广东省地方标准《信息系统内部风险管理基本要求》编制说明

一、 工作简况

1.1 任务来源

根据广东省市场监督管理局于2019年下达的广东省地方标准制修订计划（粤市监标准【2019】850号），《信息系统内部风险管理基本要求》由广东省信息安全测评中心作为牵头单位。该标准行政主管单位为广东省国际问题研究中心，技术归口单位为广东省网络空间安全标准化技术委员会。

1.2 起草单位

本标准由广东省信息安全测评中心牵头，广东安络司法鉴定所、广东外语外贸大学、广州华南信息安全测评中心和东莞市公共资源交易中心等共同参与了该标准的起草工作。

1.3 主要工作过程

（1）2020年3月，组织参与本标准编写的相关单位召开项目启动会，成立标准编制小组，确立各自分工，进行初步设计，并听取各参与单位的相关意见。

（2）2020年5月，编制组对国内外信息系统管理风险内部控制现状做了探讨，进一步佐证了标准制定的必要性以及提供了标准制定的依据。

（3）2020年7月，编制组结合研讨结果，提出详细的标准制定

计划，形成标准草案第一稿。

（4）2020 年 11 月，编制组召开组内研讨会，基于前期成果，经多次内部讨论研究，组织完善草案内容，包括增加职权电子化过程模型、细化电子岗位类别、修改标准适用范围等内容，形成标准草案第二稿。

（5）2021 年 3 月，编制组继续研究讨论，对草案进行进一步修改，形成标准草案第三稿。

（6）2021 年 4 月，为提升标准编写能力和推动标准验证推广，经编制组研究讨论，同意广州华南信息安全测评中心和东莞市公共资源交易中心等两家单位加入标准编制组。

（7）2021 年 5 月，编制组召开草案第三稿讨论会，编制组对草案进行深入讨论。根据讨论结果，编制组对草案的框架进行调整，将组织层面控制要求和电子岗位控制要求两部分合并，统一改为基本要求，共有 8 点具体要求，形成标准草案第四稿。

（8）2021 年 8 月，编制组进一步对草案进行认真研究讨论和修改完善，形成征求意见稿。

（9）2021 年 9 月 27 日-10 月 24 日，编制组向社会公开征求意见，共收到 52 家单位反馈意见，其中提出意见的单位有 13 家，无意见的单位有 39 家。共反馈 41 条意见，其中采纳 24 条，不采纳 17 条。

（10）2021 年 11 月-2022 年 3 月，编制组针对反馈意见对草案进行进一步研讨和修改完善，形成送审稿。

（11）2022 年 3 月 18 日，举行标准审定会，专家组共提出 37

条意见，建议标准名称修改为《信息系统内部风险管理基本要求》。专家组一致同意该标准通过审定。

（12）2022 年 3 月-2022 年 4 月，编制组针对审定会专家意见对标准进行进一步研讨和修改完善，其中采纳 34 条，部分采纳 1 条，不采纳 2 条，形成报批稿初稿。专家对报批稿初稿提出 6 条意见，其中采纳 4 条，不采纳 2 条，最终形成报批稿。专家无意见，同意上报。

（13）2022 年 5 月 15 日-6 月 15 日，标准行政主管单位广东省国际问题研究中心将标准报批稿向社会公开征求意见，因该中心无官方网站、公众号等对外发布渠道，故委托广东省网络空间安全标准化技术委员会的平台进行对外意见征集。

二、 立项的必要性

2.1 行业发展现状

随着信息技术的迅猛发展，一方面信息系统使我们享受着前所未有的方便与效益，同时由于信息系统本身的新特征及其应用环境的复杂性也给信息系统的管理带来了新的问题与挑战。国内外相关组织和学术界早已开始对信息系统的管理风险与控制进行研究，但至今还没有形成公认的、权威的体系。针对信息系统管理风险的内部控制问题，1977 年 IIA 发布了《信息系统可审计性与控制》的报告，1991 年鉴于 IT 业发生的巨大变化进行了更新，2001 年公布了信息系统控制模型“电子系统保证与控制”。同时，美国信息系统审计与控制协会在 1996 年公布了《信息及相关技术控制目标》（COBIT），2007 年，COBIT4.1 从 IT 治理的角度以及更高的层面指导管理层对信息系统管

理风险进行控制，2012 年 COBIT5 进一步融合了风险管理、IT 运维最佳实践，但对于信息系统管理风险的内部控制整体要求仍缺乏具体可落地的指导性要求。1992 年，COSO 发布了《内部控制-整合框架》，在其中列出了信息系统的相关控制，包括一般控制和应用控制，但其主要还是基于传统的内部控制理论，依赖于岗位分置和监控等活动。2002 年，美国国会出台了 SOX 法案，其第 404 条款中对内控体系建设提出了明确要求，其中就包括信息系统的控制体系建设。

虽然我国内部控制的理论研究起步较晚，但根据我国信息化的发展现况和趋势，有关部门在制定相关政策时也考虑到信息安全对内部控制的影响。1999 年，中国注册会计师协会的《独立审计具体准则第 20 号-计算机信息系统环境下的审计》，明确规定应充分关注计算机信息系统的特性以及其对审计的影响。2006 年，《上市公司内部控制指引》中第十条规定，公司使用计算机信息系统的，还应制定信息管理的内控制度。2008 年，五部委联合发布的《企业内部控制基本规范》中也包含了信息系统的内部控制相关要求。2009 年，银监会颁发《商业银行信息科技风险管理指引》，大量借鉴了 COBIT、ITIL 等管理理论，为信息系统管理风险内部控制奠定了坚实基础。2015 年，财政部在原有的《财政部内部控制基本规范》基础上，对其中信息系统管理风险部分进行了细化，出台了《财政部信息系统管理风险内部控制办法》(试行)，成为我国首份行业内信息系统管理风险内部控制规范。

回顾我国信息安全的发展历程，大部分时间我国的信息安全重点

关注方向在于信息系统自身的技术风险，长期处于重技术轻管理阶段，对于信息系统管理风险的内部安全控制缺乏整体性要求以及相应的标准、规范与要求。但从各行业研究情况来看，信息系统管理风险的内部安全控制是信息安全整体保障的关键，各行业主管部门开始越来越重视信息系统管理风险内部控制的作用与意义。

当前，信息技术已深入应用到我国国防、科研、政府、企业等大部分核心业务，信息安全管理的重要性日益凸显。值得注意的是，据统计信息安全威胁80%来自于单位内部管理漏洞，其根本原因在于在信息系统建设时大部分单位重技术轻管理这一现实情况。因此，信息安全管理风险的内部安全控制体系建设将会成为我国信息安全保障体系建设的重要组成部分。

2.2 行业存在痛点

信息化建设的业务安全风险特别是电子政务安全问题日益突出，各单位在信息化过程中，相关人员的决策权、执行权和监督权映射到信息系统中产生电子业务权力和电子技术权力。信息系统管理风险内部控制是否合规，决定了电子权力能否正常映射运行。同时，管理风险的安全隐患很可能会导致包括核心国家机密的外泄、政府部门公信力下降、企业核心机密与国有资产流失等重大损失。因此，强化信息安全管理风险控制，建立信息系统内部风险管理基本要求具有非常重要的意义。

信息系统管理风险内部控制的目的是为了加强信息系统管理内部控制，有效防控信息系统管理风险，提高信息系统建设与管理的规

范性和科学性，加强信息化对业务管理的支撑与流程控制能力，最大程度地减少人为恶意操纵的可能性，确保系统运行和业务流程控制的有效性，及权利行使的合规性。

2.3 拟定解决的问题

通过对本标准的制定，主要解决了现行标准的实用性问题，具体内容包括：

（1）定义了职权电子化、电子业务权力、电子技术权力、电子岗位等信息的含义。

（2）规范了信息系统业务职权电子化过程、业务流程、关键控制点、电子权力运行、电子岗位责权、敏感数据保护等方面的风险管控要求。

三、 标准编制原则和标准编制详细说明及解决的主要问题

3.1 编制原则

本标准的研究与编制工作遵循以下原则：

（1）通用性原则

本标准是参考 GB/T 20269 信息安全技术 信息系统安全管理要求、GB/T 20984 信息安全技术 信息安全风险评估规范、GB/T 29245 信息安全技术 政府部门信息安全管理基本要求等标准制定的，对相关标准在职权电子化过程中的应用，做了进一步补充、完善与细化。既保证标准编制内容的科学性，又使得标准内容更加符合我国国情。

（2）符合性原则

遵循国家现有信息安全相关标准，符合国家现有法律法规和已编

制标准规范的相关要求，符合国家主管部门的要求。

（3）实用性原则

本标准规范是对实际工作成果的总结与提升，保持整体结果合理且维持原意和功能不变，针对不同的用户群体，做到可操作、可用与实用。

（4）完备性原则

本标准的完备性原则主要体现在两个方面：其一充分分析了职权电子化的全过程，从整体方面对职权电子化涉的业务流程合规、关键要素控制，以及信息系统运行安全状况等制定了风险控制要求；其二考虑到电子权力管控要求，制定了信息系统运行时电子业务权力和电子技术权力执行过程的风险控制要求，以及敏感信息安全防护的基本要求。因此本标准作为通用性的信息系统管理风险内部控制要求，可适用于大多数政府及企事业单位的信息系统。

3.2 标准框架

《信息系统内部风险管理基本要求》文档分为前言、引言、范围、规范性引用文件、术语和定义、内部风险管理原则、内部风险管理要求、附录、参考文献等九部分。

3.3 整体格式

整体格式根据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》的相关要求，对本标准的各要素进行编写和排版。

在标准内容汇总过程中，对各编写组成员提交过来的部分，根据

GB/T 1.1 的编写要求进行了必要的增删改，以确保符合一致性、协调性、易用性等文件的表述原则及相关规定。

3.4 术语和定义

术语和定义中所列的术语的英文翻译，根据各部分编写成员提供的术语，如有类似术语的标准，参考了其翻译，没有类似术语标准翻译的，通过百度翻译和谷歌翻译后进行对比，并参考网络相关翻译后进行确定。

3.5 结构与内容

《信息系统内部风险管理基本要求》规定了政府及企事业单位在职权电子化过程中应围绕着信息系统的全生命周期，对信息系统运行过程中的每个环节所涉及的业务合规性、职权电子化过程、电子权力运行、敏感数据保护等因素进行内部风险管理。详情如下：

（1）总体要求

从风险管控的总体规划、职权电子化进程的监管、评估与控制程序、风险例外策略、协助监管等方面提出管控要求。

（2）合规性要求

从业务的流程、业务的关键控制点、系统的自主安全等方面提出须符合法律法规要求。

（3）职权电子化管理要求

从职权电子化对应关系、电子岗位权限设计、职权电子化建设过程、权责分离等方面提出控制要求。

（4）电子权力运行管理要求

从电子权力运行前的系统风险评定、电子权力清单、电子权力运行过程的监控、电子权力运行过程的审计、电子权力运行的连续性、电子权力运行的责权、技术控制的有效性、变更控制、敏感信息防护等方面提出管理要求。

（5）敏感数据保护要求

从敏感数据的识别、分类、分级、产生、存储、访问、应用等过程提出保护要求。

（7）持续改进机制要求

《信息系统内部风险管理基本要求》遵从PDCA原则，从系统自身安全评测；信息系统管理风险内部控制的自查、督查、评估；电子权力运行的稽核等方面提出周期性的工作要求。

（8）宣传与培训要求

沟通与交流主要从技术交流、培训宣贯、人员继续教育、绩效考核等方面提出要求。

3.6 参考文献

本部分列出了在本标准编写过程中所参考的主要文献名称。

四、 与现行相关法律、法规、规章及相关标准的协调性

建议本标准推荐性实施。本标准不触犯国家现行法律法规，不与其他强制性国标相冲突。

五、 标准有何先进性或特色性

《信息系统内部风险管理基本要求》是经历3年创新，6家政府单位的创新实践总结而来的。由多家单位一同发起，在基于网络与信

息安全方法论上，结合国家职权电子化的成功实践，融入COSO、COBIT、ISO 27000等标准思想，进而设立编制的。

本标准开创了两项第一。一是第一个对电子权力、电子业务权力、电子技术权力、电子岗位、电子业务管理岗、电子人事岗、电子财务岗、电子监察审计岗进行定义的标准；二是第一个对职权电子化演变过程进行描述，且从业务流程控制、业务关键点控制提出管控要求的标准。

其特点是将网络安全、信息安全、数据安全、业务安全、安全审计等与行政监管要求融合在一起，可通过网络安全风险映射出权力电子化后运行在信息系统时的行政监管风险，从而为政府、企事业单位提供科学的风险控制机制。

六、 重大分歧意见和处理经过和依据。

《信息系统内部风险管理基本要求》编制过程中未出现重大分歧。

七、 技术指标设置的科学性和可行性。

根据职权电子化全过程，本标准从管理、技术、运行、数据、持续改进及宣传六个方面对指标进行设置，共含7类62项指标要求。各指标在东莞市公共资源交易中心、广州市公共资源交易中心、东莞市建设工程交易中心、东莞市土地交易中心、佛山科技局、佛山公积金管理中心等单位均得以成功验证，且实践证明各单位通过开展信息系统管理风险内部控制工作，使其风险防控水平得到较大提升，很好的预防了行政权力行使和监管中存在的不良风险。

综上，通过项目的实践论证和专家的专业审核，足以说明该指标

的设置具备科学性和可用性。

八、 采用国际标准和国外先进标准情况

无。

九、 产业化情况、推广应用论证和预期达到的经济效果

目前，广东省数字政府改革建设已迈进新阶段，政府即将大力推动“一网通办”政务服务体系和“一网统管”省域治理新模式。通过近些年传统网络与信息安全建设，政府单位的网络安全整体状况良好，但信息系统管理风险内部的管控还存在一定缺失。

截止到2019年底，共有6家政府单位开展过信息系统管理风险内部控制工作，相继发现在职权电子化建设过程中存在业务流程不合规、关键要素未得到有效控制、岗位职权不明确、岗位职权未有效分离、越权绕权等高风险问题。但通过后续整改，管理风险得到有效控制，避免了因管理风险导致的行政审批不合规、职权滥用、行政越权、业务纠纷等问题。

《信息系统内部风险管理基本要求》旨在解决业务职权电子化过程中的业务合规、权责分明、电子权力控制有效等问题。本标准发布后，将可以为政府及企事业单位的信息系统管理风险内部控制提供科学依据。

十、 知识产权情况说明

本标准不涉及专利。

十一、标准性质的建议

建议《信息系统内部风险管理基本要求》作为推荐性省级标准发

布实施。

十二、贯彻标准的要求和措施建议

鉴于信息系统内部风险管理基本要求的标准，建议在标准贯彻执行过程中，政府及企事业单位网络运营者应当起到协调以及推广的作用，召开研讨会、协调会，政府及企事业单位首先使用本标准中的方法进行信息系统管理风险内部控制。

十三、替代或废止现行相关标准的建议

无替代或废止。

十四、其他应予说明的事项

无。

《信息系统内部风险管理基本要求》标准编制组

2022 年 5 月