ICS
L

团　　体　　标　　准

T/ISC XXXX—XXXX

互联网信息科技风险治理能力模型
总体框架

Capability model of Internet information technology risk governance—

General architecture

（报批稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中　国　互　联　网　协　会　　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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国互联网协会归口。

本文件主要起草单位：中国信息通信研究院、贝壳找房（北京）科技有限公司、阿里巴巴（中国）有限公司、杭州口口相传网络技术有限公司、度小满科技（北京）有限公司、百度在线网络技术（北京）有限公司、北京携程国际旅行社有限公司、苏宁易购集团股份有限公司、联想（北京）有限公司、北京京东世纪贸易有限公司、同盾科技有限公司、北京三快在线科技有限公司（美团）、顺丰科技有限公司、网宿科技股份有限公司、三六零安全科技股份有限公司、央广新媒体文化传媒（北京）有限公司、小米科技有限责任公司、北京快手科技有限公司、中国联合网络通信集团有限公司、OPPO广东移动通信有限公司等。

本文件主要起草人：杨玲玲、陈杨、张龙、应叶、温博、魏涛涛、高磊、李黎、董纪伟、王海棠、赵炎杰、尚梦宸、王阳、王建莹、马可、刘榕、叶串、栾浩、姚凯、王向宇、吕丽、赵一龙等。

引　言

互联网行业业务模式的快速创新和信息科技的深度应用在给企业带来巨大机遇的同时，也使企业面临着越来越多样化，越来越复杂的因信息科技应用而产生的风险。

当前，互联网企业信息科技风险治理在基本框架和治理内容方面缺少标准和共识，需企业和行业组织共同促进行业共识形成，指导企业建立信息科技风险治理机制，实现信息科技风险的识别、评估、处置和监测，保障企业运营合规，业务稳健运行，提升信息保护和风险防控能力，推动业务创新和新技术应用，促进互联网生态健康发展。

互联网信息科技风险治理能力模型　总体框架

1　范围

本文件确立互联网信息科技风险治理能力模型的总体框架。

本文件适用于互联网企业，为其信息科技风险治理活动提供参考和指引。其他相关行业或组织可参考执行。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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

GB/T 35273—2020　信息安全技术　个人信息安全规范

GB/T 22239—2019　信息安全技术　网络安全等级保护基本要求

ISACA Glossary of Terms Third edition 2015

3　术语和定义

GB/T 25069—2010、GB/T 35273—2020、ISO/IEC 38500:2015、ISO/TR 21506:2018(en)、ISO/IEC/IEEE 21841:2019(en)、ISO 9000:2015、ISO 31000:2018(en)界定的下列术语和定义适用于本文件。

3.1

治理　governance

领导和控制的体系

[来源: ISO/IEC 38500:2015, 2.8]

治理 governance

用来领导和控制组织的原则、政策、和框架

[来源: ISO/TR 21506:2018(en), 3.25]

治理 governance

建立和执行战略目标、组织政策和绩效的流程

注1：此定义来源于参考[8].

[来源: ISO/IEC/IEEE 21841:2019(en), 3.1.2]

3.2

管理　management

为达到组织治理团队所设置的策略性目标所需的控制和过程体系，管理受制于组织治理所设定的方针指南和监视。

注1：管理这一术语经常也被用作对组织中管理者的描述。管理者这一术语用以避免管理者与管理体系两个术语的混淆。

[来源: ISO/IEC 38500:2015, 2.14]

管理 management

为控制和领导组织而进行的协调活动

注1：管理包括建立政策、目标和达成目标的过程等活动。

注2：“管理”有时指人，指对组织的领导和控制负有职责和权限的一个人或一组人。此时，管理概念的使用应当避免与上述一组活动的管理概念相混淆。例如，不推荐使用“管理应...”，而推荐用“最高管理者应...”。应将如管理和管理者之类概念的不同之处传达给相关人员。

[来源: ISO 9000:2015, 3.3.3]

3.3

信息科技风险 information technology risk

在互联网企业的业务运营、内部管理等方面，信息科技运用中由于自然因素、人为因素、技术漏洞和管理缺陷产生的操作、法律和声誉等方面的风险。

3.4

风险管理 risk management

领导和控制组织面临风险的协调活动

[来源: ISO 31000:2018(en), 3.2]

3.5

风险偏好 risk appetite

组织在追求其使命、战略和目标时以及在需要采取措施处理或管理风险之前愿意接受的风险水平。

3.6

信息安全 information security

对信息的保密性、完整性和可用性的保持。

注：另外，也可包括诸如真实性、可核查性、抗抵赖和可靠性等其他性质。

[来源：GB/T 29246—2017，2.33，有修改：注中的“其他特性”改为“其他性质”]

3.7

网络安全 cybersecurity

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。

[来源：GB/T 22239—2019, 3.1]

3.8

数据安全 data security

通过管理和技术措施，确保数据有效保护和合规使用的状态。

[来源：GB/T 37988—2019,定义3.1]

3.9

控制<名词> control

改变风险的措施。

注 1：控制包括任何改变风险的过程、策略、设备、实践或其他措施。

注 2：控制未必总能达到预期或假定的风险改变效果。

[来源：GB/T 29246—2017，2.16，有修改：增加“〈名词〉”等]

3.10

个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合来识别特定自然人身份或者反映其活动情况的各种信息。

注 1：个人信息包括姓名、出生日期、公民身份号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

注 2：个人信息控制者通过个人信息或其他加工处理后形成的信息， 例如，用户画像特征标签，能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的，也属于个人信息。

[来源：GB/T 35273-2020，3.1，有修改：“身份证件号码”改为“公民身份号码”，删除原注2等]

4 缩略语

下列缩略语适用于本文件。

IT 信息科技（information technology）

5 总体框架

5.1 概述

互联网信息科技风险治理能力模型用于从风险治理能力和风险治理领域两个维度指导企业构建自身的信息科技风险治理体系、提升信息科技风险治理能力水平。

风险治理能力维度：表示企业开展信息科技风险治理活动的能力，包括组织、策略、流程和技术平台四项关键能力。

风险治理领域维度：表示企业开展信息科技风险治理活动的领域，包括法律合规、业务安全风险域、应用风险域、数据安全风险域、平台风险域、基础设施运营风险域、个人信息保护风险域、内容治理风险域、新技术应用风险域和生态建设风险域等。

互联网信息科技风险治理能力模型总体框架如图1所示。

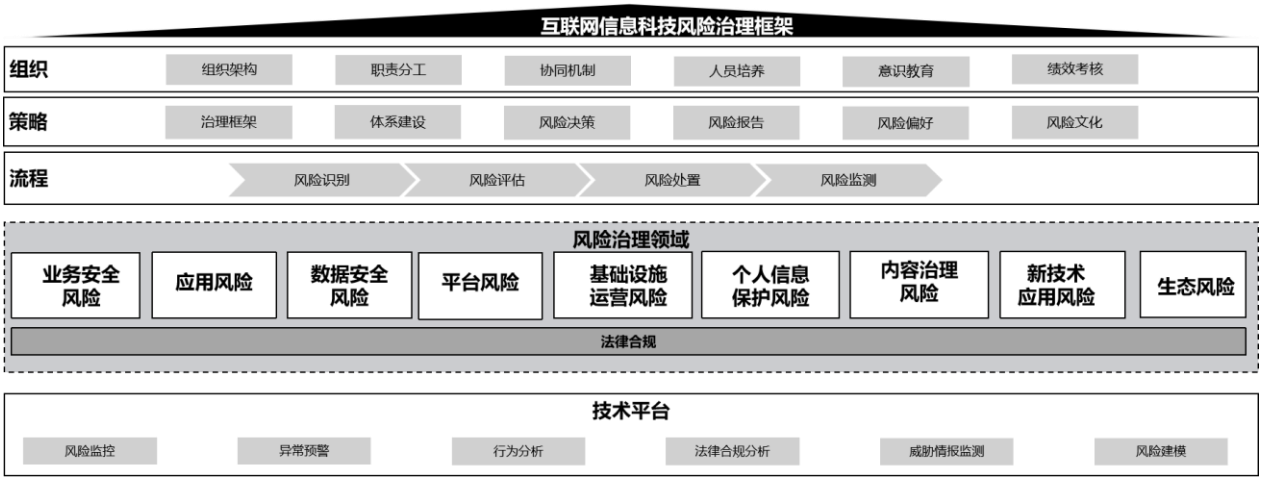

图1 互联网信息科技风险治理能力模型总体框架

5.2 风险治理能力

通过定义互联网企业开展信息科技风险治理活动须具备的能力，供企业构建和评价其信息科技风险治理活动的全面性、可靠性、有效性和成熟度。信息科技风险治理能力从组织、策略、流程和技术四个维度展开。

——组织：企业内部信息科技风险治理组织的架构建立、职责分配、沟通协作、人员培养、意识教育和绩效考核等。

——策略：企业根据自身业务类型、管理需要和外部环境确定的风险治理框架、管理体系、风险决策机制、风险汇报路径、风险偏好、风险文化等。

——流程：企业开展信息科技风险治理活动的流程，包括风险识别、风险评估、风险处置和风险监测的闭环管理机制。组织可采用适合的风险管理流程，本文件不做限定，这些风险管理流程应为实现目标而定制，并适用于其所在的内外部环境。本文件不对互联网企业风险管理流程选择做具体限定，附录A列出风险管理参考流程，供互联网企业参考。

——技术：通过技术手段和产品工具支撑各项信息科技风险治理活动，以实现风险治理流程自动化、风险控制自动化，以及风险监测、预警、决策的智能化。

信息科技风险治理的策略、组织、流程、技术应适用于信息科技风险治理活动的各个领域，可根据企业治理的实际情况进行整体能力建设，也可拆分到各个领域进行独立的能力建设。

5.3 风险治理领域

风险治理领域是互联网企业根据自身业务类型、运营模式、管理目标和技术应用情况所确定的应执行信息科技风险治理活动的风险域。

——本文件根据互联网行业的治理现状和普遍存在的风险特征提出通用风险治理领域，互联网企业应根据自身适用情况进行补充或裁剪。

5.3.1 业务安全风险域

业务安全风险指互联网业务场景中因业务流程或系统受到安全威胁而产生的风险。

——涵盖交易、支付、营销等各业务环节；

——安全威胁包括但不限于撞库、诈骗、木马、钓鱼、病毒、勒索、作弊套利等攻击方式；

——业务安全风险治理着重针对利用互联网产品或活动的业务策略漏洞、基础平台技术漏洞；

——企业管理薄弱环节开展的恶意行为和违法犯罪活动进行有效防范和及时控制，应该包括风险感知、策略和模型、监测和预警、核查和分析等内容。

5.3.2 应用风险域

应用风险指应用程序的服务端和客户端因机密性、完整性、可用性、可度量性和可追溯性缺少恰当的保障而产生的风险。

——保障互联网应用程序的机密性、完整性、可用性、可度量性和可追溯性而执行的一系列活动，针对可能导致服务中断、信息泄漏或不合规等风险的应用程序层面的风险执行的风险治理活动；

——包括应用程序的研发和运维，应用程序安全，以及接口和插件等内容。

5.3.3 数据安全风险域

数据安全风险指在数据全生命周期中数据保密性、完整性、可用性、真实性、不可抵赖性等要素缺少恰当的保障而产生的风险。

——数据安全风险治理指通过风险控制措施确保数据有效保护和合规使用的状态；

——包括数据采集安全、数据传输安全、数据存储安全、数据备份与恢复、数据处理环境、数据共享安全、数据销毁安全等。

5.3.4 平台风险域

平台风险指互联网企业为实现资源共享或集中化管理而搭建的技术平台因机密性、完整性、可用性、可度量性和可追溯性缺少恰当的保障而产生的风险。

——包括数据平台、风控平台、服务平台、云平台、开发平台等；

——向互联网企业内部多个事业部提供横向服务，或整合多项业务能力向外部提供服务；

——保障平台机密性、完整性、可用性、可度量性和可追溯性而执行的一系列活动，应该包括平台架构、平台开发和运维、平台安全、平台资源配置等内容。

5.3.5 基础设施运营风险域

基础设施运营风险指承载互联网企业业务运营的信息技术设备和组件因内外部威胁而不能平稳、持续运行的风险。

——包括基础设施建设、基础设施运维、网络安全、业务连续性、终端设备管理等内容。

注：本文件所指基础设施包括机房、服务器、网络互联设备、安全设备、终端设备等物理设施以及为满足业务连续性需求所部署的灾备设施。基础设施运营一般适用于数据中心和备援中心等；

5.3.6 个人信息保护风险域

个人信息保护风险是指互联网企业在开展业务的过程中收集、存储、使用以及委托处理、共享、转让和公开披露个人信息时未有效保护个人信息主体合法权益、确保个人信息安全、防止信息泄漏和滥用而造成的风险。

——个人信息保护风险治理涵盖企业在涉及个人信息的业务活动中为保障个人信息主体的权力以及个人信息控制者为实现个人信息主体权力所应承担的责任和义务而执行的一系列活动，如个人信息安全影响评估、告知同意、数据主体的权利、跨境传输、隐私事件应急处置、隐私工程等。

5.3.7 内容治理风险域

内容治理风险指网络信息内容服务平台在网络生态治理中未履行信息内容管理主体责任而造成的合规、声誉等风险。

——该领域包括网络信息内容管理、网络信息内容分发、网络用户管理、价值引导和不良信息管理等内容；

——互联网企业内容治理以建立健全网络综合治理体系、营造清朗的网络空间、建设良好的网络生态为目标，开展弘扬正能量、处置违法和不良信息等相关活动。

5.3.8 新技术应用风险域

新技术应用风险指互联网企业在业务模式和管理模式中引入前沿技术后产生的技术风险，以及技术与应用场景结合所产生的其他风险。

——包括企业引入新技术时可能产生的业务逻辑和管理流程、系统运行环境变更所引发的风险、新技术应用可能存在的伦理风险、新技术自身的固有风险以及对新技术过度依赖的风险等；

注：本文件所指新技术一般涵盖大数据、区块链、云计算、人工智能、物联网、工业控制等。

5.3.9 生态风险域

生态风险指互联网企业作为互联网生态的组成部分，在开展业务的过程中不可避免地与其他利益相关方互动，从而受到第三方以及外部市场环境影响的风险。

——生态风险治理包括第三方机构、第三方服务、第三方人员以及开源管理等方面；

——第三方涵盖外包服务商、软硬件供应商、合作伙伴、同行业企业等为互联网企业提供服务、与互联网企业合作的组织或个人。

5.3.10 法律合规风险域

法律合规风险指企业经营活动不符合应遵循的信息科技相关的法律、行政法规、行业准则而产生的风险。

——法律合规风险治理活动包括对法律、行政法规、行业准则的收集、解读、分析，以及对企业的合规风险评估、合规指导等内容；

——法律合规包含境内合规和境外合规；

——境内合规指企业在中华人民共和国境内运营所适用的法律、行政法规、行业准则的符合情况；境外合规指企业向海外拓展业务的过程中所适用的当地国家、区域出台的法律、行政法规、行业准则的符合情况；

——与其他风险治理领域有所区别的是，法律合规治理活动覆盖互联网企业所适用的所有信息科技相关的风险治理领域，包括业务安全风险域、应用风险域、数据安全风险域、平台风险域、基础设施运营风险域、个人信息保护风险域、内容治理风险域、新技术应用风险域和生态建设风险域。

附 录 A
（资料性附录）
风险管理流程参考

A.1 概述

本附录通过对国际通用风险管理文件进行精简整合，对比各文件特色与区别，供互联网企业建立组织风险管理流程时进行参考。

A.2 ISO 31000:2018 风险管理指南 指南

管理风险是治理的一部分，对于组织在各个层面的管理至关重要。ISO 31000 提供了管理任何类型风险的通用方法，可用于组织的整个生命周期，可应用于任何行动，包括各层级决策。其中，风险管理流程涉及系统地将政策、程序和实践应用于沟通和咨询活动，建立环境和评估、应对、监督、审查、记录和报告风险。风险管理流程的要素分为六大部分，包括沟通与咨询、范围、环境和准则、风险评估、风险应对、记录与报告、监督与审查。

A.3 ISO/IEC 27005 信息技术 安全技术 信息安全风险管理

ISO27005 为信息安全风险管理提供了指导方针，适用于所有类型的想要管理危及组织信息安全的风险的组织。ISO31000 风险管理过程适用于信息安全风险管理，相较于 ISO31000，ISO27005 信息安全风险管理过程加入风险接受环节，明确提出风险管理是迭代循环的动态过程。ISO27005 信息安全风险管理过程包括环境创建、风险评估、风险处理、风险接受、风险沟通和协商以及风险监测和审查。

A.4 GB/T 31722—2015 信息技术 安全技术 信息安全风险管理

该文件为中国国家文件化管理委员会推荐国家文件，采标 ISO/IEC 27005，适用于各类型和规模的组织，帮助其开发和实施信息安全风险管理框架。

A.5 NIST Special Publication 800-39 Managing Information Security Risk

NIST SP 800-39 是美国国家文件与技术研究院发布的适用于组织信息安全风险管理的技术文件，其中风险管理的流程分为建立风险框架、评估风险、响应风险、监测风险。建立风险框架阶段，组织需要明确其风险假设、风险限制条件、风险容忍度、风险特征和权衡；评估风险阶段，组织需要识别威胁和漏洞以及分析和评估由其造成的风险；响应风险阶段，企业需要识别可作为风险响应的资源、风险响应决策、风险响应计划及实施；风险监测方面，企业需要制定风险监测策略以及实施风险监测。

参 考 文 献

[1] ISACA Glossary of Terms

[2] GB/T 31722—2015 信息技术 安全技术 信息安全风险管理

[3] ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management

[4] ISO 31000:2018 Risk management — Guidelines

[5] NIST Special Publication 800-39 Managing Information Security Risk — Organization, Mission, and Information System View