ICS 35.020
CCS L 70

DB44

广　东　省　地　方　标　准

DBXX/T XXX—XXXX

信息系统内部风险管理基本要求

Basic requirements for internal risk management in information system

（报批稿）

（本稿完成时间：2022-4-26）

2021－XX－XX 发布　　2021－XX－XX 实施

广东省市场监督管理局　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。

本文件由广东省国际问题研究中心提出并组织实施。

本文件由广东省网络空间安全标准化技术委员会归口。

本文件起草单位：广东省信息安全测评中心、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、东莞市公共资源交易中心等。

本文件主要起草人：陈宁、骆林勇、王辉、王文佳、王常吉、袁毅鸣、李虹、李俊华、崔顺艳、邓思贤、谢柏林、宋琅靖、邓艳利、洪松远、何文婷、黄志强、邝建、张新猛、邢静、黄珊珊。

引　言

信息化建设已经进入深度应用阶段，信息系统所面临的安全风险逐步由物理、网络、主机、应用等层面向业务层面发展，给信息系统内部风险管理带来极大挑战，尤其体现在电子政务信息系统方面。组织在信息化过程中，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。业务是否合规、电子权力是否控制有效直接影响信息系统内部风险管理及职权电子化的成效。内部风险管理控制失效会给组织带来不可估量的损失，如国家核心机密外泄、政府部门公信力下降和国有资产流失等。因此，建立信息系统内部风险管理基本要求势在必行，是一项非常紧迫与重要的任务。

信息系统内部风险管理的目的是为了加强组织内部对线下业务和线上业务风险的管理，有效防控信息系统业务风险，提高信息系统建设与管理的规范性、科学性，以及信息化对业务管理的支撑和流程控制能力，最大程度减少人为操纵因素，确保业务、权力及信息系统的安全稳定运行。

本文件综合运用信息安全相关法律法规、标准规范和内审内控方法，将信息系统内部风险管理措施涉及的内控理论和控制活动贯穿于信息系统建设、管理与运营全过程，对组织业务与信息系统业务流程一致性，业务流程中业务活动控制、留痕、人员权力赋予、权力运行过程的风险进行控制，解决信息安全中由于人员行为不可控的因素导致的内部安全问题。

本文件可以作为政府部门、履行行政管理职能的事业单位和国有企业等网络运营者的信息化建设和信息系统内部风险管理控制体系建设的主要依据，也可以作为通信和信息服务、能源、交通、水利、金融等重要行业和领域信息系统内部风险控制体系建设和实施的参考标准。

信息系统内部风险管理基本要求

1 范围

本文件规定了信息系统内部风险管理的术语和定义、原则及要求。

本文件适用于政府部门、履行行政管理职能的事业单位和国有企业等网络运营者，对自身的信息系统内部风险管理情况进行内部审查，也适用于监管单位、第三方审查机构对上述组织进行外部审查，其他组织可参考执行。审查结果可作为组织内部信息化建设和信息系统内部风险管理体系建设的参考依据。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

信息系统内部风险管理 basic requirements for internal risk management in information system

指导和控制组织对内部信息系统风险开展相关协调活动，并管理不确定性，以确保组织业务目标的一致性。

3.2

职权电子化 electronization of authority

以职权为对象，利用信息技术手段将职权运行的部分或全部过程实现电子化。职权电子化既是职权实现电子化的过程，又是职权在网络空间中以另一种形态存在的表现形式。

3.3

线下职权 offline authority

国家法律、法规赋予的组织职权，是由上级组织依法依规授权下级业务部门、责任岗位和人员，依照法定程序履行的权力职责。

3.4

线上职权 online authority

国家法律、法规赋予的组织职权，通过信息化建设映射到信息系统中，形成对应的电子岗位、职权账号和权限。

3.5

电子权力 electronical authority

线下职责权限在信息系统中的映射或嵌入，包括电子业务权力和电子技术权力。

3.6

电子业务权力 electronical business authority

线下业务岗位的职责权限在信息系统中的映射或嵌入。

3.7

电子技术权力 electronical technology authority

岗位角色权力电子化时衍生的一种权限，即对支撑业务运行的计算机网络系统涉及的一系列管理权、控制权和知情权，它具有对电子业务间接的管理权限。

3.8

电子岗位 electronical post

根据线下人员岗位角色权力电子化的要求在信息系统中设立的与线下岗位相对应的虚拟岗位以及实际存在于信息系统及其相关支撑设备中的对应账号与角色。

3.9

电子技术岗 electronical technical post

线下技术岗在信息系统中的映射或嵌入，具有对承载信息系统的操作系统、数据库、中间件、网络与网络安全设备、物理机房等设施的管理、运维、操作、监控等职权。

3.10

电子业务管理岗 electronical business management post

线下业务管理岗在信息系统中的映射或嵌入，具有业务流程的设计建立、合规监督和业务档案管理等职权。

3.11

电子人事岗 electronical personnel post

线下人事岗在信息系统中的映射或嵌入，具有职权电子化后的线上人事架构的设定、人员的任免，人员业务账号及权限的初始化管控等职权。

3.12

电子财务岗 electronical finance post

线下财务岗在信息系统中的映射或嵌入，具有职权电子化后的线上财务审批和管理等职权。

3.13

电子监察审计岗 electronical supervision and audit post

线下监察审计岗在信息系统中的映射或嵌入，具有电子监察、数据流归档与审计、监督线上与线下业务的一致性和业务流程的记录审查等职权。

4 内部风险管理原则

4.1 安全需求原则

组织应根据其信息系统担负的使命，积累的信息资产的重要性，可能受到的威胁及面临的风险分析安全需求，按照信息系统等级保护要求确定相应的信息系统安全保护等级，遵从相应等级的规范要求，

从全局上恰当地平衡安全投入与效果。

4.2 系统方法原则

按照系统工程的要求，识别和理解信息安全保障相互关联的层面和过程，采用管理和技术相结合的方法，提高实现安全保障目标的有效性和效率。

4.3 依法管理原则

信息安全管理工作主要体现为管理行为，应保证信息系统安全管理主体合法、管理行为合法、管理内容合法、管理程序合法。对安全事件的处理，应依法适时发布准确一致的有关信息，避免带来不良的社会影响。

4.4 权力制衡原则

对特定职能岗位或责任领域的管理功能实施职责分离和独立审计，应确保线上职权与线下职权一一对应，遵循管理、业务、技术的“三权分立”，电子业务岗负责业务运营、电子技术岗负责技术支撑、电子监察审计岗负责监督审计。

4.5 权力最小化原则

为避免权力过分集中所带来的隐患，以减少未授权的修改或滥用系统资源的机会，任何管理、业务、技术的岗位仅享有该岗位履行职能的最小权限。

4.6 管理与技术并重原则

坚持积极防御和综合防范，全面提高风险控制应对能力，立足国情，采用管理与技术相结合，管理科学性和技术前瞻性相结合的方法，保障信息系统的安全性达到所要求的目标。

4.7 过程控制原则

遵循系统安全工程理念，对信息系统全生命周期进行全过程控制，依照安全工程要求跟踪过程、找出偏差、分析成因、研究纠偏对策、实施纠偏措施等，确保信息系统内部风险可管、过程可控。

4.8 持续改进原则

安全管理是一种动态反馈过程，贯穿整个安全管理的生命周期。应根据业务的变化、系统环境的变化、系统的脆弱性以及面临的威胁等因素，及时调整现有安全策略、风险接受程度和安全防护措施，并周期性的对信息系统安全状态进行复查、修改和调整，以调整安全管理等级，维护和改进信息安全管理体系。

5 内部风险管理要求

5.1 总体要求

本项要求主要包括：

a) 应制定信息系统内部风险管理的总体规划，包含但不限于计划安排、人员配置、资金配置等；
b) 应对总体规划开展内部组织评审、发布、宣贯，且过程记录完整、可读；
c) 宜以信息技术为支撑，积极推进职权电子化，结合实际业务工作开展风险管理；
d) 应积极推进内部事务职权电子化进程，采用信息技术手段对组织内部的人、财、物管理等权力

的使用进行监管；

e) 应建立完善的信息系统管理风险评估与控制程序，包括但不限于风险识别、风险定级、风险处置、风险例外处置策略等；

f) 应配合业务主管部门、监管部门对组织开展信息系统内部风险管理落实情况的监督检查工作。

5.2 合规性要求

本项要求主要包括：

a) 应符合国家网络安全相关法律法规及标准要求；

b) 应建立健全组织法规库，形成法规要求的业务流程及业务关键控制点清单；

c) 应对信息系统内部风险管理涉及的相关法律法规及标准要求进行梳理，形成合规性要求列表；

d) 应按照相关法规及标准要求设定电子岗位；

e) 应按照相关法规及标准要求设定信息系统的业务流程；

f) 应按照相关法规及标准要求设定信息系统的业务关键控制点；

g) 宜采用自主安全的信息技术、服务及产品建设信息系统。

5.3 职权电子化管理要求

本项要求主要包括：

a) 应明确职权电子化过程中的对应关系(见附录 A)，确定线上职权与线下职权在组织中的岗位职责、业务流程和账号权限等方面获得准确映射或嵌入；

b) 应设立电子业务管理岗，负责信息系统的业务功能、业务流程、访问方式、权限等设定，监控业务的正常运行，避免业务岗位之间存在越权或绕权；

c) 应设立电子人事岗，负责信息系统的组织架构、业务部门、责任岗位、人员账号初始化等人事信息的设定，监控人事信息的非法变动；

d) 应设立电子财务岗，负责财务信息系统电子业务权力的行使；

e) 应设立电子监察审计岗，负责监督、审查电子业务权力和电子技术权力的行使，避免电子业务管理岗、电子人事岗、电子财务岗、电子技术岗参与业务运作，确保各岗位独立运行，排除岗位间相互干预及隐患；

f) 应对职权电子化后的电子岗位进行权限设计，建立电子岗位权限清单；

g) 应明确电子岗位角色权力事项名称、内容、行使主体、法律法规制度依据、监督方式等；

h) 应依据法规要求建立职权电子化控制流程，形成电子岗位的权责不兼容矩阵，固化电子岗位权限运行流程；

i) 应根据决策、执行、监督互为独立的原则进行分岗分责，实现同一业务不同岗位、同一流程不同环节的相互制约，重点满足业务部门与技术部门的权责分离；

j) 宜建立职权电子化需求编制与变更的评审机制，确保职权电子化过程得到有效控制，包括职权电子化的需求提出、审核、审批等各个环节，并实现全程留痕；

k) 应建立全程留痕机制，留痕内容应包括但不限于可研报告、立项书、招投标文件、系统概设与详设文档、开发人员保密协议承诺、测试报告、系统功能说明、系统操作维护手册、验收文档等相关审批情况与文档记录。

5.4 电子权力运行管理要求

本项要求主要包括：

a) 应对信息系统开展上线前的风险评估，评估范围包括但不限于信息系统自身、网络设备、安全设备、数据处理全流程等，评估内容包括但不限于法律合规、逻辑设计、编码漏洞、网络安全风险、数据安全风险等；

b) 应建立电子业务权力岗位角色与权限清单，包括但不限于业务部门、电子业务岗位、电子业务岗位人员、电子业务账号、电子职责等；
c) 应建立电子技术权力岗位角色与权限清单，包括但不限于业务部门、电子技术岗位、电子技术岗位人员、系统平台账号、电子职责等；
d) 应建立电子业务权力运行流程图，包括但不限于业务受控因素、业务流全过程、业务节点输入输出信息、业务节点对应电子岗位等；
e) 应建立电子技术权力运行流程图，包括但不限于业务信息存储和访问的流程、业务对应的应用模块、信息平台对应电子技术岗位、主机设备架构、主机对应的电子技术岗位、网络及网络设备架构、网络对应的电子技术岗位、监督系统等；
f) 应识别电子业务权力运行风险点，包括但不限于权限设置不合理、无明确的权力保管要求、误操作、用户操作抵赖、职责不清、职责未有效分离、绕权、越权等风险；
g) 应识别电子技术权力运行风险点，包括但不限于职责不清、职责未有效分离、权力无明确保管要求、重要参数和策略设置不合理、业务系统安装及更新维护管理不规范、安全维护不规范、数据维护和备份管理不规范、没有例外的处理机制、运维操作无审计、无主机自身的安全保障机制、主机不可用等风险；
h) 应建立电子权力运行风险点列表，包括但不限于业务部门、电子岗位、账号信息、权力对应的业务流程节点、风险编号、风险描述、控制目标等信息；
i) 应对电子权力运行风险进行分析，明确风险点、风险控制目标、现有控制措施、风险评价结果、风险描述、风险严重程度、残余风险分析结果等信息，并提出风险控制措施；
j) 应建立有效的电子权力行使主体身份的识别、验证与管理机制，包括唯一性识别、多因子认证以及安全性管理；
k) 应对电子权力运行全过程进行监控，包括权力行使主体、时间、内容、结果等；
l) 宜建立电子权力运行预警与处置机制，实现电子权力管理风险的事前提醒、事中监督和事后追溯；
m) 宜对时效性要求高的重要电子权力承载主体，建立相应的机制，保障权限运行的连续性；
n) 应采用规划、设计和技术手段限制或消除特权电子权力的运行；
o) 应对电子权力运行情况进行定期审计，审计范围应涵盖电子业务权力运行情况与电子技术权力运行情况，具体内容应包含操作主体、事件、操作内容、合规性情况、异常信息等；
p) 应建立电子权力运行全过程留痕与追溯机制，增强关键日志的可读性，实现重要数据更改的日志报警，留痕信息保留限期应符合相关法律法规要求；
q) 宜对承载电子权力运行的主体变更建立完整的变更控制程序、流程和记录，并保留变更控制相关记录；
r) 宜对重要电子业务权力运行主体保留原始主体及其变更主体源代码的完整记录。

5.5 敏感数据保护要求

本项要求主要包括：

a) 应依法建立数据分类分级规范，确定组织的重要数据具体目录，对列入目录的数据进行重点保护；
b) 应对敏感数据进行标识，形成敏感数据资产列表，不限于公民个人、公共管理、信息传播、行业领域、组织经营等维度数据；
c) 应加强数据安全风险监测，识别数据安全缺陷、漏洞等风险，对重要数据的数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告；
d) 应建立健全全流程数据安全管理制度，明确数据安全负责人和管理机构，落实数据安全保护责

任；

e) 应采取技术措施保护数据全生命周期各阶段的数据安全，对敏感数据变更、数据高风险操作和敏感数据访问进行全流程管控和审计；
f) 宜采用密码技术保障数据的机密性、完整性、可用性、真实性、不可否认性等属性不受侵害；
g) 可利用数据资产管理、数据安全管控、数据安全威胁感知等技术对数据资产的安全属性进行有效监管。

5.6 持续改进机制要求

本项要求主要包括：

a) 应围绕信息系统内部风险管理工作，在组织内部建立自查、互查等完善的督查机制；
b) 应每年定期对信息系统内部风险管理开展自评估，根据评估结果整改并修订内部控制策略；
c) 应每年定期对信息系统内部风险管理落实情况进行检查；
d) 应积极开展对业务主管部门、监督检查部门以及内部检查工作中发现的信息系统内部风险管理控制缺陷的评估与处置；
e) 应指定相关业务部门和人员负责组织的信息系统内部风险管理评估工作，并负责风险的处置；
f) 应定期开展信息系统内部风险管理工作的监督检查，并向有关主管部门报送监督检查结果；
g) 应定期对重要的录入数据或原始数据进行完整性、可用性和真实性审计；
h) 应定期对重大电子权力的运行操作进行稽核；
i) 应定期对内控例外策略的执行情况进行检查；
j) 宜在内外部环境、业务活动或管理要求发生重大变化时组织开展检查，并对发现的问题予以改进；
k) 应不定期委托第三方机构对自身信息系统内部风险管理工作进行评估，评估报告应作为本单位建立责任制考核的参考。

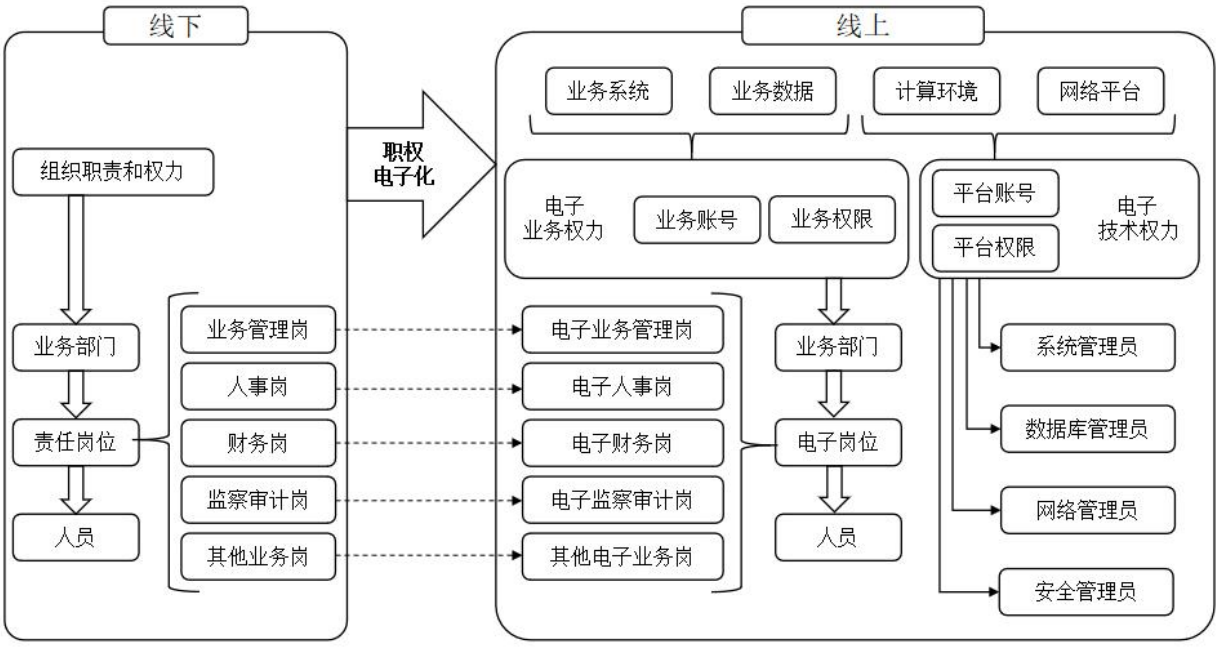
5.7 宣传与培训要求

本项要求主要包括：

a) 应定期开展信息系统内部风险管理的教育、培训和宣传活动，验证活动效果，纳入考核体系，并做好资料归档；
b) 应不定期的组织人员参加相关专业的继续教育，重要岗位人员应持有国家相关网络安全专业认证证书。

附 录 A
（资料性）
职权电子化过程中的对应关系

组织在信息化建设过程中，将线下业务和职权映射到信息系统各个业务功能、权限控制、信息平台等模块中，从而衍生出线上电子业务权力和电子技术权力，即为职权电子化过程，如图A.1所示。



图A.1 职权电子化过程示意图

职权电子化过程中的对应关系如下：

a) 线上职权与线下职权两者对应的业务部门、责任岗位和人员必须保持一致；

b) 电子业务权力与电子技术权力两者对应的所有者不为同一人；

c) 电子业务权力通过电子岗位人员的信息系统账号和权限进行行使，涉及的电子岗位包括电子业务管理岗、电子人事岗、电子财务岗、电子监察审计岗和其他电子业务岗，且与线下业务岗位保持对应；

d) 电子技术权力通过支撑信息系统运行的平台账号和权限进行行使，涉及的岗位包括但不限于系统管理员、数据库管理员、网络管理员、安全管理员等。

参 考 文 献

[1] GB 17859—1999 计算机信息系统 安全保护等级划分准则
[2] GB/T 20269—2006 信息安全技术 信息系统安全管理要求
[3] GB/T 20984—2022 信息安全技术 信息安全风险评估规范
[4] GB/T 22080—2016 信息技术 安全技术 信息安全管理体系要求
[5] GB/T 22081—2016 信息技术 安全技术 信息安全控制实践指南
[6] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
[7] GB/T 29245—2015 信息安全技术 政府部门信息安全管理基本要求
[8] GB/T 29246—2017 信息技术 安全技术 信息安全管理体系 概述和词汇
[9] GB/T 36073—2018 数据管理能力成熟度评估模型
[10] GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型
[11] 中国内部审计协会公告2013年第1号 中国内部审计准则