ICS 91.010.30
P 00

# 团 体 标 准

T/GDCSA 003—2020

# 信息技术应用创新项目综合绩效评估规范

**Information system for Performance evaluation**

2020－**－**发布 2020－**－**实施

广东省网络空间安全协会
信息技术创新联盟 发布

# 目　　次

# 前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由***提出。

本标准由广东省网络空间安全协会和信息技术创新联盟归口。

本标准起草单位：　。

本标准主要起草人：　。

本标准是首次发布。

# 信息技术应用创新项目网络安全绩效评估规范

## 1 范围

本标准规定了信息技术应用创新项目网络安全绩效评估的要素和方法。

本标准适用于组织或第三方评价机构对信息技术应用创新项目网络安全的绩效评估工作。

## 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 25069-2010 信息安全技术 术语

## 3 术语和定义

下列术语和定义适用于本文件。

3.1

**自主可控 independently controllable**

依靠自身研发设计，全面掌握产品核心技术，实现信息系统从硬件到软件的自主研发、生产、升级、维护的全程可控。

3.2

**通信安全 communication security**

保护网络中所传输信息的完整性、保密性、可用性等。

3.3

**入侵防护 intrusion prevention**

是一种可识别潜在的威胁并迅速地做出应对的网络安全行为。

3.4

**网络安全 cyber security**

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

3.5

**身份鉴别 identification**

通过相关技术，将实体标识和实体联系在一起，为其他安全服务提供支撑。

3.6

**绩效评估 performance evaluation**

按照设置的评价指标，对工作业绩进行的评价。

3.7

**经济效益 economic benefit**

从信息化项目产生的直接、间接经济效益出发，表征信息化项目在资金占用、成本支出与有用成果之间的比较。

## 4 评价原则

### 4.1 面向需求原则

确定评估重点和相关细则时应充分考虑信息技术应用创新项目的特点和对应的具体需求。

### 4.2 科学性原则

选择科学的分析及评价方法，坚持定性与定量相结合。

### 4.3 客观性原则

评估所用的数据必须以符合法律、法规及相关文件规定的方式获得，确保数据来源的可靠性、准确性，并根据项目的具体情况，实事求是的开展评估工作。

### 4.4 公正性原则

评估人员要客观、合理的采集信息材料，对项目具体情况进行观察、分析和判断，按照评估要求独立打分，做出相关评价。

### 4.5 系统性原则

评估要全面、综合、系统地考虑各个方面情况。

## 5 评估的主要内容

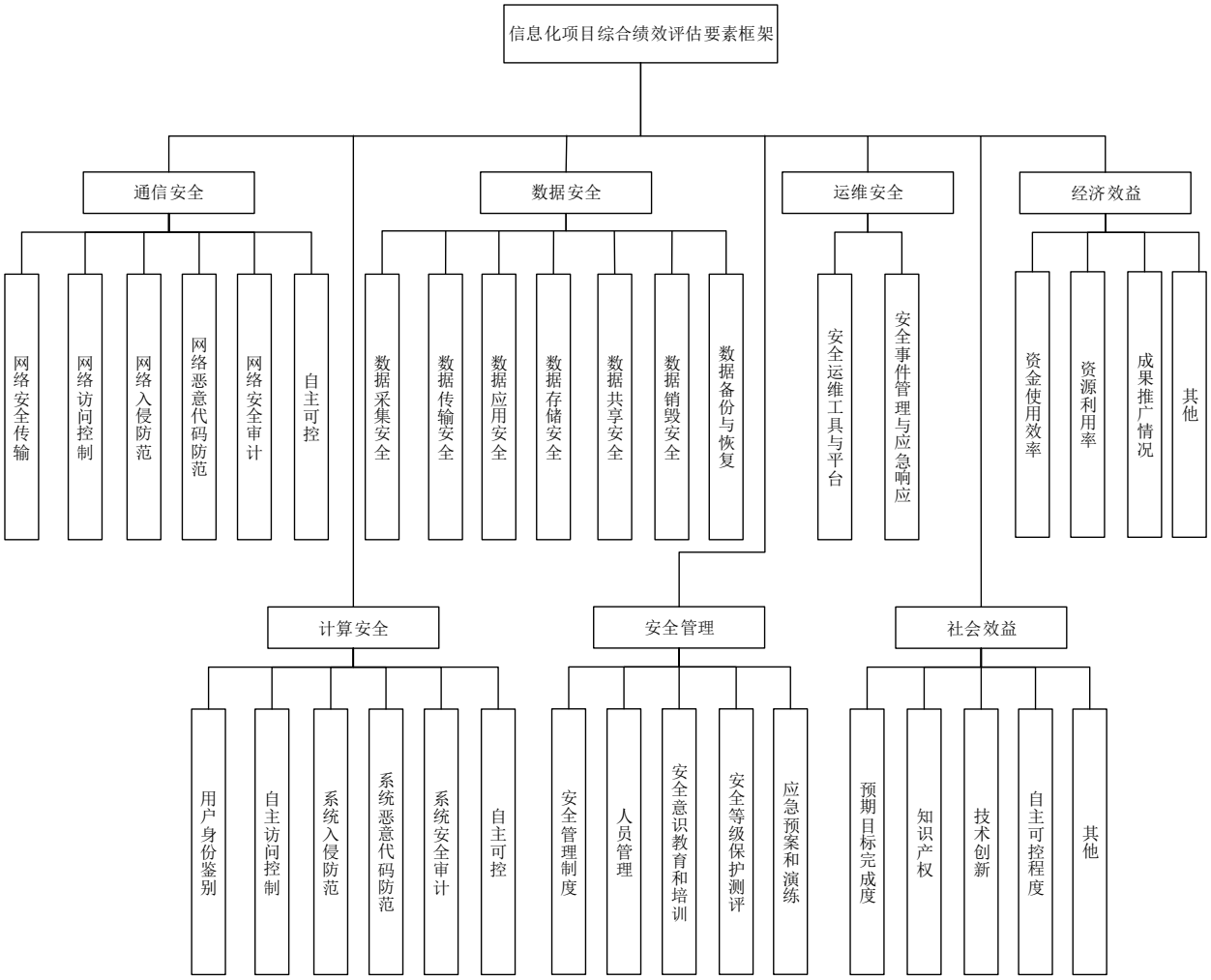


图1 评估的主要内容图

## 6 评估指标

### 6.1 通信安全

信息技术应用创新项目的网络通信安全，是针对通信网络提出的安全控制要求。评估指标包括网络安全传输、网络访问控制、网络入侵防范、网络恶意代码防范、网络安全审计、自主可控等。

表1 通信安全评估指标及要素说明表

| 序号 | 指标名称 | 评估要素 |
|---|---|---|
| 1 | 网络安全传输 | 通信链路是否采用符合国家密码管理局要求的密码技术 |
| 2 | 网络访问控制 | 网络边界和安全区域之间是否采取了访问控制措施 |
| 3 | | 网络内部计算机终端是否采取了违规内外联控制措施 |
| 4 | 网络入侵防范 | 网络边界和网络关键网络节点处是否采取了入侵防范措施 |

| 序号 | 指标名称 | 评估要素 |
| --- | --- | --- |
| 5 | | 入侵防范特征库是否及时更新 |
| 6 | 网络恶意代码防范 | 网络边界和网络关键网络节点处是否采取了恶意代码防范措施 |
| 7 | | 恶意代码特征库是否及时更新 |
| 8 | 网络安全审计 | 网络边界和网络关键网络节点处是否采取了安全审计措施 |
| 9 | | 安全审计日志是否集中存储管理和分析 |
| 10 | | 安全审计日志留存时间是否符合相关法律法规要求 |
| 11 | 自主可控 | 采用的网络产品和网络安全产品是否符合国家公安部的要求 |

## 6.2 计算安全

信息技术应用创新项目的计算安全是针对系统内部应用平台相关方面提出的安全要求。评估的主要对象为网络设备、安全设备、计算机终端、应用系统、数据对象和其他设备等，评估的安全点包括用户身份鉴别、自主访问控制、系统入侵防范、恶意代码防范、系统安全审计以及自主可控等。

**表2 计算安全评估指标及要素说明表**

| 序号 | 指标名称 | 评估要素 |
| --- | --- | --- |
| 1 | 用户身份鉴别 | 应用系统（包含操作系统、业务系统等）是否采取了身份鉴别措施 |
| 2 | | 远程访问和管理是否采取了基于密码技术的身份鉴别措施对用户进行身份鉴别 |
| 3 | 自主访问控制 | 访问控制主体是否采取了细粒度的安全策略控制措施 |
| 4 | | 访问控制客体是否采取了细粒度的安全策略控制措施 |
| 5 | 系统入侵防范 | 应用系统（包含操作系统、业务系统等）是否采取了入侵防范措施 |
| 6 | | 入侵防范特征库是否及时更新 |
| 7 | 系统恶意代码防范 | 计算机终端、服务器主机、云主机等是否采取了恶意代码防范措施 |
| 8 | | 恶意代码特征库是否及时更新 |
| 9 | 系统安全审计 | 应用系统（包含操作系统、业务系统等）是否采取了安全审计措施 |
| 10 | 自主可控 | 采用的网络产品和网络安全产品是否符合国家公安部的要求。 |

## 6.3 数据安全

信息技术应用创新项目的数据处理安全，评估指标包括数据采集、数据传输、数据应用、数据存储、数据共享、数据销毁以及数据的备份与恢复等环节进行安全评估。

**表3 数据安全评估指标及要素说明表**

| 序号 | 指标名称 | 评估要素 |
|---|---|---|
| 1 | 数据采集安全 | 数据采集的权限是否具备精细化的安全控制策略和管理制度 |
| 2 | 数据传输安全 | 数据传输是否采用了符合国家密码管理局要求的密码技术 |
| 3 | 数据应用安全 | 针对访问查询、运维操作等数据使用场景是否设置了访问授权策略 |
| 4 | 数据存储安全 | 是否制定了数据存储安全管理制度 |
| 5 | | 重要数据在存储过程中是否采用密码技术保证数据的完整性和保密性 |
| 6 | 数据共享安全 | 针对软件开发、系统测试、数据共享等涉及敏感数据环节，是否能够自动准确的识别敏感数据并脱敏 |
| 7 | | 脱敏后的数据是否与原数据保持一致的关联关系，是否保证不能被还原 |
| 8 | 数据销毁安全 | 是否制定了数据销毁的流程和方法 |
| 9 | 数据备份与恢复 | 是否制定了数据备份与恢复的管理制度 |
| 10 | | 系统数据和应用系统数据是否采取了数据备份与恢复措施 |
| 11 | | 是否定期开展数据备份恢复演练工作 |

## 6.4 安全管理

信息技术应用创新项目的安全管理，评估指标包括安全管理制度、人员管理、安全意识教育和培训以及安全等级保护测评等。

**表4 安全管理评估指标及要素说明表**

| 序号 | 指标名称 | 评估要素 |
|---|---|---|
| 1 | 安全管理制度 | 网络安全工作的技术和标准是否遵循有关法律制度、政府间协定或国际条约 |
| 2 | | 信息安全工作的总体方针和安全策略是否制定 |
| 3 | | 安全管理制度是否完善 |

| 序号 | 指标名称 | 评估要素 |
| --- | --- | --- |
| 4 | | 安全管理制度是否履行正式的审批发布手续并保持持续有效 |
| 5 | 人员管理 | 是否设立信息安全管理工作的职能部门 |
| 6 | | 是否配备三员：系统管理员、安全保密管理员和安全审计员 |
| 7 | 安全意识教育和培训 | 是否制定年度安全意识教育和培训计划 |
| 8 | | 是否根据培训计划实施培训 |
| 9 | 安全等级保护测评 | 项目建设完成后是否完成网络安全等级保护测评 |

### 6.5 运维安全

信息技术应用创新项目的运维安全，评估指标包括安全运维工具与平台、安全时间管理与应急响应等。

**表5 运维安全评估指标及要素说明表**

| 序号 | 指标名称 | 评估要素 |
| --- | --- | --- |
| 1 | 安全运维工具与平台 | 是否配备适宜的运维工具、运维平台，方便用户进行自主化运维 |
| 2 | | 是否提供统一的运维接入、身份认证及操作权限管理，规范运维管理 |
| 3 | 安全事件管理与应急响应 | 是否建立完善的安全事件响应体系，包括不限于应急预案、事件恢复策略、事件报告规范等 |
| 4 | | 是否按照要求处理安全事件并详细记录，确保系统业务正常运转，并在事后及时总结分析 |

### 6.6 社会效益

信息技术应用创新项目的社会效益，评估指标包括预期目标完成度、知识产权、技术创新、自主可控程度及其他方面等。

**表6 社会效益评估指标及要素说明表**

| 序号 | 指标名称 | 评估要素 |
| --- | --- | --- |
| 1. | 预期目标完成度 | 信息和信息系统的属性是否达到预期保障效果 |
| 2. | | 项目质量指标是否达标 |
| 3. | | 项目管理指标是否达标 |

| 序号 | 指标名称 | 评估要素 |
| --- | --- | --- |
| 4. | | 是否达到建设方案中的其他预期绩效 |
| 5. | 知识产权 | 项目成果转化为发明专利情况 |
| 6. | | 项目成果形成论文并发表情况 |
| 7. | | 项目成果转化标准情况 |
| 8. | | 项目成果转化为其他知识产权情况 |
| 9. | 技术创新 | 技术首创性：项目成果被列入国家及省市的信息技术应用创新相关产品名录 |
| 10. | | 技术先进性：项目成果获得国家及省市等相关奖项 |
| 11. | | 技术影响力：项目对网络安全秩序、安全管理与体制是否有积极影响；对网络安全管理工作发展态势影响是否具有长远性影响 |
| 12. | 自主可控 | 技术能力：网络安全相关代码受控情况 |
| 13. | | 供应链：软硬件产品自主生产情况 |
| 14. | 其他 | 对管理能力的提升是否具有促进影响 |
| 15. | | 是否存在技术壁垒影响区域交流与合作 |

## 6.7 经济效益

**表7 经济效益评估指标及要素说明表**

| 序号 | 指标名称 | 评估要素 |
| --- | --- | --- |
| 1. | 资金使用效率 | 资金管理是否达标 |
| 2. | | 资金使用效率=实际使用资金/计划使用资金×100%<br>资金使用效率指标评价时使用区间偏离情况，以100%为中值的为最佳区间 |
| 3. | 资源利用率 | 设备利用率=实际在用设备/所有设备×100% |
| 4. | | 基础设施利用率 |
| 5. | | 设备或系统运行效率 |
| 6. | 成果推广情况 | 项目成果在同类项目中应用推广情况 |
| 7. | 其他 | 标准化程度 |

| 序号 | 指标名称 | 评估要素 |
| --- | --- | --- |
| 8. | | 对网络安全风险的预防是否有效 |

## 7 评估程序

### 7.1 评估准备

#### 7.1.1 确定绩效评估范围

信息技术应用创新项目通过验收正式运行六个月后，开展实施项目的网络安全综合绩效评估工作，确定被评估对象，进行初步调研，确定绩效评估范围，并下发绩效评估通知。

### 7.2 组建绩效评估团队

绩效评估实施小组由委托方任命，由组长、评估技术人员以及保障人员构成。必要时，应聘请相关专业的技术专家和技术骨干担任顾问。

### 7.3 系统调研

系统调研时了解、熟悉被评估对象的过程，调研内容包括（但不限于）：

网络安全相关内容：

a）系统完成情况；

b）信息安全管理制度；

c）网络安全建设情况；

d）预期效益达成情况。

### 7.4 编制评估方案

绩效评估方案是实施评估活动的总体计划，用于指导绩效评估小组开展后续工作。绩效评估方案一般包括（但不限于）：

a）被评估系统概述；

b）绩效评估策略：包括评估指标选取和分值的确定，综合分值算法等；

c）评估团队介绍：包括被评估团队成员、组织结构、角色、责任等；

d）时间进度安排。

### 7.5 评估实施

根据绩效评估方案收集数据，计算各指标单项分值，并按照绩效评估方案的评估策略计算出综合分值。

### 7.6 评估总结

根据评估实施阶段获得的数据，结合项目情况，得出绩效评估的综合得分，得出并编制绩效评估报告。

## 8 评估方法

### 8.1 评估指标选取

绩效评估应覆盖所有一级指标，并根据评估对象的实际情况选择相应的二级指标进行评估。当选取部分二级指标进行评估时，未被选取的指标所占分值以恰当的方式计入已选取指标中。

### 8.2 得分评定

采用单项评估指标根据所占权重综合评定，计算公式见式（1），单项评估指标所占权重范围见表1。

$$E=\sum_{n=1}^{6}K_nC_n \qquad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots（1）$$

其中，

E – 综合绩效评估值，取值范围为0～100；

$K_n$ – 第n个评估指标所占的权重值，所有权重值之和为1；

$C_n$ – 第n个评估指标得分值，取值范围为0～100。

各项指标权重占比如下见表1。

**表8 权重占比一览表**

| 序号 | 指标名称 | 权重占比 |
|---|---|---|
| 1 | 通信安全 | 15%至20% |
| 2 | 计算安全 | 10%至15% |
| 3 | 数据安全 | 10%至15% |
| 4 | 安全管理 | 10%至15% |
| 5 | 运维安全 | 10%至15% |

| | | |
|---|---|---|
| 6 | 社会效益 | 5%至 10% |
| 7 | 经济效益 | 5%至 10% |

## 9 结果评价

### 9.1 初始等级计算

按照得分由高至低分为：优（≥90）、良（<90，≥80）、中（<80，≥70）、可（<70，≥60）、差（<60）5 级。

每个一类指标根据得分进行单独评价，得到分项初始等级；

综合评估结果按照公式（1）的计算结果进行评价，得到项目初始等级。

### 9.2 最终等级评估

出现两项或以上的分项初始等级低于项目初始等级情况下，项目最终等级比最低的分项等级最多高一档。

# 附　录　A
（规范性附录）
评估报告模板

**（项目名称）项目绩效评价报告**

（文档编号）

XXXX 年 XX 月 XX 日

（评估单位名称）

| 一、项目基本概况 | |
|---|---|
| 项目名称 | |
| 项目编号 | |
| 项目金额 | |
| 项目描述 | （对项目情况以及项目建设内容进行描述。） |
| 评估依据 | |
| 检查地点 | |
| 绩效评估结果 | （对项目的绩效评价等级做整体描述） |

## 二、评价报告综述

（一）项目基本概况

（描述被评估项目的基本情况。）

（二）项目绩效评估策略说明

（对本次项目绩效评估策略进行说明，包括一级指标系数确定、二级或三级指标选取方式等）

（三）项目绩效及评价结论

（描述本次项目绩效评价的综合结论，并按照一级指标的维度简单评价指标满足情况。）

（四）评价发现的问题

（描述本次项目绩效评价中得分相对较低的分项存在的问题。）

（五）相关意见与建议

（根据上述问题，给出相关建议。）

**附录：项目绩效评价指标完成情况**

（针对评估过程指标的完成情况填写）

| 项目绩效评价指标完成情况 | | | |
|---|---|---|---|
| **一级指标** | **二级指标** | **三级指标** | **指标完成情况** |
| | | | |
| | | | |