ICS XXX
CCS XXX

DBXX

广　东　省　地　方　标　准

DBXX/T XXX—XXXX

信息系统管理风险内部控制基本要求

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。

本文件由广东省网络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。

本文件主要起草人：陈宁、骆林勇、王辉、王文佳、王常吉、邢静、李虹、崔顺艳、谢柏林、宋琅靖、邓艳利、何文婷、袁毅鸣、邝建、张新猛、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，给信息系统的业务风险管控带来极大挑战，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业务风险管控及职权电子化的成效。业务风险管控失效会给网络运营者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、企业核心机密与国有资产流失等。因此，强化业务风险管控，建立信息系统管理风险内部控制基本要求势在必行，也是一项非常紧迫与重要的任务。

信息系统管理风险内部控制的目的是为了加强组织内部对信息系统风险的管控，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、科学性和信息化对业务管理的支撑与流程控制能力，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。

本标准综合运用信息安全管理制度、标准规范和内部控制方法，将信息系统管理风险内部控制措施中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、权力运行过程的管理风险进行控制，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。

本标准可以作为政府部门、企事业单位在信息系统全生命周期中的内部控制体系以及安全管理方面建设的主要依据或参考。

信息系统管理风险内部控制基本要求

1 范围

本文件规定了政府、企事业单位信息化建设应满足的信息系统管理风险内部控制基本要求。

本文件适用于网络运营者、监管单位、第三方审查机构对政府、企事业单位的信息系统管理风险内部控制情况进行内、外部审查，审查结果可作为政府部门和企事业单位风险内部控制的参考依据。

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 17859 计算机信息系统 安全保护等级划分准则

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

GB/T 29246 信息技术 安全技术 信息安全管理体系 概述和词汇中的相关理念、模型、方法与定义

3 术语和定义

下列术语和定义适用于本文件。

3.1

信息系统业务风险 information system business risk

信息系统业务风险，是指在信息系统建设运行管理过程中，因信息系统业务活动中岗位角色权力风险管理制度、系统电子角色权力防控措施不完善或执行不到位，业务流程控制、敏感信息数据应用管理等方面存在隐患，导致系统鉴权混乱、运行混乱、系统运行不可靠、业务活动偏离控制目标，系统无法有效发挥业务支撑与流程管控作用的可能性。

3.2

信息系统管理风险内部控制 internal control for information system management risk

信息系统管理风险内部控制是综合运用信息化建设管理制度、标准规范和内部控制方法，将信息系统管理风险防控措施贯穿于信息系统建设、管理与应用的全过程，对信息系统建设、管理和运行进行全程控制，包括将内部控制活动和措施嵌入至信息系统等。

3.3

信息系统业务风险管控 information system business risk control

信息系统业务风险管控是综合技术、管理、检测、评估等方法，将信息系统业务风险管控措施贯穿于信息系统业务的全生命周期和职权管理的全过程，对信息系统建设、业务管理和权力运行进行全程管理与控制。

3.4

职权电子化 electronization of authority

职权电子化是以职权为对象，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。

3.5

线下职权 offline authority

国家法律、法规赋予的行政职权，是由行政单位释放到各业务科室，再由业务科室划分到各责任岗位，岗位再配备人员代表国家履行权力职责。

3.6

线上职权 online authority

国家法律、法规赋予的行政职权，通过信息化建设将职权电子化，将行政职权映射到信息系统中，形成对应的电子岗位，以及对应岗位的职权账号、权限。

3.7

电子权力 electronical power

现实职责权限在计算机系统上的映射或嵌入，包括电子业务权力和电子技术权力。

3.8

电子业务权力 electronical business power

现实业务岗位的职责权限在计算机系统上的映射或嵌入。

3.9

电子技术权力 electronical technology power

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

3.10

电子岗位 electronical post

根据现实人员岗位角色权力电子化的要求在信息系统中设立的与现实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。

3.11

电子业务管理岗 electronical business management post

现实业务管理岗在计算机系统中的映射，负责信息系统的业务流程矩阵的建立、业务流程的合规设定、业务归档等职权。

3.12

电子人事岗 electronical personnel post

现实人事岗在计算机系统中的映射，负责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。

3.13

电子财务岗 electronical finance post

现实财务岗在计算机系统中的映射，负责职权电子化后的线上财务审批和管理等职权。

3.14

电子审计岗 electronical audit post

现实纪检、监察、审计岗在计算机系统中的映射，负责电子监察，数据流归档的审计，监督线上与线下业务的一致性，业务流程的记录审查等职权。

3.15

电子签名 electronical signature

数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。

3.16

敏感信息 sensitive information

一旦泄露、非法提供或滥用可能危害国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的所有信息。

4 管理风险内部控制原则

a) 安全需求原则：组织机构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；
b) 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；
c) 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，应由授权者适时发布准确一致的有关信息，避免带来不良的社会影响；
d) 职权分离原则：对特定职能或责任领域的管理功能实施职责分离、独立审计，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。任何实体（如用户、管理员、进程、应用或系统）仅享有该实体需要完成其任务所必须的权限，不应享有任何多余权限；

e) 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；

f) 自保护和国家监管相结合原则：对信息系统安全实行自保护和国家保护相结合。组织机构要对自身的信息系统安全保护负责，政府相关部门有责任对信息系统的安全进行指导、监督和检查，形成自管、自查、自评和国家监管相结合的管理模式，提高信息系统的安全保护能力和水平，保障国家信息安全；

g) 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 管理风险内部控制要求

信息系统管理风险内部控制是围绕着信息系统的全生命周期，对信息系统业务执行过程中的每个环节所涉及的业务合规、关键要素控制、人员职责、权力执行、信息保护等因素进行风险管控。

5.1 总体要求

a) 应制定信息系统风险管控的总体规划，包含但不限于：计划安排、人员配置、资金配置等；
b) 总体规划应在组织内部进行评审、发布、宣贯，过程记录应完整、可读；
c) 应以信息技术为支撑，积极推进职权电子化，结合实际业务工作开展风险防控；
d) 应积极推进法定职权电子化进程，涉及行政审批、行政处罚、行政给付、政府投资项目、公共资源交易、财政专项资金管理使用等领域权力的使用均应采用信息技术手段进行监管；
e) 应积极推进内部事务职权电子化进程，包括单位内部的人、财、物管理等权力的使用均应采用信息技术手段进行监管；
f) 应建立完善的信息系统管理风险评估与控制程序，包括但不限于管理风险评估、风险定级、风险处置等；
g) 应指定相应部门或人员负责信息系统管理风险的评估与处置；
h) 应制定信息系统风险的例外处置策略；
i) 应支持并配合业务主管部门、监管部门针对信息系统业务风险管控落实情况的监督检查工作，开放监管接口。

5.2 合规性要求

a) 应建立健全组织法规库，并建立法规要求的业务流程及业务关键控制点清单；
b) 应对信息系统风险管控工作相关的法律、法规和制度要求进行梳理，并形成合规性要求列表；
c) 业务信息系统的流程应按相关法规及标准要求设定；
d) 业务信息系统的关键控制点应按相关法规及标准要求设定；
e) 业务信息系统建设应采用自主安全的信息技术、服务及产品；
f) 业务信息系统的安全防护应满足《中华人民共和国网络安全法》、《中华人民共和国密码法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法规及标准要求。

5.3 职权电子化控制要求

a) 应明确职权电子化的对应关系，包括现实岗位与职责、电子岗位与职责、现实岗位与电子岗位对应关系、职权电子化依据等；
b) 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，包括电子账号、电子岗位、电子职责、责任人等。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；
c) 应针对电子人事岗、电子业务管理岗、电子财务岗、电子审计岗等电子岗位设立专人专职；
d) 应依据法规要求明确业务流程，并建立职权电子化控制流程；
e) 应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；
f) 职权电子过程应建立全程留痕机制，留痕内容应包括但不限于相关审核审批情况与文档记录，如可研报告、立项书、招投标文件、系统概设与详设文档、开发人员廉洁协议承诺、测试报告、系统功能说明、系统操作维护手册、验收文档等；
g) 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；
h) 应建立职权电子化所涉及电子岗位的权责不兼容矩阵，固化电子岗位权限运行流程。

5.4 电子权力运行管理要求

a) 电子权力运行前，应对信息系统（包含信息系统自身、网络设备、安全设备等）开展风险评估，评估内容包括但不限于法律合规、逻辑设计、编码漏洞、网络安全风险等；
b) 应建立电子业务权力岗位角色与权限清单、电子技术权力岗位角色与权限清单、电子业务权力运行流程图、电子技术权力运行流程图等；
c) 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。留痕信息应至少保留五年。应对日志的访问和存储进行保护，不被非授权访问，不被篡改；
d) 应建立有效的电子权力行使主体身份识别、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；
e) 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；
f) 应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；
g) 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；
h) 对承载电子权力运行的主体变更应建立完整的变更控制程序，并保留变更控制相关记录；
i) 对重要电子业务权力运行主体自身（信息系统）应保留原始主体及其变更主体的完整记录（源代码）；
j) 对时效性要求高的重要电子权力承载主体，应建立相应的机制，保障权限运行的连续性。

5.5 电子权力运行控制要求

a) 电子权力应明确岗位职责；
b) 电子权力应做到职责有效分离；
c) 业务操作权限符合电子岗位职责要求，应符合实际岗位职责；
d) 应具备明确的权力管控要求并遵照执行；

e) 应杜绝误操作；
f) 应确保输入/输出信息的正确性、完整性及可用性；
g) 应按照合理的流程预先定义例外处理机制并遵照执行；
h) 应确保信息输入的及时性；
i) 应防止用户操作抵赖；
j) 应按照既定的流程定义及操作规范进行网络运维，且操作可审计追溯；
k) 应确保新增网络设备的配置按照既定的流程定义及操作规范与标准要求进行；
l) 应确保相关网络及网络安全设备的策略变更按照既定的流程定义及操作规范进行；
m) 应确保权力账号及其权限的变更按照既定的流程定义及操作规范进行；
n) 例外控制应按照合理的流程进行预先的定义，且审核相关人员执行或处理的记录；
o) 应确保日志记录的完整性、可用性及机密性；
p) 应确保网络的高可用性。

5.6 敏感信息保护要求

a) 应建立业务信息数据的分级分类管理规则，明确访问权限保护要求；
b) 应对信息系统中的敏感信息进行识别，明确敏感信息的类别与保护登记；
c) 应明确敏感信息的产生过程、存储过程及位置；
d) 应确保敏感信息在传输过程中的安全；
e) 应确保敏感信息不被外泄；
f) 应明确各电子权力对敏感数据具有的的相关权限，包括知情权、使用权、管理权等；
g) 应根据实际业务运行情况，评估敏感信息的安全风险，如保密性、完整性、可用性等，并根据相关风险制定对应的安全防护措施；
h) 应对敏感信息的变更建立全程的监控与审计追溯机制，确保敏感信息的管理风险得到有效的控制。

5.7 持续改进机制要求

a) 应定期（每年至少一次）对信息系统管理风险进行评估，并修订内部控制策略与具体要求；
b) 应定期（每年至少一次）对信息系统管理风险内部控制落实情况进行检查；
c) 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业务风险内部控制缺陷的评估与处置；
d) 应指定相关业务部门和人员负责组织信息系统管理风险内部控制的评估工作，并负责风险的处置；
e) 应定期开展信息系统管理风险管控的检查，并及时向相关组织或部门报告监督检查结果；
f) 应定期对重要的录入数据或原始数据进行完整性、可靠性和真实性审计；
g) 应定期对重大电子权力的运行操作进行稽核；
h) 应定期对内控例外策略的执行情况进行检查；
i) 在内外部环境、业务活动或管理要求发生重大变化时，应及时组织开展检查，并对发现的问题予以改进；
j) 应不定期的委托第三方机构对自身信息系统管理风险内部控制工作进行评估，评估报告应作为本单位建设责任制考核的参考。

5.8 沟通与交流要求

a) 应每年定期开展信息系统管理风险内部控制的教育、培训与宣传活动，并对活动效果进行验证，验证结果纳入考核；

b） 教育、培训与宣传活动记录文档应具备完整性、可读性；
c） 重要岗位人员应持有国家相关安全专业认证证书，并不定期的参加相关专业的继续教育。

附 录 A
（资料性）
线下职权与线上职权的关系

职权电子化是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的过程。将线下的业务和职权通过信息建设移植、分散到线上信息系统的各个信息平台、业务功能模块及权限管理中，将业务和职权运行在信息系统中，衍生出多个新的电子岗位及电子权力。职权电子化过程图如图1所示。

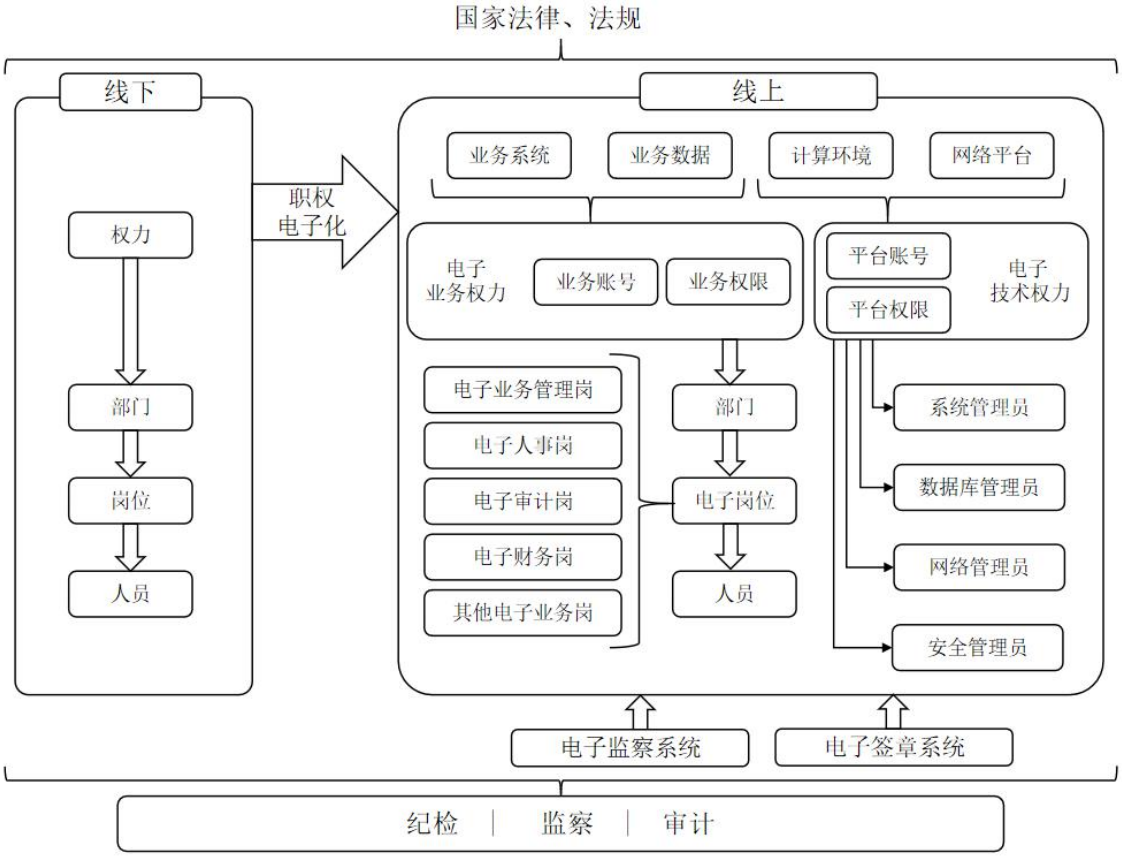

图1 职权电子化过程图

在整个职权电子化过程中，线下职权和线上职权的关系如下：

a) 线下职权是线上职权在信息系统中的映射，线下职权和线上职权都必须遵从国家相关法律、法规。

b) 线下职权与线上职权对应的部门、岗位、人员必须是一样的。但职权电子化后，会衍生诸如电子业务管理岗、电子人事岗、电子审计岗、电子财务岗等特殊性电子岗位，这些特殊性电子岗位需要特定人员去担任。

c) 线下职权经过职权电子化后，其权力会在信息系统中映射为电子业务权力和电子技术权力。在业务上，线下的一项权力可能会对应到线上的多个权限。业务权力所有者原则上必须与技术权力所有者分开，也就是拥有技术权力者不得参与业务权力的行使，或不得具备对应的线上职权的行使权限。

d) 线下职权和线上职权在行使过程时，均受纪检、监察、审计等部门监管或督察。

参 考 文 献

[1] GB/T 17859 计算机信息系统 安全保护等级划分准则
[2] GB/T 20269 信息安全技术 信息系统安全管理要求
[3] GB/T 20984 信息安全技术 信息安全风险评估规范
[4] GB/T 22080 信息技术 安全技术 信息安全管理体系要求
[5] GB/T 22081 信息技术 安全技术 信息安全控制实践指南
[6] GB/T 22239 信息安全技术 网络安全等级保护要求
[7] GB/T 29245 信息安全技术 政府部门信息安全管理基本要求
[8] GB/T 29246 信息技术 安全技术 信息安全管理体系 概述和词汇中的相关理念、模型、方法与定义