HANKUN

汉坤法律评述

2026 年 7 月 27 日

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

筑安于数：银行业网络安全合规新规解读

作者：郑婷 | 应尔寅 | 梁笑 | 张馨予 | 王若男

一、概览

2026 年 7 月 3 日，中国人民银行（“**央行**”）、国家金融监督管理总局（“**金监局**”）、中国证券监督管理委员会与国家外汇管理局，就联合起草的《金融业网络安全管理办法（征求意见稿）》（“**《金融业网安办法（征求意见稿）》**”），向社会公开征求意见。该征求意见稿适用于各类金融机构，意见反馈截止日期为 2026 年 8 月 3 日。

一周后，金监局发布了更为专项的《银行业保险业网络安全管理办法（征求意见稿）》（“**《银保网安办法（征求意见稿）》**”）公开征求意见，意见反馈截止时间为 2026 年 8 月 10 日。该征求意见稿适用对象包括银行业金融机构、保险业金融机构、金融控股公司，其中“银行业金融机构”不仅包括各类商业银行，还涵盖集团财务、金融租赁、消费金融、信托、理财、货币经纪等银行业非银持牌机构。

两份征求意见稿的相继出台，体现了金融业一般监管要求与银行保险业专项规则互为补充的制度安排。而在此之前，对于银行业金融机构而言，已有多部核心法规相继出台，构成了严密的监管规则：

- 《网络安全法》（“**《网安法》**”）：发布于 2016 年 11 月 7 日并于 2025 年 10 月 28 日修正，为首部系统规范网络安全的国家法律，建立了包括网络运行安全及网络信息安全在内的原则性要求。
- 《网络数据安全管理条例》（“**《网数条例》**”）：发布于 2024 年 9 月 30 日，从国家行政法规层面确立了数据分类分级、重要数据保护及跨境流动的法律框架。
- 《银行保险机构数据安全管理办法》（“**《银保数安办法》**”）：发布于 2024 年 12 月 27 日，侧重于规范银行业保险业的数据处理全生命周期活动与安全治理职责。
- 《中国人民银行业务领域数据安全管理办法》（“**《央行业务数安办法》**”）：发布于 2025 年 5 月 1 日，明确了央行监管职责领域内业务数据分类分级、技术防护及合规审计的基线要求。
- 《中国人民银行业务领域网络安全事件报告管理办法》（“**《央行业务网安事件报告办法》**”）：发布于 2025 年 5 月 23 日，专门针对央行监管职责领域的安全事件报告时限与量化分级做出规定。
- 《网络数据安全风险评估办法》（“**《网安评估办法》**”）：发布于 2026 年 6 月 18 日，明确了网络数据处理者开展风险评估的分类分级管理制度。

在结合现有监管规则的基础上，本文旨在提示银行业金融机构[非关键信息基础设施运营者（**“关基运营者”**）]在新规即将实施后需履行的合规义务及重点关注事项。

二、主要对比

两部草案在监管思路和核心制度设计方面总体保持一致。下表围绕公司治理架构、等级保护与商用密码、供应链与外包管理、风险评估与监管报告四个重点方面，对两部草案的监管要求进行对比，并结合银行业金融机构现阶段适用的相关监管规则，分析其与既有合规要求的衔接。

对比维度	《金融业网安办法（征求意见稿）》	《银保网安办法（征求意见稿）》	简要解读
公司治理架构	■ 确定网络安全负责人（第 5 条） ■ 建立管理组织架构和议事决策机制，指定牵头管理部门（第 6 条）	■ 党委（党组）、董（理）事会负主体责任，主要负责人为第一责任人，分管网络安全的高级管理人员为直接责任人（第 7 条） ■ 指定网络安全主管部门归口管理（第 8 条）	两部征求意见稿和《网安法》第 23 条及《银保数安办法》第 10 条和第 11 条对银行业金融机构数据安全治理架构及责任体系的要求基本保持一致
等级保护与商用密码	■ 定级备案、按期测评、整改风险（第 8 条） ■ 按等保要求使用商用密码（第 9 条）	■ 落实等级保护制度，三级及以上网络每年至少开展一次等级测评（第 33 条） ■ 开展密码保障系统规划、建设、运行和商用密码应用安全性评估，使用符合国家相关要求的密码产品和服务（第 34 条）	两部征求意见稿未新增关于等级保护及商用密码的要求，而是要求银行业金融机构遵循现有的国家网络安全等级保护制度要求，即《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》《金融行业网络安全等级保护实施指引》等项下规定的监管要求
供应链与外包	按照国务院金融管理部门有关规定报送年度网络产品和服务、云计算服务采购清单（第 17 条）	■ 建立信息科技供应链安全风险管理制度，建立供应链产品清单，与重要外包供应商签订服务水平协议，制定供应中断预案并开展演练（第 30 条） ■ 新技术引入前开展安全评估（第 31 条） ■ 按信息科技外包监管要求开展外包管理（第 32 条） ■ 关基运营者应与网络产品和服务提供者签订安全保	《银保网安办法（征求意见稿）》进一步细化了银行保险机构在信息科技供应链及外包管理方面的具体要求，相关要求整体上与现行《银行保险机构信息科技外包风险监管办法》下的监管要求保持一致。《金融业网安办法（征求意见稿）》新增的报送年度网络产品和服务、云计算服务采购清单的要求在《银保网安办法（征求意见稿）》下明确仅适用于关基运

对比维度	《金融业网安办法（征求意见稿）》	《银保网安办法（征求意见稿）》	简要解读
		密协议，可能影响国家安全的应当通过国家网络安全审查，且应向金监局报送年度网络产品和服务、云计算服务采购清单（第56条）	营者。
风险评估与监管报告	针对关基运营者，提出了每年至少进行一次网络安全检测和风险评估的要求（第18条）	■ 发现可能对行业造成影响的供应链安全风险，可能对行业造成影响的漏洞缺陷，或可能涉及其他金融机构或可能对行业造成影响的威胁情报，应当立即向金监局或者其派出机构报告（第23、30和39条） ■ 将网络安全年度工作情况纳入信息科技年度工作报告，每年1月15日前向金监局或其派出机构报送。报告内容应当包括网络安全治理、网络安全建设和运行管理、网络安全风险监测、事件响应与处置等（第65条）	《金融业网安办法（征求意见稿）》未针对银行业金融机构单独设置网络安全风险评估及年度报告要求，相关义务主要依据各机构所在各领域监管规则执行。 针对非关基运营者的银行业金融机构，《银保网安办法（征求意见稿）》进一步明确了网络安全年度报告及重大风险报告机制。实践中，银行等机构往往将相关年度报告的内容进行整合提交。
应急处置	开展网络运行监测、网络安全风险和事件处置报告等工作，建立健全网络安全事件应急预案，采取相应的技术和管理措施，保障网络运行安全（第7条）	■ 建立网络安全事件管理制度，网络安全事件应急响应与处置组织架构，制定应急预案，并在发生网络安全事件后根据应急预案进行调查、评估、处置及报告金监局或其派出机构（第42条至第48条）	《银保数安办法》第68条及第69条和《央行业务数安办法》第44条规定了与数据安全事件相关的应急处置相关要求，银行业金融机构可统一制定及实施适用于网络安全事件及数据安全事件的应急处置机制。

三、合规清单

我们注意到，《银保网安办法（征求意见稿）》相较《金融业网安办法（征求意见稿）》在企业日常合规管理方面提出了更为具体和细化的要求。结合现行适用的法律法规及监管规定，我们梳理了银行业金融机构

在网络安全及数据安全领域需定期履行或重点关注的主要合规事项如下[1]：

合规事项	强制频率要求	法规依据
一、评估类		
网络安全风险评估	每年至少一次（对于银行业金融机构，应将境内外分支机构及附属机构的网络安全工作纳入评估范围）	《银保网安办法（征求意见稿）》第 41 条
数据安全风险评估	重要数据处理者应当每年度对其网络数据处理活动开展风险评估，并向省级以上有关主管部门报送风险评估报告	《网络数据安全管理条例》第 33 条
	重要数据处理者应当每年度开展网络数据安全风险评估。鼓励处理一般数据的网络数据处理者至少每 3 年开展一次风险评估	《网安评估办法》第 5 条
	所有银行保险机构（无论是否重要数据处理者）每年一次，评估报告需在次年 1 月 15 日前报送至金监局	《银保数安办法》第 66 条和第 74 条
	在央行业务领域，重要数据的处理者应当每年度对其业务数据开展风险评估，并于每年 1 月 15 日前报送上一年度评估报告至央行或其住所地省级分支机构	《央行业务数安办法》第 42 条
注：《网络数据安全管理条例》第 55 条允许重要数据风险评估和网络安全等级测评的内容重合的，相关结果可以互相采信。银行业金融机构可合并开展相关风险评估及审计，以减少重复评估、审计的行政成本。此原则同时适用于下述审计类合规要求。		
触发式（专项）评估	当重要数据的安全状态发生重大变化（如系统重大变更、处理目的/范围实质性变化、发生数据泄露事件等）时，应当及时开展评估	《网安评估办法》第 5 条
	互联网信息系统、等保三级及以上网络和重要信息系统，在投产或发生重大变更前，应当通过安全测试评估	《银保网安办法（征求意见稿）》第 26 条
特定活动前置评估	处理敏感级及以上数据、开展数据委托处理、共同处理、转移、公开、共享等对主体有较大影响的活动前，应当事先开展评估	《银保数安办法》第 22 条
	涉及批量敏感级及以上数据的数据共享、委托处理、转让交易、数据转移，银行保险机构应当在处理、合同签署前 20 个工作日向金监局或者其派	《银保数安办法》第 73 条

[1] 提请注意，《银保网安办法（征求意见稿）》目前尚未正式生效，以下合规事项主要基于现有监管要求及征求意见稿内容进行整理，旨在提示银行业金融机构提前开展合规准备工作。相关具体实施要求仍需以正式发布的监管规定为准。

合规事项	强制频率要求	法规依据
	出机构报告	
	信息系统、模型算法在投入使用前，应当开展数据安全审查，评估其合理性、正当性及对主体权益的影响	《银保数安办法》第 51 条
	向其他数据处理者提供、委托处理、共同处理重要数据前，应当事先开展评估	《央行业务数安办法》第 22 条
	新技术引入前应当开展安全评估	《银保网安办法（征求意见稿）》第 31 条
商用密码评估	按国家商用密码管理制度要求开展 注：国家商用密码管理制度主要包括《中华人民共和国密码法》《商用密码管理条例》《商用密码应用安全性评估管理办法》等，关基运营者应当自行或者委托商用密码检测机构每年至少开展一次商用密码应用安全性评估，确保商用密码保障系统正确有效运行；非关基运营者无年度评估的强制要求。	《银保网安办法（征求意见稿）》第 34 条
二、审计类		
网络安全审计	每三年至少开展一次	《银保网安办法（征求意见稿）》第 41 条
重大（二级）及以上网络安全事件专项审计	及时开展	《银保网安办法（征求意见稿）》第 49 条
重大数据安全事件专项审计	及时开展	《银保数安办法》第 66 条
数据安全全面审计	每三年至少开展一次	《银保数安办法》第 66 条
数据操作行为审计	定期进行，审计周期不超过六个月	《银保数安办法》第 43 条
三、其他		
全员安全培训	每年至少一次 注：《央行业务数安办法》第 13 条要求数据处理者每年组织业务数据处理活动参与人员开展相关教育培训。培训内容应当包括与业务数据安全相关的制度标准、风险防范常识、岗位责任、保护措施和事件应急处置要求。银行业金融机构可合并开展前述培训。	《银保网安办法（征求意见稿）》第 12 条
漏洞处置分析	每季度至少一次情况分析	《银保网安办法（征求意见稿）》

合规事项	强制频率要求	法规依据
		第 23 条
等级保护测评	三级及以上网络每年至少一次	《银保网安办法（征求意见稿）》第 33 条、《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》第二（二）点
互联网渗透测试	每年至少一次	《银保网安办法（征求意见稿）》第 41 条
应急演练	每年至少一次（需至少包含重要外包服务提供商）	《银保网安办法（征求意见稿）》第 44 条、《银行保险机构信息科技外包风险监管办法》第 31 条

《银保网安办法（征求意见稿）》第 13 条至第 29 条同时规定了银行业金融机构就其网络安全建设和运营管理应实施的管理与技术保护措施，银行业金融机构可结合《银保数安办法》第四章（*数据安全管理*）、第五章（*数据安全技术保护*）与《央行业务数安办法》第三章（*全流程业务数据安全管理要求*）、第四章（*全流程业务数据安全技术要求*）对照落实。

四、安全事件评级及报送要求

《银保网安办法（征求意见稿）》《央行业务网安事件报告办法》及《银保数安办法》分别针对网络安全事件及数据安全事件建立了事件分级和报告机制。三套规则均将安全事件划分为四个等级（特别重大、重大、较大、一般），并规定了相应的报告及处置要求。

需要注意的是，虽然三套规则在事件等级划分及报告机制方面存在较大程度的相似性，但由于监管关注重点不同，各规则对于事件影响范围、数据类型、业务中断程度、受影响主体数量等具体定级标准存在一定差异。以下对三套规则下的**主要评级标准**及**报告要求**进行汇总列示：

	《银保网安办法（征求意见稿）》/银保网络安全事件	**《央行业务网安事件报告办法》/央行业务网络安全事件**	**《银保数安办法》/银保数据安全事件**
一、数据安全/网络安全事件等级划分			
一级（特别重大）	■ 网络安全原因导致敏感级及以上数据泄露/破坏 ■ 2 个及以上省业务停摆 3h；或 1 个省业务停摆 6h ■ 网络安全原因导致重要信息系统服务中断	■ 实际影响自然人 1,000 万，或法人/组织 100 万 ■ 央行业务领域核心数据遭篡改/泄露 ■ 泄露敏感信息 1,000 万条或个人信息 1 亿条	■ 核心数据遭到泄露、破坏或者非法获取、非法利用。 ■ 重要数据泄露、破坏或者非法获取、非法利用影响 2 个以上省级区域经济

	《银保网安办法（征求意见稿）》/银保网络安全事件	《央行业务网安事件报告办法》/央行业务网络安全事件	《银保数安办法》/银保数据安全事件
			■ 敏感级及以上数据遭到大规模泄露、破坏或者非法获取、非法利用对国家安全、政治安全、经济金融安全、公共利益造成特别严重影响
二级（重大）	■ 重要数据、敏感数据遭到泄露、破坏、非法获取、非法利用 ■ 2 个及以上省业务停摆 0.5-3h；或 1 个省业务停摆 3-6h ■ 重要信息系统（非关键基础设施）被入侵获取权限	■ 实际影响自然人 100 万，或法人/组织 10 万 ■ 央行业务领域重要数据遭篡改/泄露 ■ 泄露敏感信息 100 万条或个人信息 1,000 万条	■ 重要数据泄露、破坏或者非法获取、非法利用影响省级区域经济 ■ 敏感级及以上数据泄露致多个机构业务或系统严重受损或对公共利益、个人和组织权益造成严重影响
较大（三级）	■ 重要数据、敏感数据遭到泄露、破坏或者非法获取、非法利用 ■ 重要系统异常，致 1 个省业务中断 0.5-3h ■ 重要信息系统被入侵或攻击篡改	■ 实际影响自然人 10 万，或法人/组织 5,000 个 ■ 泄露征信/财产信息 500 条；或个人信息 5 万条 ■ 遭受勒索恶意程序攻击造成危害	敏感级及以上数据遭到泄露、破坏或者非法获取、非法利用致机构自身部分业务停摆或声誉受损或对个人财产、名誉造成难消除的负面影响
一般（四级）	对组织或个人造成一定影响的事件，或一般数安事件。	■ 业务网络单省中断 30min；或主要功能中断 1h ■ 实际影响自然人 1 万 ■ 发生或可能发生个人信息泄露、篡改或丢失	除上述外，对组织或者个人造成一定影响的数据安全事件
二、报告要求			
简要/初步报告	针对较大（三级）及以上网络安全事件，2 小时内口述/书面	针对较大等级以上网络安全事件，1 小时内报送简要报告	2 小时内（不区分事件等级）
正式书面报告	24 小时内提交	24 小时内报送	24 小时内提交
处置进展更新	一级事件每 2 小时报告一	二级（重大）及以上事件至少	一级事件每 2 小时报告一次

	《银保网安办法（征求意见稿）》/银保网络安全事件	《央行业务网安事件报告办法》/央行业务网络安全事件	《银保数安办法》/银保数据安全事件
	次进展	每 2 小时报告一次	进展
事后总结报告	针对较大（三级）及以上网络安全事件，处置结束后 5 个工作日内	处置结束后 10 个工作日内。无法按时报送事后调查总结报告的，金融从业机构应当先按时报送初步报告，说明承诺报送事后调查总结报告的日期并按时报送。承诺日期原则上应当在处置结束之日起 40 个工作日内。涉及个人信息泄露的，总结报告须说明补救措施及通知个人的情况	处置结束后 5 个工作日内（含改进报告）

五、总结

对于银行业金融机构而言，《金融业网安办法（征求意见稿）》和《银保网安办法（征求意见稿）》是金融行业主管部门针对金融机构在网络安全领域的统领性规范，为银行进一步完善网络安全治理体系、落实相关合规要求提供了明确指引。由于网络安全同时包含网络设施、信息系统、数据资源等多个维度，其与网络安全等级保护、信息系统外包、商用密码保护、及数据安全保护等既有法规存在相呼应与衔接的紧密关系，银行业金融机构应系统化梳理各监管要求并可合并遵从相关监管要求。我们也将持续关注相关监管动态，并结合监管要求及行业实践，跟进分析银行业金融机构网络安全及数据安全合规要求的最新发展。

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：

郑婷

电话： +86 21 6080 0203
Email： ting.zheng@hankunlaw.com