文件规定了能源区块链系统的具体要求、评估方法、判定准则等。

本文件适用于能源企业对能源区块链的系统设计、软件开发、系统评估。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

JR/T 0193-2020 区块链技术金融应用 评估规则

DB43/T 1838-2020 信息安全技术 区块链共识安全技术测评要求

3 术语和定义

下列术语和定义适用于本文件。

3.1 区块链（Blockchain）

一种由多方共同维护，使用密码学保证传输和访问安全，能够实现数据一致存储、防篡改、防抵赖的技术体系。

[来源：JR/T 0193-2020]

3.2 能源区块链（Energy Blockchain）

能源区块链主要指区块链技术在能源物联网领域的应用，能源系统中的各个能源结点通过区块链技术加密存储能源交易信息数据，利用共识机制完成分布式能源决策，然后利用智能合约机制完成能源的自动交易，实现能源交易过程中能量流、信息流和价值流的有效衔接。

3.3 联盟链（Consortium Blockchain）

联盟链主要是面向部分群体的一种区块链，它是一种半开放式的区块链系统，联盟链主要部署在少数群体之间，由这些成员共同管理的区块链系统，每个成员的加入和退出都需要经过允许。系统内的交易数据和用户数据等信息只能允许联盟链成员来进行追溯，相比于中心化过度的私有链，联盟链更加开放，权限要求更为复杂，也能保障数据的安全。所以联盟链更受企业和组织机构的欢迎，其主要应用就是企业级区块链服务平台等。

3.4 密码机制（cryptographic mechanism）

区块链最初所用到的密码算法主要有杂凑算法和数字签名算法，随着区块链技术的发展，越来越多的密码算法逐渐被引入到区块链中，如环签名、多重签名、零知识证明、同态密码以及安全多方计算等。用于构建可信身份、实现交易确权、隐私保护和共识安全。

3.5 共识机制（consensus mechanism）

指确保系统记账一致性的算法、措施和规则，旨在解决不同节点之间信任的问题。
[来源：DB43/T 1838-2020]

3.6 工作量证明（PoW, Proof of Work）

在基于工作量证明机制构建的区块链网络中，节点通过计算随机哈希散列的数值解争夺记账权，求得正确的数值解以生成区块的能力是节点算力的具体表现。

3.7 权威证明机制（PoA, Proof of Authority）

依赖于可信验证者，只有可信验证者可以生成区块，可信验证者的添加和删除需要所有可信验证者的投票完成。不需要浪费算力以获取生成区块的资格，极大地提高了交易吞吐量。

3.8 智能合约（Smart contract）

一种嵌入式程序化合约，可以内置在任何区块链数据、交易、有形或无形资产上,形成可编程控制的软件定义的系统、市场和资产。

3.9 数据上链

由节点将相关业务数据打包至区块链的区块中存储。

3.10 数据校验

采用区块链系统中的哈希算法和公钥密码算法对数据进行运算，保证数据的完整性、不可篡改性。

4 能源区块链技术评估概述

4.1 评估范围

由于能源区块链技术评估涉及到文档分析、技术分析以及人工评估的工作，所以在进行能源区块链应用系统评估时，一般采用的抽样评估的方式。本次主要是针对能源企业的区块链系统。

4.2 评估方法

采用以下工作方法对能源区块链应用进行评估达到上述目标：

a） 客户访谈：通过客户访谈，可以从解析区块链技术、电力公司管理、策略等角度深层次地了解对客户电力业务的需求。

b） 文档信息挖掘：顾问通过客户对电力应用业务需求的相关管理制度、规范、区块链技术文档、历史事件和日志等等的研究和分析，从更高层次的评估能源区块链的应用。

c） 专家分析：通过专家经验在能源区块链应用的咨询服务是不可替代的关键地位，目前尚没有成型的工具、模型、算法等可以将能源区块链专家的经验完全体现。通过对客户访谈、文档信息挖掘的收集的资料进行分析，顾问会将自己的经验体现于最终输出，也就是本项目标准。

4.3 评估过程

能源区块链应用系统评估包括以下几个步骤：

a） 确定具体的应用评估对象；

b） 根据评估对象的特点定制评估列表；

c） 收集一些能源区块链应用系统的相关资料；

d） 对应用系统进行文档分析；

e） 访谈能源区块链应用系统设计相关人员；

f） 总结应用系统的安全和现状并纂写业务系统评估报告。

5 基本评估

5.1 密码机制

包括以下要求：

a） 评估指标：支持对称加密、非对称加密的模式。

b） 评估对象：平台加密支撑模式。

c） 评估实施包括以下内容：

1） 是否支持 SM2 数字签名算法、SM2 公钥加密算法、SM4 对称加密算法以及 SM3 哈希算法等国产商用密码算法。；

2） 是否支持 ECDSA 数字签名算法、ECIES 公钥加密算法、AES 对称加密算法、SHA 系列哈希算法等主流国际标准密码算法；

3） 为满足不同场景的安全需求，区块链平台支持定制安全可控的私有化密码算法的能力，包括：数字签名算法、公钥加密算法、对称加密算法和哈希算法等；

4） 是否支持其他主流密码算法。

d） 评估判定：支持各类自主可控的对称加密、非对称加密算法，可将真实数据加密后再上链。

5.2 共识机制

包括以下要求：

a） 评估指标：能够提供可灵活选择的共识机制的能力。如 PoW、PoA 等主流共识机制。

b） 评估对象：平台共识支撑模式。

c） 评估实施包括以下内容：

1）节点按照 PoW 预定规则，生成合法区块，并广播至网络中。按照 PoW 预定规则，接收到新

区块的其他节点验证新区块的有效性，若验证通过，则将新区块添加到自己的链上。

2） 根据预设规则以及可信验证者的投票，添加新的可信验证者。根据预设规则以及可信验证者的投票，删除可信验证者。按照 PoA 的预定规则，可信验证者收集交易并生成合法区块，并广播到网络中。按照 PoA 的预定规则，接收到新区块的其他节点验证新区块的有效性，若验证通过，则将新区块添加到自己的链上。

d） 评估判定：可灵活选择共识机制。

5.3 智能合约

包括以下要求：

a） 评估指标：具备可在线编译、部署智能合约的能力，并可根据需要提供定制化的智能合约业务模板，如合同签订模版，减少用户因为不熟悉智能合约开发及部署造成的隐私泄漏和资源死锁等情况发生。

b） 评估对象：智能合约存储与运算。

c） 评估实施包括以下内容：

1） 是否提供基本的数据存储功能；

2） 是否可以通过调用智能合约对不同类型的数据进行操作，并更新数据；

3） 是否能为不同的数据类型提供了基本运算；

4） 是否支持其他合约调用；

5） 是否支持对数据进行基本的操作。

d） 评估判定：具有逻辑上的独立存储区，使用 Merkle Patricia Tries 组织每个智能合约的数据，并将树根的哈希值存储到合约账户的账户状态中写入区块链，支持的数据类型包括值类型、引用类型以及映射；通过调用智能合约可以对不同类型的数据进行操作，并更新数据；智能合约为不同的数据类型提供了基本运算，方便智能合约开发过程中对数据的操作；支持其他合约调用，实现代码复用，在降低开发者开发难度时，提供高质量的合约代码，减少代码漏洞的出现；允许对数据进行基本的操作，包括数据上链（即将数据存储到区块链中，以保证其不可篡改性）、数据查询、数据下载（以支撑平台应用的数据下载需求）及完整性校验。

5.4 数据处理

包括以下要求：

a） 评估指标：允许对数据进行基本的操作，包括数据上链（即将数据存储到区块链中，以保证其不可篡改性）、数据查询、数据下载（以支撑平台应用的数据下载需求）及完整性校验。

b） 评估对象：区块链平台的基础功能数据处理

c） 评估实施包括以下内容：

1） 是否上链数据预处理和存储结果返回；

2） 是否实现对数据的查询；

3） 是否支持数据下载请求解析和数据下载结果返回功能；

4） 是否支持数据校验请求解析和数据校验结果发布；

d） 评估判定：通过完整性校验功能可以快速检验数据是否被篡改，为平台应用及用户提供防篡改服务。

5.5 日志管理

包括以下要求：

a） 评估指标：当平台出现安全问题或者不稳定状况时，可以通过查询日志进行快速排查，确保平台能够健康稳定的运行。

b） 评估对象：对日志的管理

c） 评估实施包括以下内容：

1） 平台运行日志；

2） 应用管理日志；

3） 节点管理日志；

4） 监督管理日志；

d） 评估判定：通过日志管理实现了对各类日志的分类记录、查询及分析功能。

5.6 用户管理

包括以下要求：

a） 评估指标：可以对 PKI/CA 体系进行管理。

b） 评估对象：对区块链用户管理

c） 评估实施包括以下内容：

1） 用户证书的注册；

2） 密钥生成与分发；

3） 证书颁发；

4） 密钥恢复；

5） 证书撤销与更新；

6） 身份认证以及对用户权限设置；

d） 评估判定：对电子证书进行全生命周期管理。

5.7 监督管理

括以下要求：

a） 评估指标：实现对平台的实时监督。

b） 评估对象：能源区块链应用监督功能。

c） 评估实施包括以下内容：

1） 平台运行状况查看，以可视化的方式展现平台运行健康状态、平台硬件资源利用率，平台访问量等信息；

2） 应用支撑情况查看，以可视化的方式展示平台支撑的应用情况，包括应用规模、应用类别、地域分布等；

3） 安全问题处理情况查看；

4） 平台实时运行状态查看；

d） 评估判定：直观的动态图像的方式向展示平台当前运行的状态，包括当前采用的共识机制、密码算法，在线节点数量及其分布状况，区块数量产生速率等信息。

5.8 存储管理

包括以下要求：

a） 评估指标：实现对能源区块链数据安全的存储。

b） 评估对象：能源区块链应用的数据存储功能。

c） 评估实施包括以下内容：

1） 对结构化数据存储和非结构化数据存储；

2） 对数据的维护实现授权数据的修改、删除以及授权操作的记录；

3） 映射关系维护实现将云服务器数据与区块链数据建立映射关系，在云服务器上存储原始数据，在链上保存对应数据的标识（哈希值），实现协同存储；

4） 数据一致性校核和数据目录维护；

d） 评估判定：平台数据当发生非法篡改时，能够在一定时间范围内发现篡改行为并发出提醒。

5.9 负载均衡

包括以下要求：

a） 评估指标：实现对能源区块链应用服务器负载均衡。

b） 评估对象：能源区块链应用的负载功能。

c） 评估实施包括以下内容：

1） 服务器定时向每个节点发送心跳包，检测节点在线状态；

2） 各个节点主动向负载均衡服务器推送机器当前运行状态，如内存、硬盘等；

3） 通过负载均衡算法进行流量分发，使得多个区块链节点分担应用、用户请求，消除单点故障，提升系统可用性；

4） 区块链平台采用区块链和多个数据库协同存储，将数据在多个节点上冗余存储，分担数据请求，提升数据可用性；

5） 采用微服务的思想将区块链平台提供的服务进行拆分到多个节点上班，避免单个节点承担过多服务请求；

d） 评估判定：当出现应用服务器压力过大的时候，会将一部分压力“均摊”不同的服务器，不集中在一个服务器上。

6 性能评估

6.1 数据上链效率评估

包括以下要求：

a） 评估指标：数据上链处理时间应小于申明数值。

b） 评估对象：数据上链效率。

c） 评估实施包括以下内容：

1） 数据量较小的上链处理时间；

2） 单条数据记录上链处理时间；

3） 数据量较大的上链处理时间；

4） 逻辑复杂的批量数据上链处理时间。

d） 评估判定：不同容量的数据上链的处理时间在以上评估实施内容的申明数值内。

6.2 数据查询响应评估

包括以下要求：

a） 评估指标：数据查询处理的后台响应时间应小于申明数值。

b） 评估对象：数据查询响应时间。

c） 评估实施包括以下内容：

1） 单条数据查询响应时间；

2） 多条数据查询响应时间。

d） 评估判定：不同数量的数据查询处理的后台响应时间在以上评估实施内容的申明数值内。

6.3 数据校验响应评估

包括以下要求：

a） 评估指标：数据校验处理的后台响应时间应小于申明数值。

b） 评估对象：数据校验响应时间。

c） 评估实施包括以下内容：

1） 单条数据校验响应时间；

2） 多条数据校验响应时间。

d） 评估判定：不同数量的数据校验处理的后台响应时间在以上评估实施内容的申明数值内。

6.4 并发服务评估

包括以下要求：

a） 评估指标：能源区块链平台应具备能够支撑不少于申明数值的业务系统并发调用。

b） 评估对象：并发调用业务系统数量。

c） 评估实施包括以下内容：

1） 并发调用业务系统的最大数量及相应的服务请求时间。

d） 评估判定：能源区块链平台并发调用的业务系统最大数量在申明数值以上。

6.5 部署效率评估

包括以下要求：

a） 评估指标：能源区块链节点封装、服务封装、组件部署以及专用集群部署时间在申明数值内。

b） 评估对象：节点、系统等部署时间。

c） 评估实施包括以下内容：

1） 编写相应节点的启停脚本、配置文件时间；

2） 应用类服务、管理类服务完成模块打包并以虚拟机或容器化的形式进行封装的时间；

3） 根据分配的服务器，为区块链平台建立独立的集群和部署组的时间；

4） 在专用集群上部署时，网络配置、配置访问策略的时间；

d） 评估判定：以上实施内容所用时间时间在申明数值内。

6.6 支撑用户能力评估

包括以下要求：

a） 评估指标：能源区块链平台应具备能够支撑的业务系统（例如 OA 应用、人工智能应用等）数

量不少于申明数值，提供相应的区块链服务。

b） 评估对象：区块链服务对象的业务系统数量。

c） 评估实施包括以下内容：

1） 多个业务系统的区块链服务。

d） 评估判定：能源区块链平台支撑的业务系统数量在申明数值以上。

7 安全性评估

7.1 安全保护等级评估

包括以下要求：

a） 评估指标：能源区块链平台的安全等级保护为三级。

b） 评估对象：安全保护等级。

c） 评估实施内容：

根据《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）以及《电网管理信息系统安全等级保护标准》要求，经过专家评审后，确定电网区块链平台的安全保护等级。并需要按照中华人民共和国国家标准《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）进行系统的安全防护。

d） 评估判定：经过专家评审后，确定电网区块链平台的安全保护等级为三级。

7.2 物理和环境安全评估

包括以下要求：

a） 评估指标：能源区块链平台部署环境及保护措施等是否符合法令条规。

b） 评估对象：物理和环境安全措施。

c） 评估实施内容：

1）电网区块链平台需部署在专业机房内。专业机房需符合国家以及公司信息机房建设技术规范以及运营相关要求。具备防震、防风、防雨、防雷、防火、防盗等保护措施。机房温、湿度的变化在电网区块链平台设备运行所允许的范围之内；

2）通过符合国产密码要求的电子门禁系统确保机房出入控制；通过符合国产密码要求的视频监控系统实现视频监控。

d） 评估判定：专业机房符合国家以及公司信息机房建设技术规范以及运营相关要求；视频监控系统符合国产密码要求。

7.3 网络和通信安全评估

7.3.1 网络拓扑结构

包括以下要求：

a） 评估指标：网络结构安全保证网络设备的业务处理能力，具备冗余空间和链路负载均衡能力，满足业务高峰期需要。

b） 评估对象：网络结构。

c） 评估实施内容：

1）根据能源区块链平台的安全属性，其部署在信息内网。并按照“三级（及以上）系统独立成域、二级（及以下）系统集成成域”的原则，通过虚拟化网络技术或者 SDN 技术实现能源区块链平台单独设域，与其他系统实现逻辑隔离，在不同网段之间进行路由控制，建立安全的访问路径，实行针对性、差异化防护；

2） 涉及 internet 的应用，需部署在信息外网区，使用统一集中的互联网出口，并通过信息安全交换平台实现强逻辑隔离；

3） 要求采用冗余技术设计网络拓扑结构，确保路由冗余；

4） 网络优先级配置：根据能源区块链平台的重要性设置带宽分配级别，保证在网络发生拥堵的时候优先能源区块链平台服务连续性；

5） 网络设备冗余配置：避免存在网络单点故障，确保网络设备高可靠性。

d） 评估判定：网络结构安全保证网络设备的业务处理能力，具备冗余空间和链路负载均衡能力。

7.3.2 网络边界防护

包括以下要求：

a） 评估指标：保证信息及网络资源不被非法使用和访问。

b） 评估对象：网络边界。

c） 评估实施内容：

1）通过 ACL 技术或防火墙技术，在网络边界或区域之间根据访问控制策略设置访问控制规则，实现对能源区块链平台域实现端口级访问控制，默认情况下除允许通信外受控接口拒绝所有通信；应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。并对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；

2）通过入侵监测技术，在网络边界处监视如端口扫描、强力攻击、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攻击行为，并给予告警以及响应和处理；

3）在网络边界及核心业务网段处对恶意代码进行检测和清除；

4）通过网络安全扫描工具，利用优化系统配置和打补丁等各种方式最大可能地弥补最新的安全漏洞和消除安全隐患。

d） 评估判定：信息及网络资源不被非法使用和访问；对攻击行为给予告警以及响应和处理；及时实现恶意代码库升级和检测系统更新；弥补最新的安全漏洞和消除安全隐患。

7.3.3 网络安全审计

包括以下要求：

a） 评估指标：对网络设备、安全设备运行状况、网络流量、用户行为等进行日志信息实时采集、集中监控及实时预警。

b） 评估对象：网络安全审计。

c） 评估实施内容：

审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

d） 评估判定：对网络设备、安全设备运行状况、网络流量、用户行为等进行日志信息实时采集、集中监控及实时预警。

7.4 设备和计算安全评估

7.4.1 硬件安全

包括以下要求：

a） 评估指标：采用服务器设备应确保能源区块链平台处理性能要求

b） 评估对象：服务器设备。

c） 评估实施内容：

1） 采用的服务器设备是否具备冗余配置（包括双机热备等）、不间断电源保障、运行状态监控等；

2） 对登录的用户进行身份标识和鉴别；

3） 是否具备登录失败处理功能；

4） 进行远程管理时是否安全。

d） 评估判定：采用的服务器设备具备冗余配置（包括双机热备等）、不间断电源保障、运行状态监控；对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；具有登录失败处理功能，配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；当进行远程管理时，有相应的加密措施。

7.4.2 操作系统安全

包括以下要求：

a）评估指标：具备操作系统账号管理、认证授权、安全日志等功能，能够从多个方面进行主机安全基线加固。

b） 评估对象：操作系统。

c） 评估实施内容：

1） 操作系统账号管理、认证授权、安全日志等功能测试；

2） 身份鉴别，访问控制，安全审计入侵防范，恶意代码规范，资源控制等功能测试.

d） 评估判定：操作系统采用 Linux，通过加强操作系统账号管理、认证授权、安全日志等功能，实现从身份鉴别，访问控制，安全审计入侵防范，恶意代码规范，资源控制几个方面进行主机安全基线加固。

7.4.3 中间件与数据库安全

包括以下要求：

a）评估指标：具备从多个方面进行主机安全基线加固的功能，能够避免非法用户进入到网络后查看相关信息。

b） 评估对象：中间件与数据库。

c） 评估实施内容：

1） 从身份鉴别，访问控制，安全审计，通信完整性，通信保密性，软件容错，资源控制几个方面进行中间件安全测试。

2） 采用默认的管理员账号和密码登录测试。

d） 评估判定：从身份鉴别，访问控制，安全审计，通信完整性，通信保密性，软件容错，资源控制几个方面进行中间件安全基线加固；禁止了默认的管理员账号和密码，避免非法用户进入到网络后通过直接调用监控末端设备查看相关信息。

7.5 应用和数据安全评估

7.5.1 数据安全

包括以下要求：

a） 评估指标：采用身份认证、权限控制、加密存储、加密传输、数据防泄密等技术，加强能源区块链平台数据机密性及安全性防护。

b） 评估对象：数据机密性及安全性。

c） 评估实施内容：

1） 通过对数据库表设置完整性约束，如 Check、NOT NULL、Unique、Primary、Foreign key 来测试数据的完整性；

2） 使用国产密码技术对能源区块链平台数据库表访问权限进行控制；

3） 采用国产密码技术对能源区块链平台的重要数据进行加密存储，防止数据库被黑客攻击导致系统机密泄漏；

4） 使用国产密码技术保证能源区块链平台重要数据传输过程中的机密性及完整性；

5） 仅采集和保存业务必需的用户个人信息；禁止未授权访问、使用用户个人信息；

6） 通过数据防泄密网关，减少敏感数据泄密；

7） 采用数据本地备份或者数据灾备技术，确保能源区块链平台核心数据安全，确保在某个存储设备故障或灾害发生时，数据不会丢失；

8） 存储设备报废前按照规定通过消磁粉碎一体机进行信息彻底清除，确保数据不能被恢复、还原；

9) 确保能源区块链平台日志信息保持 6 个月以上。并采用国产密码技术实现电网区块链平台日志信息完整性保护；

10） 采用国产密码技术实现电网区块链平台的加载和卸载安全控制；

11） 实现数据库访问审计。

d） 评估判定：能源区块链平台数据完整可验证；用户个人信息安全、敏感数据等重要数据安全可信；异常情况下数据可恢复。

7.5.2 应用安全

包括以下要求：

a) 评估指标：能源区块链平台应具备完善的权限管理，贯穿全系统的分级授权和界面信息操作控制，完整的应用程序日志记录和审计机制。

b） 评估对象：能源区块链平台应用。

c） 评估实施内容：

1） 通过角色划分使各层各级人员对于功能页面的访问控制；依据安全策略控制用户对文件、数据库表等客体的访问；访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作；授权主体配置访问控制策略，并严格限制默认帐户的访问权限。

2） 对登录用户的统一身份标识和鉴别，进行身份鉴别信息的防截获、防假冒和防重用，保证能源区块链平台用户身份的真实性。

3） 启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

4） 采用基于国产密码的数据验签技术验证通信过程中数据的完整性；

5） 通过基于国产密码的加解密技术，测试对重要数据的传输安全。

6） 通过基于国产密码的加解密技术校验数据有效性

7） 对数据进行有效性检查，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。

8） 关闭不需要的端口及服务。

9） 通过负载均衡技术，确保在突发数据流的情况下，能源区块链平台依然可以提供适当的服务能力。

10） 当通信双方中的一方在一段时间内未作任何响应，另一方自动结束会话；对系统的最大并发会话连接数进行限制；对单个账号的多重并发会话进行限制。

11） 通过防病毒系统，实现统一控制台对应用系统病毒防范，包括统一的分发、维护、更新和报警等。

12） 通过对用户的登录、退出、增加用户、修改用户权限等进行应用审计。

13） 通过信息安全运行预警系统，实现对能源区块链平台的运行状态、用户体验等的实时监控与预警。

14） 要求通过支持国产密码的堡垒机等技术，实现对能源区块链平台运维的统一管控，避免对网络和服务器资源的直接访问，对不合法命令进行命令阻断，过滤掉所有对目标设备的非法访问行为，减少和恶意攻击，拦截非法访问，并实现运维操作行为审计。

d） 评估判定：访问控制的覆盖范围包括了与资源访问相关的主体、客体及它们之间的操作，限制了默认帐户的访问权限；实现对登录用户的统一身份标识和鉴别，实现身份鉴别信息的防截获、防假冒和防重用，保证能源区块链平台用户身份的真实性；启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数；保证了数据的完整性、安全性、有效性；在突发数据流的情况下，能源区块链平台依然可以提供适当的服务能力。可控制系统的最大并发会话连接数和限制对单个账号的多重并发会话。实现统一控制台对应用系统病毒防范。可对用户的登录、退出、增加用户、修改用户权限等进行应用审计。实现对电网区块链平台的运行状态、用户体验等的实时监控与预警。

7.6 终端设计安全评估

包括以下要求：

a） 评估指标：较强的桌面终端监控审计管理，具备提高移动存储介质使用管理能力与病毒、木马检测防护、桌面终端行为监控审计能力。

b） 评估对象：终端。

c） 评估实施内容：

1） 通过上网行为管理系统，加强信息外网办公终端 internet 访问控制，如网络应用控制、带宽流量管理、上网行为分析等。对内部网络中出现的内部用户未通过准许私自联到外部网络的行为进行检查；

2） 存储设备报废前按照规定通过消磁粉碎一体机进行信息彻底清除，确保数据不能被恢复、还原；

3） 对访问的移动终端进行安全防护，通过沙箱等技术确保本地数据安全存储，通过身份认证及权限控制技术确保访问安全；通过加密技术实现传输安全。通过设备远程控制技术，如设备定位、设备远程数据擦除、锁定、更改密码等确保重要数据一键式擦除。

d） 评估判定：加强信息外网办公终端 internet 访问控制；彻底清除的数据不能被恢复、还原；通过身份认证及权限控制技术确保了访问安全；加密技术可实现传输安全；通过设备远程控制技术可将重

要数据一键式擦除。

7.7 安全管理评估

7.7.1 安全管理机构与人员

包括以下要求：

a）评估指标：是否具备专门的职能部门及专职安全管理员等。

b） 评估对象：安全管理机构与人员。

c） 评估实施内容：

1） 确认是否设立信息安全管理工作的职能部门；

2） 确认是否具备专职安全管理员，具备明确岗位及职责；

3） 确认是否建立关键岗位人员保密制度和调离制度；

4） 确认是否对被录用人员的身份、背景、专业资格和资质等进行审查；人员离职时应及时终止离岗员工的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。

d）评估判定：设立了信息安全管理工作的职能部门；具备专职安全管理员，具备明确岗位及职责。建立了关键岗位人员保密制度和调离制度；对被录用人员的身份、背景、专业资格和资质等进行审查；人员离职时及时终止离岗员工的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。

7.7.2 安全运维管理

包括以下要求：

a）评估指标：是否具备安全高效的运维管理服务。

b） 评估对象：安全运维管理。

c） 评估实施内容：

1） 定期更新漏洞库。采用漏洞扫描、数据库扫描等检测技术，定期检测操作系统、中间件、数据库、能源区块链平台的安全漏洞，全面评估安全漏洞和认证、授权、完整性方面的问题，并进行安全加固。

2） 能源区块链平台统一 IT 资产统一管理以及运维管理服务。

3） 能源区块链平台统一的安全运维及集中监控及预警。

4） 能源块链平台定期本地备份。

5） 能源块链平台远程数据级灾备，定制应急预案并加强定期演练。

6） 能源块链平台应用级灾备防护，定制应急预案并加强定期演练。

7） 自主运维，是否有明确约定外包运维的范围、工作内容及工作要求。

d） 评估判定：定期检测操作系统、中间件、数据库、能源区块链平台的安全漏洞；具备区块链平台统一IT资产统一管理以及运维管理服务；具备电网区块链平台统一的安全运维及集中监控及预警；对电网区块链平台进行定期本地备份；安全事件快速响应、及时处理；正确使用密码相关产品；自主运维。