HANKUN

汉坤法律评述

2026 年 7 月 10 日

北京 | 上海 | 深圳 | 杭州 | 武汉 | 海口 | 香港 | 新加坡 | 纽约 | 硅谷 | 伦敦

统一底线与协同监管：《金融业网络安全管理办法（征求意见稿）》核心要点解析

作者：段志超 | 权威 | 夏迎雨 | 王雨婷

2026 年 7 月 3 日，中国人民银行、国家金融监督管理总局、中国证券监督管理委员会、国家外汇管理局联合发布《金融业网络安全管理办法（征求意见稿）》，公开向社会征求意见，反馈截止时间为 2026 年 8 月 3 日。

这是国务院金融管理部门拟在金融业层面对网络安全管理作出的统一制度安排。此前，银行保险、证券期货、支付等领域的相关要求主要分布于不同监管条线和业务规则之中。本次《办法》的重要作用，在于拉齐金融业网络安全保护的基本要求，并通过监督管理协同、信息共享和责任衔接，强化金融业网络安全治理。

一、监管定位：面向各类金融从业机构的通用底线规则

《办法》的适用范围不局限于传统的银行、保险、证券机构。凡在我国境内建设、运营、维护和使用网络的金融从业机构，以及金融业网络安全的监督管理活动，均受本办法约束。其他主管部门已有专门规定的，机构仍需同步遵守对应要求。涉及存储、处理国家秘密信息的网络安全管理，《办法》明确国家另有规定的，从其规定。

从定义看，《办法》可能覆盖银行、保险、证券期货、基金、支付、征信、外汇等受国务院金融管理部门监管的机构，以及其他经国务院金融管理部门批准设立或者认定的主体，具体适用仍需结合机构资质、监管条线和业务类型判断。对于地方金融组织，《办法》拟由地方金融管理机构牵头负责其履行网络安全保护义务的监督管理，并允许地方金融管理机构参照《办法》及国务院金融管理部门网络安全相关规定制定相应制度。

值得注意的是，《办法》属于金融业网络安全领域的通用底线规则，并不替代网络安全等级保护、关键信息基础设施保护、商用密码管理、网络安全审查、数据安全与个人信息保护等既有制度，其他主管部门另有规定的，金融从业机构仍需同步遵守。它并不对所有技术控制措施作细颗粒度规定，核心价值在于将金融业共性的网络安全保护义务集中列明，通过监管协同、责任衔接、重点领域特别要求等设计，将国家层面的网络安全制度融入金融行业监管体系。机构落地执行时，仍需结合所属行业、业务类型、系统等级、是否构成关键信息基础设施、处理数据类型等具体场景，匹配对应的专项规则。

二、组织治理：网络安全责任需落实到决策机制和各级主体

《办法》延续上位法的监管思路，明确金融从业机构对本机构网络安全承担主体责任，坚持安全与发展并重，为网络安全工作匹配必要的资源保障，建立健全适配自身业务的安全保障体系。

机构需要建立并落实网络安全责任制，明确网络安全负责人，搭建对应的管理组织架构与议事决策机制，指定网络安全牵头管理部门。资金与人员投入要落到实处，同时应制定内部网络安全管理制度和操作规程，并结合本机构、分支机构、下属法人机构的实际分工，明确网络安全保护职责。

这项要求对集团化、平台化运营的金融机构影响尤为直接。对于集团化、平台化运营的金融机构，如既有网络安全管理主要由信息科技部门或安全团队牵头，仍需进一步明确决策层、业务条线、分支机构和下属法人主体在网络安全治理中的职责。对于同时经营多类金融业务、存在多个系统运营或数据处理主体的集团，需要通过正式制度明确总部与子公司、业务部门与科技部门、内控部门与运维部门的职责划分，避免安全责任被业务边界或法人边界切割。

三、等保、商用密码与技术创新应用：从基础保护到风险管理

网络安全等级保护是金融业网络安全工作的基础制度。《办法》在《网络安全法》要求的基础上，进一步明确金融从业机构需合理确定网络安全保护等级，履行定级备案义务，按期开展等级测评，并对测评发现的风险及时整改。

《办法》将商用密码使用与网络安全等级保护要求相衔接，要求金融从业机构按照国家网络安全等级保护制度要求，使用商用密码保护网络安全；国务院金融管理部门另有规定的，还应按照相关规定执行。在金融场景中，商用密码的应用覆盖身份认证、传输加密、存储加密、数字签名、密钥管理等多个环节。对于被认定为金融业关键信息基础设施运营者的机构，年度网络安全检测和风险评估内容还应包括商用密码应用安全性评估。

信息技术应用创新也被正式纳入网络安全保护义务范畴，机构需依法做好信创相关的风险管理。金融信创不只是软硬件的替换，改造过程中需要重点关注系统迁移的稳定性、兼容性与安全性，评估供应商支持能力、运维连续性、应急回退安排与业务影响。核心业务系统、支付清算系统、交易系统、风控系统等重要系统开展信创改造时，宜同步考虑等级保护测评、漏洞管理、供应链安全管理、业务连续性管理和外包管理；如相关采购属于关键信息基础设施运营者采购且可能影响国家安全的，还需进一步判断是否触发网络安全审查。

四、关键信息基础设施：金融业专属保护要求进一步落地

金融是《网络安全法》和《关键信息基础设施安全保护条例》明确列举的重要行业和领域之一，但并非金融机构的所有网络设施和信息系统均当然构成关键信息基础设施。一旦重要网络设施、信息系统遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生与公共利益的，才需要结合认定规则进一步判断。按照上位规则，行业保护工作部门需制定本领域认定规则，组织开展认定并通知运营者。

根据征求意见稿，《办法》拟在行业层面细化认定与管理流程。国务院金融管理部门按照金融业关键信息基础设施认定规则组织识别金融业关键信息基础设施，确定认定结果后通知运营者，并通报公安部门、抄送网信部门。运营者发生合并、分立、解散等情况，或者关键信息基础设施出现较大变化可能影响认定结果的，需要及时向监管部门报告。

被认定为金融业关键信息基础设施运营者的机构，需要承担更高强度的组织与技术义务，相关要求在上位条例基础上做了金融行业的专属细化。组织架构上，运营者主要负责人对安全保护工作负总责，明确主管网络安全的领导班子成员担任首席网络安全官，并为每个关键信息基础设施明确一名安全管理责任人。运营者还应设置专门安全管理机构，并对专门安全管理机构负责人和关键岗位人员进行安全背景审查。

供应链安全方面，运营者需要按照国家网络安全审查规定与金融行业预判指南申报审查，按要求报送年度网络产品和服务、云计算服务采购清单，同时规范商用密码的使用管理。这项要求与上位法中关键信息基础设施采购的国家安全审查规则形成呼应。

风险评估方面，运营者每年至少开展一次全面的网络安全检测与风险评估，覆盖等级保护测评、商用密码应用安全性评估、关基保护制度与标准落实情况、数据与个人信息保护情况、风险监测处置情况、应急处置改进情况等内容。检测评估发现的问题需要及时整改，相关情况按年度向监管部门报送。

一个容易产生误区的地方在于，金融业关键信息基础设施合规并不是一次性的认定工作，而是持续性的日常管理机制。认定完成后，机构仍需持续投入治理资源，围绕组织管理、人员审查、供应链管控、年度评估和应急演练等事项建立日常管理机制。《办法》本身未列明金融业关键信息基础设施认定规则的具体内容。机构可结合网络设施、信息系统对关键核心业务的重要程度、受损后的危害程度以及对其他行业和领域的关联性影响开展内部摸排，但最终仍应以监管部门认定和告知为准。

五、网络运行、应用分发与违法违规信息处置纳入明确要求

除传统信息系统安全要求外，《办法》进一步明确了金融从业机构在网络运行与信息服务环节的管理义务。机构需要常态化开展网络运行监测、安全风险与事件处置报告工作，建立网络安全事件应急预案，通过技术与管理双重措施保障网络运行安全。此外，《办法》在总则中要求金融从业机构积极为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。机构在落实该要求时，还需同步关注内部授权、资料留存、数据提供范围和个人信息保护等配套管理。

网络信息内容管理也被纳入监管要求。机构发现法律、行政法规禁止发布或者传输的信息，需要立即停止传输，采取处置措施防止信息扩散，留存相关记录并向主管部门报告。对于向公众提供应用软件下载服务的机构，还需要履行恶意程序与违法违规信息检测义务。发现应用软件存在设置恶意程序，或者含有法律、行政法规禁止发布、传输的信息的，应立即停止提供下载服务，保存有关记录，并向有关主管部门报告。

这项要求对提供手机银行、证券交易、支付钱包、贷款申请、财富管理、商户服务等移动应用的机构均有直接影响。对于提供相关移动应用的金融从业机构，APP 上架、版本更新、下载包校验、恶意代码检测、第三方 SDK 管理、应用签名证书管理、仿冒应用监测等事项，宜纳入应用安全和网络安全管理范围。

六、数据安全与个人信息保护：纳入网络安全治理框架，并与既有规则衔接

《办法》没有对数据安全与个人信息保护做大量细化规定，仅将其纳入网络安全整体治理框架。明确要求机构加强网络数据分类分级管理，采取技术与管理措施防范数据被篡改、破坏、泄露或者非法获取、非法利用，同时依法规范个人信息处理活动，保障个人信息安全，鼓励使用国家网络身份认证公共服务开展用户身份核验。

这种处理方式契合《办法》的通用框架定位。金融机构的数据安全与个人信息保护工作，仍需依据《数据安全法》《个人信息保护法》《网络数据安全管理条例》以及各监管条线的专项规则具体落实。《办法》主要是将相关要求纳入金融业网络安全整体治理框架，提示机构统筹开展体系建设，避免将系统安全、数据安

全、个人信息保护割裂处理。

七、监管协同与法律责任：跨部门共治的执法逻辑

《办法》设置了专门的监督管理协同章节，明确国务院金融管理部门按照监管职责分工开展工作，同时支持配合国家网信部门、公安部门、密码管理部门及其他主管部门，依据职责开展金融业网络安全保护与监督管理工作。金融管理部门的同级分支机构、派出机构之间，需要强化安全事件、风险、态势、情报等信息共享，根据工作需要会商研判行业整体风险态势。

法律责任层面，《办法》采用衔接式立法思路，不另行创设大量罚则，而是打通金融监管部门与其他主管部门的既有执法权限。比如机构未按规定使用商用密码的，金融管理部门将案件信息移送同级密码管理部门，并配合开展执法。拒绝、阻碍监督检查的，依照人民银行法、商业银行法、银行业监督管理法、保险法、证券法、网络安全法等对应法律法规处理。其他网络安全保护义务，如《网络安全法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》《网络数据安全管理条例》已有处罚规定，金融管理部门将依照上述法律、行政法规并按监管职责分工处理；上述法律、行政法规未作处罚规定但其他法律、行政法规已有处罚规定的，依照其他规定处理。

这种设计带来的直接影响是，同一网络安全风险事件或违规行为，可能引发金融监管、网络安全监管、数据安全监管、个人信息保护监管、密码监管等多个维度的关注；情节严重的，还可能延伸至治安管理或刑事责任。网络安全合规已经成为典型的综合性监管事项，需要科技、安全、法务、合规、数据、业务连续性、采购与外包管理等多个部门协同参与。

八、机构的合规准备方向

目前《办法》仍处于公开征求意见阶段，正式文本内容可能进一步调整。结合当前规则，机构可以提前开展几方面的准备工作。

一是完成主体与规则的梳理。确认自身是否属于《办法》适用范围，系统比对现行有效的网络安全、数据安全、个人信息保护与信息科技相关规则，明确通用要求与分业要求的重叠和差异。地方金融组织可以关注属地监管的后续动态。

二是补全治理架构的短板。明确网络安全负责人和牵头部门，保障资金与人员投入，把分支机构、下属法人机构、重要外包服务商都纳入管理范围。集团化机构尤其需要理清总部与下属主体的权责边界，并通过正式制度固定。

三是基础合规工作要落到实处。全面梳理自有系统的等保定级情况，核对备案与测评的时效性，把历史测评发现的问题逐项整改到位。同步排查现有商用密码应用场景；对于等保、关基或监管规则要求开展商用密码应用安全性评估的系统，提前准备相应材料和整改计划。

四是可能涉及关键信息基础设施的机构提前摸排。按照系统重要性、受损危害程度做内部预判，提前梳理人员、制度、供应链方面的合规缺口。如待正式认定通知后再启动相关工作，可能面临组织架构、人员审查、供应链材料和年度评估机制短期内难以补齐的问题。

五是供应链和信创风险宜前置管理。采购重要网络产品和服务时，应在合同中明确安全义务、漏洞修复、事件响应、保密要求、数据安全和个人信息处理要求。信创项目应同步开展安全评估，并准备必要的应急回退安排，降低迁移过程中的安全事件和业务中断风险。

六是应急和报告机制需具备可执行性。机构应对照《办法》和各监管条线的事件报告要求，统一内部事件分级、上报流程、证据留存和对外沟通规则，并通过定期演练检验预案有效性。

结语

整体看，《办法》的核心监管信号，是金融业网络安全监管正在从分业规则走向协同治理，从技术防护要求进一步延伸至组织治理、资源保障和责任落实。虽然规则篇幅不长，但后续正式落地后，可能对机构内部治理、技术管理、合规审查、采购管理和外包管理产生持续影响。机构可结合自身业务情况，在征求意见期内向监管反馈实操问题与建议，并以本次规则为契机，系统排查现有网络安全体系的短板，提前做好制度和执行层面的准备。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

段志超

电话： +10 8516 4123
Email： kevin.duan@hankunlaw.com

权威

电话： +21 6080 0946
Email： wei.quan@hankunlaw.com