ICS 点击此处添加 ICS 号
CCS 点击此处添加 CCS 号

团　　体　　标　　准

T/XXX XXXX—XXXX

企业整体发展规划平台技术规范

Technical specifications for the overall development planning platform of enterprises

－XX－XX 发布　　XXXX－XX－XX 实施

全国城市工业品贸易中心联合会　　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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由　　提出。

本文件由全国城市工业品贸易中心联合会归口。

本文件主要起草单位：

本文件主要起草人：

企业整体发展规划平台技术规范

1 范围

本文件规定了企业整体发展规划平台技术规范的术语和定义、功能要求、安全要求、性能要求、运维要求。

本文件适用于企业整体发展规划平台。

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。

GB/T 21052 信息安全技术 信息系统物理安全技术要求

GB/T 22239 信息安全技术 网络安全等级保护基本要求

3 术语和定义

本文件没有需要界定的术语和定义。

4 功能要求

4.1 战略规划管理要求

4.1.1 设定并管理企业长期和短期的发展目标。

4.1.2 平台应能分析市场趋势、竞争态势和内部资源，为战略决策提供数据支持。

4.1.3 平台应支持多部门、多层级协同制定和调整战略计划。

4.2 资源管理要求

4.2.1 集中管理企业的人力资源、财务资源、物资资源等，确保资源的高效配置。

4.2.2 平台应提供资源使用情况的实时监控和报告，为优化资源分配提供依据。

4.2.3 平台应支持资源的申请、审批和分配流程，确保资源的合理使用。

4.3 业务执行支持要求

4.3.1 平台应整合企业各业务系统，实现数据共享和业务协同。

4.3.2 平台应提供项目管理、任务分配、进度监控等功能，支持业务流程的顺畅执行。

4.3.3 平台应支持移动办公和远程协作，提高工作效率和响应速度。

4.4 绩效评估与监控要求

4.4.1 应设定关键绩效指标（KPIs），实时监控业务执行情况和目标完成情况。

4.4.2 平台应能提供多维度的数据分析工具，帮助企业发现问题、分析原因并优化决策。

4.4.3 整合内部和外部的评估数据，为企业整体发展提供全面的评估报告。

4.5 风险管理要求

4.5.1 平台应能识别、评估和管理企业面临的各类风险，如市场风险、财务风险、运营风险等。

4.5.2 平台应提供风险预警和应对策略，帮助企业及时应对风险事件。

4.5.3 平台应支持风险管理的持续改进和优化，提高企业的抗风险能力。

4.6 决策支持要求

4.6.1 平台应能利用大数据分析、人工智能等技术，为企业高层提供决策支持。

4.6.2 平台应能自动整合各类信息和数据，提供全面、深入的决策分析报告。
4.6.3 平台应支持模拟分析和预测分析，帮助企业制定更加科学合理的决策方案。

4.7 系统扩展与集成要求

4.7.1 平台应支持系统的扩展和升级，以满足企业不断发展的需求。
4.7.2 平台应能提供丰富的 API 接口和集成方案，方便与其他系统进行对接和集成。
4.7.3 平台应支持多语言、多币种等国际化功能，满足跨国企业的需求。

4.8 数据安全与隐私保护要求

4.8.1 平台应采用先进的数据加密和权限控制技术，确保企业数据的安全性和隐私保护。
4.8.2 平台应提供数据备份和恢复机制，防止数据丢失和损坏。
4.8.3 平台应支持安全审计和日志记录功能，方便企业进行安全监控和溯源分析。

5 安全要求

5.1 身份安全要求

5.1.1 应具有机密性，可采用对称和非对称加密技术，确保敏感信息不被窃取。
5.1.2 应具有完整性，可采用数字摘要确保身份信息不被篡改。
5.1.3 应具有真实性，身份鉴别可采用数字证书确保身份真实性。
5.1.4 应具有不可抵赖性，可采用数字签名确保数据发送方不可否认自己的信息。

5.2 网络传输安全

5.2.1 应在参与联盟链的节点之间建立安全传输通道，保证数据传输的完整性和不可篡改性。
5.2.2 应对数据和信息采取相应的防护措施，保证其能抵抗篡改、重放等主动或被动攻击。
5.2.3 应保证节点间通信过程中敏感信息字段或整个报文的保密性，宜采用密码学技术。
5.2.4 应确保信息在存储、传输过程中不被非授权用户读取和篡改，可采用有权限的网络访问控制，在参与分布式账本节点之间构建虚拟专用网络（VPN），降低网络攻击造成的危害。

5.3 物理安全

应符合GB/T 21052的要求。场地安全部署物理数据中心及附属设施的，用于业务运行、数据存储和处理的物理设备需符合国家监管要求。

5.4 节点部署安全

5.4.1 应保证承担共识的节点冗余部署，保证系统可用性；避免将所有承担共识的节点部署在同一机房内，能在单一机房节点不可用时保证系统整体的可用性。
5.4.2 确保部署节点的硬件设备存储容量可扩展，避免因数据容量达到上限而无法同步数据。

5.5 硬件设备

5.5.1 应对设备运行状态、资源使用情况等进行监控，能在发生异常时发出告警。
5.5.2 设备和存储介质在重用、报废或更换时，能对其承载的数据进行清除且不可恢复。

6 性能要求

6.1 功能完备性

平台应完整地实现所有的功能需求，并且应经过全面的测试，以确保其正常运行并满足用户需求。

6.2 性能表现

平台需要具有良好的性能表现，包括响应时间、吞吐量、并发能力等方面。性能指标应满足或超过用户需求，并且平台应在各种情况下都能保持稳定的性能表现。

6.3 安全性

平台需要具有良好的安全性能，能够保护用户的数据安全，并防范各种安全威胁和攻击。在验收过程中，需要对平台的数据安全、用户权限管理、系统漏洞等方面进行测试。

6.4 可维护性

平台的代码结构应易于理解和维护，注释规范，模块化程度高。

6.5 可移植性

平台应具有良好的可移植性，能够在不同的硬件和软件环境下运行，以满足不同用户的需求。

7 运维要求

7.1 系统监控

7.1.1 应具备对系统状态实时监控的能力，包括物理服务器状态、虚拟机状态、数据库服务状态、节点同步状态等。
7.1.2 应支持自定义设置监控采集数据资料库保存时间。
7.1.3 应支持自动警告推送功能。
7.1.4 宜具备系统状态监控结果实时可视化展示的能力。

7.2 设备管理

7.2.1 加密机应放于专门区域，指定专人管理，并定期进行维护管理。
7.2.2 应采用白名单机制控制对加密机的访问，阻止非授权设备访问加密机。
7.2.3 在报废加密机前，应将加密机内的密钥完全清除，确保加密机内的密钥等敏感数据无法被恢复重用。
7.2.4 严格控制加密机的变更操作，经过审批后才可进行变更操作，并须留下变更相关的审计日志。
7.2.5 加密机以外的设备应遵循 GB/T 22239 中的相关要求。
7.2.6 对网络中的节点性能，需要根据实际承载的业务场景协商接入标准。
注：网络中节点性能指标包括CPU、内存、带宽等指标。

7.3 数据/漏洞维护管理

7.3.1 漏洞发现/修复要求

7.3.1.1 涵盖节点服务器自身漏洞、软件漏洞、智能合约漏洞等不同层次漏洞至少每月扫描一次。扫描时可合理采用第三方扫描工具。
7.3.1.2 漏洞扫描记录保持与扫描策略一致，发现漏洞及时提出修改方案并修复，对于无法修复的漏洞及时报告，如果漏洞修复影响到账本数据，则应通过共识协议进行数据的修正。系统日志留存记录，达到漏洞修复可追溯的效果。

7.3.2 数据备份/恢复要求

7.3.2.1 数据备份策略根据业务需要进行实时备份。
7.3.2.2 密钥等关键数据备份策略根据业务需要进行定期备份。
7.3.2.3 根据密钥等关键数据的恢复策略定期进行恢复演练，最近一次恢复记录表明备份数据的可用性，保证在出现重大事件时能够及时的进行数据恢复。