ICS 03.060

CCS L 6650

**T/CCUA**

|  |
| --- |
|  |

|  |
| --- |
|  T/CCUA XXXX—XXXX  |

|  |
| --- |
|  |

中国计算机用户协会 发布

金融信息科技审计

基本框架与原则

**Financial information technology audit - Basic framework and principles**

团体标准

**（征求意见稿）**

（在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上）

2XXX – XX – XX发布

2XXX – XX – XX实施

目 次

[前言 II](#_Toc24354)

[1 范围 1](#_Toc30268)

[2 规范性引用文件 1](#_Toc23039)

[3 术语和定义 1](#_Toc31603)

[4 金融信息科技风险分析 2](#_Toc6416)

[4.1分析内容 2](#_Toc16824)

[4.2分析方法 2](#_Toc27894)

[5 金融信息科技审计标准框架 2](#_Toc16016)

[6 金融信息科技审计基本原则 3](#_Toc15318)

[6.1 合法合规原则 3](#_Toc20355)

[6.2 独立客观原则 3](#_Toc2725)

[6.3 安全保密原则 4](#_Toc5173)

[6.4 专业有效原则 4](#_Toc11858)

[6.5 风险导向原则 4](#_Toc17537)

[6.6 持续关注原则 4](#_Toc31117)

[7 其他 4](#_Toc17420)

[7.1 审计目标 4](#_Toc30292)

[7.2 审计规划和计划 4](#_Toc32288)

[7.2 审计结果的有效期 5](#_Toc20227)

[附录A （资料性） 金融信息科技风险分析矩阵 6](#_Toc18548)

[参考文献 7](#_Toc6357)

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。

金融信息科技审计标准包括基本框架与原则、审计机构与审计人员、审计过程、审计方法、审计工具、具项审计细则和审计评价等部分，本文件是金融信息科技审计标准的第一项标准。

本文件由中国计算机用户协会提出并归口管理。

本文件起草单位：中国计算机用户协会信息科技审计分会、深圳前海微众银行股份有限公司、国家开发银行、中国进出口银行、中国工商银行股份有限公司、中国农业银行、中国银行股份有限公司、中国建设银行股份有限公司、中信银行股份有限公司、华夏银行股份有限公司、厦门国际银行股份有限公司、洛阳银行股份有限公司、武汉众邦银行股份有限公司、安徽省农村信用联合社、太平金融稽核服务（深圳）有限公司、中信建投证券股份有限公司、山东重工集团财务有限公司、农信银资金清算中心、中治研（北京）国际信息技术研究院、中国信息通信研究院、全球能源互联网研究院、南京审计大学、北京信息科技大学、招银云创（深圳）信息技术有限公司、深圳前海普华永道咨询管理公司、北京中润长弘管理咨询有限公司、北京银丰新融科技开发有限公司、北京同创永益科技发展公司。

本文件主要起草人：金磐石、闫振平、孙卫东、杨晓平、杜宁宁、吕震浩、王立校、郝超、王琰、洪振龙、刘文星、顾呈页、王鹏虎、李艳东、于锋、崔玉玺、王中央、罗锋、朱道荣、张建军、方立雄、李治平、尹君、魏东、牛晓玲、郭昊、余小兵、崔国玺、陈欣炜、杨丰禹、李长征、王润丰、阎若彤、孙启仲、冯永生、王衍锋、邱庆华、颜涵、窦春坦、翁雨烟、陈雪、周玉、蔡茂森、王刚、李海龙、薛君敖、贺晓红、朱斌、杨玲玲、郭昊、方渝军、王东红、何小芸、王晓宁、孙阳、樊宇。

金融信息科技审计

基本框架与原则

1. 范围

本文件主要规定了金融信息科技审计标准框架及制定、实践标准的基本原则。

本文件适用于金融信息科技审计标准的规划与制定及风险控制。也适用于任何开展金融信息科技内部控制、风险评估和审计的机构。

1. 规范性引用文件

本文件没有规范性引用性文件。

# 术语和定义

下列术语和定义适用于本文件。

3.1

金融信息科技 financial information technology

是指涉及金融服务的机构所应用的计算机、通信、微电子、软件工程等现代信息技术，包括云计算、大数据、区块链和AI等应用。

3.2

金融信息科技风险 financial information technology risk

是指信息科技在金融服务应用的生命周期和结果可能产生的操作、法律、声誉和系统性金融风险。

3.3

金融信息科技审计 financial information technology audit

对金融信息科技风险和控制进行的独立、客观的监督、评价与咨询活动。包括但不限于其运行的基础设施、信息系统和输入输出数据、治理和管理规程等。

3.4

金融信息科技审计服务机构 financial information technology audit service institution

是指开展金融信息科技审计服务的专业机构。

3.5

审计工具 audit instrument

审计工作中利用技术手段进行检查和验证的辅助工具，以及为提高审计的能力水平、效率效果和规范性而使用的专用工具或方法。

# 金融信息科技风险分析

金融信息科技审计应以风险分析为基础。

## 4.1分析内容

信息科技风险分析的内容包括但不限于：

1. 风险识别、计量、监测、控制机制;
2. 控制机制有效性;
3. 风险事件的影响程度和发生概率。

## 4.2分析方法

4.2.1 应对各种风险事件的影响程度进行分类，影响程度可分为五类:

1. 低：非关键控制失效，无明显影响；
2. 较低：非关键控制失效、影响非重要业务；
3. 中：部分关键控制失效，影响非重要业务；
4. 较高：关键控制实效，影响重要业务；
5. 高：控制丧失，系统性影响机构运行。

4.2.2 应对各种风险事件发生的概率进行分类，发生概率可分为五类：

1. 低；
2. 较低；
3. 中；
4. 较高；
5. 高。

4.2.3 实施信息科技审计应建立信息科技风险分析矩阵，每个风险事件应在矩阵上被量化，确定该事件的影响程度和发生概率，以确定风险事件的强度，并做出降低风险的建议。信息科技风险分析矩阵是信息科技审计风险分析工具，见附录A。

# 金融信息科技审计标准框架

金融信息科技审计标准体系包括外部监管要求、企业内部的管理规定和金融信息科技审计标准三部分，如图1所示。虚线框表示依据的规范、标准和制度监管要求以及企业内部的规章制度，这些不属本文件的范畴。实线框表示本系列标准主要涉及的内容。



图1 金融信息科技审计标准框架

金融科技审计标准主要包括：基本框架和原则、审计机构与审计人员、审计过程、审计方法、审计工具、金融信息科技具项审计细则和审计评价七部分，其中：

1. 金融信息科技审计基本框架和原则：规定了金融信息科技审计标准的体系框架，以及应遵循的基本原则
2. 审计人员与机构：规定了从事金融信息科技审计工作的人员的能力水平要求，金融业内部审计机构、第三方金融信息科技审计服务机构资质能力要求
3. 审计过程：规定了内部和第三方金融信息科技审计服务机构审计过程管理的规范性要求
4. 审计方法：规定了开展金融信息科技审计的可采取的方法的规范性要求
5. 审计工具：规定了金融信息科技审计工具的选择、建设、应用和管理的规范性要求
6. 具项审计细则：规定了具体金融信息科技审计项目及规范性要求
7. 审计评价：规定了金融信息科技审计合规与价值评价方法、模型等规范性要求

# 金融信息科技审计基本原则

## 6.1 合法合规原则

金融信息科技审计应依据相应的法律、法规、制度、流程等要求，开展相关场景审计工作，提出审计意见和结论。应包括：

1. 金融信息科技审计应遵循国家相关的法律法规、监管和行业规范与指引；
2. 金融信息科技审计应依据被审计机构或组织内部规章制度；
3. 金融信息科技审计应依据被审计机构或组织与相关方的合同或协议。

## 6.2 独立客观原则

金融信息科技审计应保持独立、客观、公正，确保审计监督真实有效。

## 6.3 安全保密原则

金融信息科技审计服务机构及人员应遵守信息安全和保密规定。应建立对审计活动中相关人员、信息和活动的信息安全和保密机制，包括但不限于：

1. 应建立对审计人员的职业道德、信息安全、保密教育、考核机制；
2. 应对审计过程中接触到的被审计服务机构及其服务相关方的敏感信息、被发现的系统的缺陷等信息建立保密机制；
3. 应有效评估审计技术测试过程可能带来的安全风险，制定有效的防范措施；
4. 对审计过程中发现的技术缺陷、测试结果，应通知有关各方；
5. 审计测试工具应经过安全性测试。

## 6.4 专业有效原则

金融信息科技审计应保持专业性和有效性，包括：

1. 金融信息科技审计服务机构应建立持续的审计专业人员培养、考核机制，保障人员专业能力的有效性；
2. 应建立对审计范围的专业性能力覆盖和涉及的技术及应用的持续研究机制；
3. 应建立对金融信息科技审计服务机构自身的专业性评估机制。

## 6.5 风险导向原则

金融信息科技审计应坚持风险导向原则，在风险评估的基础上，开展审计工作，包括：

1. 应建立综合风险识别、缺陷评估、控制有效性分析的风险管理机制；
2. 应根据审计发现、风险评估，监督被审计机构制定有效的整改、控制措施；
3. 应建立对科技创新、管理创新的风险和价值评估机制。

## 6.6 持续关注原则

金融信息科技审计服务机构应持续关注审计发现和结果的变化，包括：

1. 金融信息科技审计服务机构应建立持续关注审计发现的整改情况和风险变化的机制；
2. 应建立审计结果的汇报或通报机制；
3. 应建立对审计内容的技术与控制变化跟踪机制。

# 其他

## 7.1 审计目标

金融信息科技审计服务机构应根据合法合规和风险导向要求确定审计目标。

## 7.2 审计规划和计划

金融信息科技审计服务机构应根据审计目标确立信息科技审计规划和计划，保障审计周期内对审计目标的有效覆盖。

## 7.3 审计结果的有效期

金融信息科技审计结果有效期为3年。如果在此期间被审计机构发生重大的风险结构变化，审计结果应同时失效，应重新审计或对变化的部分进行专项审计。

1.
2.
3. （资料性）
信息科技风险分析矩阵

信息科技风险分析矩阵见图A.1



图A.1 信息科技风险分析矩阵图

参考文献

[1] ISO/IEC 38500:2015 信息科技 IT治理

[2] GB/T 34960.1-2017 信息技术服务 治理 第1部分：通用要求

[3] GB/T 34960.4-2017 信息科技服务 治理 第4部分：审计导则

[4] 企业内部控制审计指引，中华人民共和国财政部（财会[2010]11号）

[5] 金融信息科技发展规划（2019-2021年）,中国人民银行（银发[2019]209号）

[6] 银行业信息科技风险监管指引，中国银行保险业监督管理委员会

[7] 内部审计基本准则，中国内部审计协会（2013年第1号公告）

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_