新规背景下的境外上市网络安全审查路径

近期，证监会发布的境外上市备案新规，开启了企业境外上市全口径备案监管的新时代。网信部门联合其他部委发布的网络安全审查新规，则对何类主体境外上市需要申报网安审查、赴港上市是否需要主动申报审查等核心问题，提供了阶段性的信号。证监会备案新规与网安审查新规相互配合映衬，为发行人完成网安审查预判、上市时间安排等关键事项，赋予了更加清晰的指引路径。本文对此进行解读，并就未来可能面临的问题和待澄清的事项进行分析和展望。

一. 新规发布与背景

2021年12月24日，中国证券监督管理委员会（“证监会”）联合国务院有关部门起草发布了《国务院关于境内企业境外发行证券和上市的管理规定（草案征求意见稿）》（“《境外上市管理规定意见稿》”）和《境内企业境外发行证券和上市备案管理办法（征求意见稿)》（“《境外上市备案办法意见稿》”，与《境外上市管理规定意见稿》合称“境外上市新规意见稿”），给中国企业境外上市带来了具有根本制度性变革的全新监管框架。

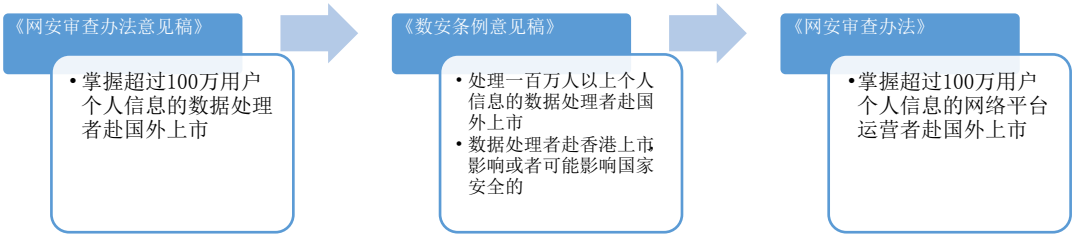
在境外上市新规意见稿出台前，国家互联网信息办公室（“网信办”）于2021年7月10日发布《网络安全审查办法（修订草案征求意见稿）》（“《网安审查办法意见稿》”），于2021年11月14日发布《网络数据安全管理条例（征求意见稿）》（“《数安条例意见稿》”）；近期，作为对《网安审查办法意见稿》的最终敲定，网信办于2022年1月4日联合国家发展和改革委员会、工业和信息化部等部委正式发布《网络安全审查办法》（“《网安审查办法》”）。上述规定通过演进的规则探讨，对企业的网络安全审查提供了规则指引，同时将网络安全审查与境外上市之间进行了关联，使得网络安全审查成为部分境外上市项目流程中的必备申报环节。

证监会及网信办等部门的上述一系列新规，亦回应了“滴滴事件”发生以来，各界对境外上市流程中的网络安全审查程序的关切与疑问。2021年7月2日，网信办发布《网络安全审查办公室关于对“滴滴出行”启动网络安全审查的公告》，由网络安全审查办公室对“滴滴出行”实施网络安全审查。“滴滴事件”首次在公众视野下将企业境外上市与网络安全审查制度进行了联结。

在此之后，网信办先后迅速发布《网安审查办法意见稿》和《数安条例意见稿》，在规则层面，首次要求在特定情境下的境外上市过程中，发行人应主动申报网络安全审查。但是，这两项规定本身含有许多留白，一些细节也引起业界较大争议与讨论。更重要的是，就上市程序而言，在没有证监会境外上市新规意见稿出台的情况下，网信办新规期待的网络安全审查程序，应当被放置在境外上市过程中的哪个具体阶段，是否需要与证监会或者其他监管部门的程序协同建构监管一致性机制，都给市场主体留下了许多疑问。

《网安审查办法》《境外上市管理规定意见稿》和《境外上市备案办法意见稿》等新规回应了一段时间以来市场关于网络安全审查制度如何影响企业境外上市的困惑和疑虑，聚焦并指引了新形势下企业境外上市过程中核心关注的与网络安全审查有关的程序性问题，明确了规则界限，在一定程度上减轻了制度的不确定性，同时也提出了企业境外上市过程中可能需关注的网络安全及数据合规领域的新问题。本文主要对此进行分析与提示。

二. 证监会及网信办等部门的新规释放的阶段性明确信号



(一)赴国外上市需主动申报网络安全审查的情形仅限于处理大量个人信息的网络平台运营者

《网安审查办法》明确限定，仅符合一定情况的“网络平台运营者”赴国外上市，需要主动申报网络安全审查。

这一主体范围，比《数安条例意见稿》中规定的“数据处理者”这一申报主体，要更加限缩，体现了监管态度向务实化、谦抑化、合理化的方向发展。

《数安条例意见稿》规定的“数据处理者”指在数据处理活动中自主决定处理目的和处理方式的个人和组织。在绝大部分场景中，大量的企业就与其相关的数据处理活动而言，均可能被认定为数据处理者。虽然《数安条例意见稿》对上市主动申报网络安全审查的数据处理者也附加了其他条件（例如处理一百万人以上个人信息），但由于“数据处理者”本身过于普遍、宽泛，适用“数据处理者”作为框定范围的基础条件将使得适用的主体基数过于庞大。无论是何种行业领域的企业，在经营过程中或多或少会进

行数据处理活动。一些数据处理者尽管处理的数据量较大，但是其服务或活动性质本身不敏感，数据处理活动处理的数据类型亦不敏感，涉及的业务条线并不典型，如果将全部类型的数据处理者都作为网络安全审查的适用主体，会加重市场主体的负担和分散监管重点。

《网安审查办法》规定的“网络平台运营者”，在较多情境下作为“数据处理者”的一种类型，能够体现监管机构在监管资源有限的情况下，聚焦监管敏感主体、敏感情境的思路，有利于实现精准监管、高效监管的目标。当然，“网络平台运营者”具体的含义，在现有规则框架下有一定的类似制度可供参考借鉴（详见后文第“三”部分的讨论），但是关于“网络平台运营者”的明确含义和边界，还有待网络安全审查实践给出答案。

(二)没有要求赴香港上市需要主动申报网络安全审查

《数安条例意见稿》引发广泛讨论和争论的一项制度是，其新增要求数据处理者赴香港上市，影响或者可能影响国家安全的，应主动申报网络安全审查。首先，在当前国际政治经济局势和市场环境下，大量企业从计划的其他上市地转赴香港上市，如果香港上市被纳入网络安全审查监管，会使得大量企业负有申报义务。其次，香港是我国的一部分，香港证券市场监管者对发行人的监管立场、尺度，以及潜在可能因个人信息出境和数据交换引发的顾虑，与其他国家的证券市场及其监管者可能引发的顾虑相比，应当有所不同。

因此，《网安审查办法》最终的规定，仅仅规定赴国外上市需要主动申报网络安全审查，没有加入香港上市需要主动申报。这一定程度上顺应了市场的期待与需求。

此外，对于《数安条例意见稿》规定的赴港上市需要申报网络安全审查的要求，由于《网安审查办法》已经明确不要求赴港上市申报审查，所以，在后续《数安条例意见稿》经修订变为正式的《网络数据安全管理条例》的过程中，起草机关从合理的角度，也应当保持与《网安审查办法》已经释放的信号相一致的思路，就境外上市申报审查不创造新的申报情境，只有这样，才能保持同一部门就同一事项监管的一致性，否则可能引发较大的执法和守法难题。

(三)拟上市企业网络安全审查申报的时间节点明朗化

《境外上市管理规定意见稿》以及《境外上市备案办法意见稿》将H股、大红筹、小红筹等各类境外上市形式，统一纳入证监会的备案监管框架内，要求各类企业境外上市需要向证监会提交备案材料。其中，要求在适用的情况下，网络安全审查意见将作为一项证监会备案的必备材料，划定了拟上市企业应进行网络安全审查申报的时间节点，即在向证监会提交

上市备案材料前需要完成网络安全审查并收到审查意见。

结合境外上市新规征求意见稿，以首次公开发行为例，企业应当在境外提交首次公开发行上市申请文件后3个工作日内，向证监会提交备案材料。因此，企业实际上在境外提交首次公开发行上市申请文件之前，就应完成网络安全审查。

就网络安全审查法定审查期限而言，根据适用的程序类型不同：

- 理论上最短法定审查期限约**55**个工作日（即：10个工作日内确定是否需要审查 + 30个工作日内完成初步审查 + 网络安全审查工作机制成员单位15个工作日回复书面意见）。

- 理论上最长法定审查期限约**160+N**个工作日（即：10个工作日内确定是否需要审查 +30个工作日内完成初步审查 + 情况复杂的延长15个工作日 + 网络安全审查工作机制成员单位15个工作日回复书面意见 +特别审查程序90个工作日 +情况复杂的可以延长）。

- 实际操作中，由于材料提交及往复沟通并补充材料需要时间，且提交补充材料的时间不计入上述审查时限，所以实际需要的时间，较有可能比上述时间更长。

尽管在复杂情况下，额外延长的规定且补充材料的时间不计入法定审限，但是上述申报时间框架给企业提供了一个相对明晰的时间表，一定程度上有利于明确IPO时间表的预期，便利发行人倒算时间进行IPO准备排期。

但是，需要关注的是，发行人应提前对其是否需要申报网络安全审查进行较为谨慎的预判。例如，对于是否“掌握超过100万用户个人信息”，是否属于“网络平台运营者”，应当以更为谨慎的尺度进行全面衡量和评估。需要谨慎预判的原因在于，如果发行人以较为匆忙或冒进的立场，判断自己不需要申请网络安全审查，那么：

- 首先，发行人不会因为自身预判不需要申报网安审查，就使其在证监会的备案流程中可以回避网安审查的问题。证监会建立跨部门协调机制，所以在其审核发行人提交给证监会的备案材料过程中，证监会依旧可能联合网信办对发行人是否需要申报网络安全审查进行判断。例如，证监会2021年12月24日发布的《证监会有关负责人答记者问》中提及，“证监会将牵头建立企业境外上市跨部门监管协调机制，在收到企业备案申请材料后，主动与有关主管部门加强沟通或征求意见，以提高备案效率。同时，证监会将配合推动有关主管部门明晰相关领域的监管制度规则，提高政策可预期性。最后，

对涉及外商投资安全审查、网络安全审查等法律法规规定范围内的企业境外上市，在提交备案申请前，企业应当依法申报安全审查”。由此可见，无论在发行人自我预判中是否认定需要完成网络安全审查并进行申报，证监会在接收企业提交的备案材料时，均有权并可能会就企业是否需要进行网络安全审查与网信办等主管部门沟通并征求其意见。

- 其次，这样的预判，可能会严重拖延发行人完成证监会的备案流程的进度。尽管《境外上市备案办法意见稿》规定，备案材料完备、符合规定要求的，证监会在20个工作日内出具备案通知书，但是需要特别注意，如果“不需申报”的预判与证监会的理解（以及证监会会同网信办等主管部门协商的理解）不同，则《境外上市备案办法意见稿》规定了两个法定延期机制：（1）《境外上市备案办法意见稿》第10条第2款规定，备案材料不完备或不符合规定要求的，证监会在收到备案材料后5个工作日内告知需补充的内容，并且补充材料的时间不计算在备案时限内；（2）如果上述（1）的情形，还可以理解为证监会必须在收到备案材料后5个工作日内告知，具有明确时限和可预期性，那么影响更为深远的是《境外上市备案办法意见稿》第10条第3款规定，在备案过程中，发行人可能存在《境外上市管理规定意见稿》第7条[1]所列情形的，证监会征求有关主管部门意见的时间不计算在备案时限内。这意味着，如证监会认为发行人可能需要申报网安审查，并询网信办意见，证监会、网信办的征求和协商意见过程没有法定时限。此刻，发行人在境外的IPO申请文件已经提交，但是可能面临证监会和网信办一项无明确期限的监管协商与审查，无疑容易将整个IPO计划拖入被动局面。

(四)网络安全审查中的风险消解整改制度初探和展望

《网安审查办法》规定了申请人的网络安全风险消解整改制度。其第16条规定，“为了防范风险，当事人应当在审查期间按照网络安全审查要求采取预防和消减风险的措施”。

纯粹以文意解读和结构解读的角度考虑，上述制度体现在《网安审查办法》第16条中，该条款规定了主管机关主动启动网络安全审查程序的情形。因此，该条规定的风险消解整改制度本身可能仅在主管机关主动启动网络安全审查的程序中出现及适用。

[1] 《境外上市管理规定意见稿》第7条规定，存在下列情形之一的，不得境外发行上市：……（二）经国务院有关主管部门依法审查认定，境外发行上市威胁或危害国家安全的……。

但是，上述制度以外，《境外上市管理规定意见稿》也规定了实质具有风险消解整改效果的制度。其第8条规定，“境内企业境外发行上市的，应当严格遵守外商投资、网络安全、数据安全等国家安全法律法规和有关规定，切实履行国家安全保护义务。涉及安全审查的，应当依法履行相关安全审查程序。国务院有关主管部门可以要求剥离境内企业业务、资产或采取其他有效措施，消除或避免境外发行上市对国家安全的影响”。如前文所述，在发行人向证监会提交备案材料前，就应当已经完成网络安全审查程序。因此本条所述“有关主管部门可以要求剥离境内企业业务、资产或采取其他有效措施”，在较多情境下应指网信办会同其他部门审核网络安全审查申报的程序中，可以采取相应措施。

网信办与证监会的两条规定如何协同，是有待网络安全审查实践探寻的问题。从企业完成上市的动力和动机角度而言，在业务结构支持的情况下，企业有可能在主动申报的过程中，为了能通过网安审查，主动承诺剥离部分业务，服务“完成上市”这一主目标。因此，期待的一个方面是，主管机关也可以综合考虑，在企业主动申报的网安审查程序中，是否允许企业承诺采取剥离等风险消解整改措施，以便能在消解国家安全顾虑的同时，给企业一条相对便捷合理的上市通道。

不论企业主动申报的过程中还是主管机关主动启动网安审查的过程中，如果允许风险消解整改制度存在，并且如果期待这一制度的效果能延及网安审查程序结束之后，形成长效机制，那么风险消解整改制度的执行机制，或许值得参考经营者集中申报中的附条件批准制度，形成结构性、持续性的承诺措施。例如，风险消解整改制度应当考虑实际执行效果，特别是剥离行为不应是表面性的、暂时性的剥离，是否可能在具体案例中，要求申请人聘请律师事务所或者行业顾问等“监督受托人”，对剥离的承诺与执行进行持续性的监督，以避免在上市完成后，申请人立即恢复了剥离业务、从而减损了承诺效果。

(五)上市过程中的信息出境仍是主管机关的关注要点

《境外上市管理规定意见稿》第16条规定，“境内企业境外发行上市的，应当严格遵守国家法律法规和有关规定，建立健全保密制度，采取必要措施落实保密责任，不得泄露国家秘密，不得损害国家安全和公共利益。境内企业境外发行上市涉及向境外提供个人信息和重要数据的，应当符合国家法律法规和有关规定”。

上述规定既是证监会对企业境外上市信息与数据出境热点事件的再次回应，也是对近年颁布的《中华人民共和国数据安全法》（“《数据安全法》”）以及《中华人民共和国个人信息保护法》（“《个人信息保护法》”）中重要数据出境以及个人信息出境制度的呼应。

关于企业境外上市信息与数据出境的顾虑由来已久。例如，就上市企业的审计底稿出境问题，中国证监会、国家保密局、国家档案局早在2009年曾联合发布的《关于加强在境外发行证券与上市相关保密和档案管理工作的规定》中要求“在境外发行证券与上市过程中，提供相关证券服务的证券公司、证券服务机构在境内形成的工作底稿等档案应当存放在境内”。

审计底稿之外，与境外上市有关的其他信息，是否可能因上市行为产生额外的出境风险，也是主管机关一直以来关注的问题。尽管当前境外证券监管机构要求发行人披露的信息相对限缩，也不直接涉及大量系统性的底层业务数据或经营生产中的全局个人信息，但鉴于境外证券主管机关有权修改披露规则和信息提供规则，所以这也作为我国主管机关立法过程中特别关注的事项。例如，在2019年《中华人民共和国证券法》修订时特别增加了第177条第2款规定，“境外证券监督管理机构不得在中华人民共和国境内直接进行调查取证等活动。未经国务院证券监督管理机构和国务院有关主管部门同意，任何单位和个人不得擅自向境外提供与证券业务活动有关的文件和资料”。此外，该等信息也需要受到个人信息与重要数据出境的相应规则的规管，例如：

- 《个人信息保护法》第38条至第43条中规定的诸如个人信息出境的几项前提条件，需要取得个人信息主体的单独同意，以及达到一定数量的个人信息出境时完成安全评估等；同时，《个人信息保护法》第41条明确要求，非经中华人民共和国主管机关批准，个人信息处理者不得向外国司法或者执法机构提供存储于中华人民共和国境内的个人信息。

- 《数据安全法》第31条对关键信息基础设施的运营者和其他数据处理者在境内收集和产生的重要数据的出境规定亦需要被遵守。此外，《数据出境安全评估办法（征求意见稿）》第4条也点明，出境数据中包含重要数据的，需要申报数据出境安全评估。但是，重要数据的认定还有待各地区、各部门确定地区以及相关行业、领域的重要数据具体目录，企业对此还需持续关注。

需要特别注意的是，上述规定中，无论是证监会管制的“与证券业务活动有关的文件和资料”还是其他法律法规中约束的“个人信息”和“重要数据”出境，其适用条件均划定为向“境外”提供信息的场景，而不仅局限于向“国外”提供。所以，赴香港上市的企业也需要特别注意遵守和落实上述信息跨境传输的规管要求。

三. 需要关注或可能面临的新问题

(一) 二次上市及再融资等交易是否需要主动申报网络安全审查，尚有待明晰

《境外上市备案办法意见稿》对何种境外资本市场交易安排需要报证监会备案有相对细致、明确的规定。例如，除企业典型的首次公开发行（IPO）外，《境外上市备案办法意见稿》明确规定二次上市也需按相同标准提交材料进行备案[2]，明确了境外上市后再融资的，也需要按照较为缩减的要求提交一些备案材料[3]。

相比之下，《网安审查办法》规定何种“上市”需要主动提交网安审查，仍带有一定的模糊性。目前规定的情形是“上市”，也使用了“拟提交的首次公开募股（IPO）等上市申请文件”的描述，所以典型的首次公开发行必定属于主动申报网安审查的情形。但是，例如“二次上市”或上市后在同一市场的再融资是否需要主动申报网安审查，仍有待实践检验。《网安审查办法》提及的“拟提交的首次公开募股（IPO）等上市申请文件”虽然指向IPO，但是这一规定仅仅是在《网安审查办法》第8条所述需要提交的材料清单中，以列举示范的形式出现，并且也带有“等上市申请文件”这样的兜底尾缀，所以具体是否严格限定为IPO，亦有待检验。市场主体也有充分的动力期待网信办、证监会等主管机关能够在实践中尽快明确尺度，便利企业尽早作出更有确定性的规划。

(二)赴港上市在多大程度上依旧与网络安全审查有关，仍有待主管机关明晰及实践的检验，也敦促企业把握底线思维，注重网安与数据处理合规

《网安审查办法》的一大重要指向是不再提及赴港上市需要主动申报网络安全审查，但赴港上市在机制上并不必然与网络安全审查制度隔绝。

例如，《网安审查办法》第16条保留了主管机关依职权主动启动网络安全审查的机制，其启动触发点依旧是“影响或者可能影响国家安全”。这一规定在根本逻辑上与《数安条例意见稿》规定的“影响或者可能影响国家安全”的赴港上市需要申报网安审查是相通的。

作为配套的制度，如上文所述，证监会明确表达了对境外上市要建立跨部门监管协调机制。所以在赴港上市过程中，基于当前的规定，发行人固然没有主动事先申报网安审查的法律义务，但是在向证监会提交备案材料后，依旧需要面临证监会、网信办对于其赴港上市是否“可能影响国家安全”的审视；如确有疑虑，证监会、网信办也有上文所述的各类制度性规则

---

[2] 《境外上市备案办法意见稿》第5条第2款规定，发行人境外发行上市后在其他境外市场发行上市的，应当按照本条规定履行备案程序。

[3] 《境外上市备案办法意见稿》第6条规定，发行人境外上市后发行境外上市证券，应当在发行完成后3 个工作日内，向中国证监会提交备案材料，包括但不限于：（一）备案报告及有关承诺；（二）境内法律意见书。

来启动网安审查。这一系列配套措施也从另一个角度要求并敦促发行人，即使在赴港上市项目中，也应当始终关注网络安全合规及数据处理合规状况，其中特别需要关注数据与信息的出境实践及企业管控，力争避免出现重大合规瑕疵与问题，避免被拉近“可能影响国家安全”这一网安审查启动底线的可能性。

(三)网络平台运营者的界定

《网络安全审查办法》中规定的主动申报义务主体为“网络平台运营者”，但没有直接给出“网络平台运营者”的详细定义，该定义及适用范围的界定关乎是否需要主动申报网络安全审查。

参考法律规范中相类似的概念，较为接近的是《中华人民共和国电子商务法》所称“电子商务平台经营者”、《数安条例意见稿》所称“互联网平台运营者”以及《互联网平台落实主体责任指南（征求意见稿）》所称“互联网平台经营者”等概念。具体参考以下表格：

法规名称	相关内容
《中华人民共和国电子商务法》	第9条 “电子商务平台经营者”，是指在电子商务中为交易双方或者多方提供网络经营场所、交易撮合、信息发布等服务，供交易双方或者多方独立开展交易活动的法人或者非法人组织。
《数安条例意见稿》	第73条 “互联网平台运营者”是指为用户提供信息发布、社交、交易、支付、视听等互联网平台服务的数据处理者。 “大型互联网平台运营者”是指用户超过五千万、处理大量个人信息和重要数据、具有强大社会动员能力和市场支配地位的互联网平台运营者。
《互联网平台落实主体责任指南（征求意见稿）》	“互联网平台”，是指通过网络信息技术，使相互依赖的双边或者多边主体在特定载体提供的规则下交互，以此共同创造价值的商业组织形态。 “平台经营者”，是指向自然人、法人及其他市场主体提供经营场所、交易撮合、信息发布等互联网平台服务的法人及非法人组织。通过互联网等信息网络从事销售商品或者提供服务的自建网站经营者，可参照平台经营者适用本指南。

《网络交易监督管理办法》	第7条　本办法所称网络交易平台经营者，是指在网络交易活动中为交易双方或者多方提供网络经营场所、交易撮合、信息发布等服务，供交易双方或者多方独立开展网络交易活动的法人或者非法人组织。
《国务院反垄断委员会关于平台经济领域的反垄断指南》	第2条 相关概念 （一）平台，本指南所称平台为互联网平台，是指通过网络信息技术，使相互依赖的双边或者多边主体在特定载体提供的规则下交互，以此共同创造价值的商业组织形态。 （二）平台经营者，是指向自然人、法人及其他市场主体提供经营场所、交易撮合、信息交流等互联网平台服务的经营者。

尽管如此，从上述不同法律规范中观察到相类似表述的立法定义，依据网络平台的特征，大致可以分为两种类型：

第一种定义基于功能主义，立法定义着重于“互联网服务应用媒介”的本质。例如，《互联网平台落实主体责任指南（征求意见稿）》规定：“互联网平台是指通过网络信息技术，使相互依赖的双边或者多边主体在特定载体提供的规则下交互…”。

第二种定义基于场景理论，着眼于社会经常使用的互联网服务应用，将此类常用网络服务的特征按照所属的业务领域划分，动态的予以类型化规范。例如，《数安条例意见稿》规定“互联网平台运营者定义为用户提供信息发布、社交、交易、支付、视听等互联网平台服务的数据处理者”。

结合上述，企业在排查判断自身是否构成《网安审查办法》中网络平台运营者时，可以重点考虑三个要素：

(1) 网络服务的内容是否涉及信息发布、社交或交易等公众经常使用的典型网络平台服务类型。

(2) 运营者提供的网络服务应用，其服务内容是否具有便利“交互”、“联结”双边或多边群体的主要特征。应考虑的是，网络服务应用联结的类型是人与物、人与人或是物与物等类型，在无进一步的规范出台前，均可能构成“平台”。

(3) 网络服务是否具有积累或撮合大量信息和数据的可能性。

(四)数据安全审查制度与网络安全审查制度的关系和进一步衍化

在《网安审查办法意见稿》和《网安审查办法》的成文过程中，因为主管机关多处强调“数据安全”和“数据处理活动的安全性”，所以数据安全被理解为

属于网络安全审查评估过程中需要考虑的重要风险因素。

但是，《网安审查办法》同时也明确提出，国家对数据安全审查、外商投资安全审查另有规定的，应当同时符合其规定。因此，在机制上，数据安全审查成为与网络安全审查并列的一项独立制度。《境外上市管理规定意见稿》和《境外上市备案办法意见稿》中，也多次将网络安全与数据安全并列。因此，“网络安全审查制度”与“数据安全审查制度”之间的关系以及未来的发展演变，成为值得关注的一个话题。

网络安全审查制度和数据安全审查制度都依托于国家安全审查监管制度，其最早由《国家安全法》确立。《国家安全法》规定：“国家建立国家安全审查和监管的制度和机制，对影响或者可能影响国家安全的…特定物项和关键技术、网络信息技术产品和服务…进行国家安全审查…”。此后，网络安全审查制度与数据安全审查制度于不同的法规中明晰。其中，网络安全审查制度源于《网络安全法》第35条的规定，“关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查”；数据安全审查制度通过《数据安全法》第24条确立：“国家建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查”。

两者审查的内容各有侧重，网络安全审查制度的审查对象主要是针对关键信息基础设施运营者采购网络产品和服务或网络平台运营者影响或可能影响国家安全的数据处理活动；数据安全审查制度的客体对象是影响或者可能影响国家安全的数据处理活动，数据处理活动包括数据的收集、存储、使用、加工、传输、提供、公开等。从《网安审查办法》第1条所述的法源依据条款来看，包含了《国家安全法》《网络安全法》和《数据安全法》；第2条明确了适用主体，既包含关键信息基础设施运营者采购网络产品和服务，又包含网络平台运营者开展数据处理活动。因此，立法者有意在目前尚未单独建立系统性的“数据安全审查制度”的情况下，为了先行抓住监管重点，将数据安全审查的核心顾虑情境并入网络安全审查流程中，在该过程中主管机关可依据网络安全审查这一现有且具有相对成熟流程的制度，一并审查上市这一特定情境中的部分数据处理活动的安全性。值得期待的是，未来应全面落实《数据安全法》的要求，建立更为完整的数据安全审查制度，并可能与网络安全审查制度在机制上做进一步的厘清。

注：曾俊刚、王筱蓁对本文亦有贡献