汉坤法律评述

2024 年 8 月 2 日

HANKUN
汉坤律师事务所
Han Kun Law Offices

北京 | 上海 | 深圳 | 香港 | 海口 | 武汉 | 新加坡 | 纽约

未雨绸缪：企业如何迎接个人信息保护合规审计？

作者：李珺 | 黄颖

2021 年，《中华人民共和国个人信息保护法》（“**《个保法》**”）首次明确个人信息保护合规审计（“**个保合规审计**”）作为个人信息处理者的一项法定义务。个保合规审计是指对个人信息处理者的个人信息处理活动是否遵守法律、行政法规的情况进行审查和评估的监督活动[1]，该制度在其他司法管辖权也有应用的先例。例如，2018 年生效的欧盟《通用数据保护条例》较早地引入了数据保护审计（Data Protection Audit）制度。

为落地个保合规审计制度，国家网信办于 2023 年 8 月发布《个人信息保护合规审计管理办法（征求意见稿）》（“**《审计办法》**”），拟从部门规章层面提供实施依据。进一步地，全国网络安全标准化技术委员会于 2024 年 7 月发布了《数据安全技术 个人信息保护合规审计要求（征求意见稿）》（“**《审计要求》**”），拟从国家标准层面为合规审计工作提供操作指引。

作为与现有法律、法规的配套标准，近期发布的《审计要求》详细规定了个保合规审计的具体操作，涵盖了审计流程、审计证据、审计内容、审计方法等内容，并提供了审计底稿模板和审计报告模板等参考文件，为个保合规审计落地提供了可参考的执行框架。本文旨在分享我们对个保合规审计要求的理解，帮助企业更有效地迎接和应对该制度的正式落地。

一、程序性实施要求对企业合规工作的参考

（一）个保合规审计触发场景

根据《个保法》，个保合规审计分为“自主审计”和“监管审计”两种类型。“自主审计”是指个人信息处理者定期自行开展审计[2]。关于自主审计的频率，根据《审计办法》，处理超过 100 万人个人信息的个人信息处理者每年至少进行一次，处理不满 100 万人的每二年至少进行一次。而“监管审计”则由监管部门发起，通常在发现企业个人信息处理活动存在较大风险或企业发生个人信息安全事件时要求进行[3]。

[1] 《审计办法》，第 3 条。

[2] 《个保法》，第 54 条。

[3] 《个保法》，第 64 条。

需要注意的是，根据《审计办法》，相较于自主审计，监管审计有严格的时限要求，该类审计原则上应当在 90 个工作日内完成，除非因情况复杂，经监管机构批准后才能延长。此外，监管审计中形成的审计报告还需报送监管部门，这意味着监管部门可能对审计结果进行审查和确认。

（二）审计执行主体

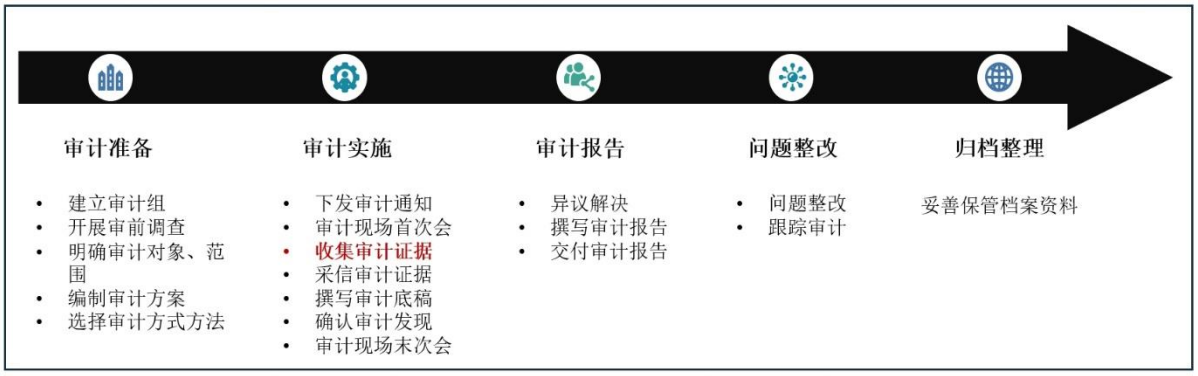
根据《审计办法》，个保合规审计执行主体分为企业内部机构和外部专业机构两大类。对于自主审计，企业可以根据实际情况灵活选择由内部机构或委托专业机构开展审计。但监管审计仅能由专业机构执行。

对于外部专业机构，《审计办法》提出国家网信部门将建立个保合规审计专业机构推荐目录，鼓励企业优先选择推荐目录中的专业机构执行审计活动。对于内部机构，此次《审计要求》明确了组建方式——企业可以根据自身内部资源的情况，从内部专职个保合规审计团队中选派组建，也可以从内审团队、安全团队、法务团队等具有审计或个人信息保护相关专业能力的团队中按合理比例选派人员进行组建。

值得注意的是，《审计要求》对审计人员的专业性、独立性、客观性、公正性和保密性提出了具体的要求。例如，根据专业性要求，审计人员应当具备个人信息保护相关领域专业能力的资质认证，但《审计要求》尚未明确具体如何落实该要求。此外，根据独立性要求，企业内部机构的审计人员应回避自身负责的业务内容，不应直接参与企业日常业务运营或个人信息保护工作。

（三）审计流程

根据《审计要求》，个保合规审计主要通过收集、审阅和评估审计证据，梳理审计发现，出具审计意见，整改并跟踪所发现的问题，具体可分为如下五个阶段。



图：个保合规审计工作流程

根据上述流程，我们建议现阶段企业关于个保合规审计工作的重点应在于审计证据的梳理和准备。根据《审计要求》，审计证据是指审计人员获取的、能够为个保合规审计结论提供合理基础的所有事实。审计证据通常包括但不限于企业的个人信息保护组织架构、涉及个人信息处理的场景和活动、处理规则、管理制度、操作规程，以及相关协议文件等。《审计要求》还对审计证据的有效性提出了具体要求。例如，委托处理协议、个人信息出境合同等协议文件必须获得各方有效同意并实际生效和执行。

需要特别提示的是，个保合规审计是对个人信息处理活动的事后评估，但审计证据作为审计工作中具体查验和评估对象，不能通过事后补救的方式制作。因此企业应将审计证据准备工作融入日常管理中，形成规范化的记录和归档机制，合规留痕，以便在审计过程中提供真实、充分、有效的审计证据，

确保审计顺利进行并取得可信的结论。

二、实质审计要点对企业合规工作的参考

除个保合规审计开展的程序性要求外，《审计要求》在附录C《个人信息保护合规审计内容和审计方法》中也详细列举了审计过程中需要审查的实质性合规要求，其中有相当部分内容系既有强制性规定的延伸或解释。结合我们的理解，以下针对值得企业关注的审计要求进行重点提示，以期为企业提供参考。

（一）完善告知与同意机制

告知和同意为《个保法》项下处理个人信息处理的基本义务，实践中企业往往通过隐私政策向个人进行告知个人信息处理规则，并获取个人对隐私政策的同意或依赖其他合法性基础满足个人信息处理的合法性要求。

对此，《审计要点》进一步明确，对于未取得同意的个人信息处理情形，审计人员需查验企业是否在隐私政策等告知文件中予以明确说明，并评估该等情形是否属于法律、行政法规规定的不需要取得个人同意的情形。实践中，很多企业笼统依赖“实施人力资源管理所必需”这一合法性基础（而非采用同意机制）处理员工所有个人信息。企业也鲜少在员工隐私政策中对具体适用的合法性基础予以说明。对此，我们建议企业审查所有个人信息处理场景中所适用的合法性基础，特别是评估那些适用同意以外的其他合法性基础的场景，并在相关隐私政策中予以充分说明。此外，《审计要点》也重申了对于处理敏感个人信息、对外提供个人信息、公开个人信息等特殊场景的单独同意要求，并进一步提出了通过产品或服务上的弹窗取得个人单独同意的方式要求。

（二）夯实出境申报豁免场景适用性

根据《个保法》及相关实施细则，个人信息处理者因业务需要，确需向中国境外提供个人信息的，应当完成数据出境安全评估、个人信息保护认证、标准合同备案等适用的出境申报程序。而国家网信部门近期出台的《促进和规范数据跨境流动规定》（“**《出境新规》**”）对前述申报程序的适用范围进行了调整，并为个人信息处理者提供了特定豁免场景。

就出境申报程序履行情况的审计内容，《审计要求》结合了《出境新规》的部分调整内容，主要关注：（1）企业是否履行了适用的出境申报程序；（2）企业实际开展的个人信息出境行为是否超出所申报的出境范围。就前述关注点，审计人员需查验数据出境安全评估报告及评估通知书、个人信息保护认证报告、与境外接收方订立的个人信息出境标准合同、平台系统中的个人信息出境记录等。值得注意的是，《审计要求》并未明确对出境申报豁免场景的审计要求。

根据我们的观察，很多企业已经依赖《出境新规》的豁免情形开展个人信息出境活动，特别是跨国企业适用“跨境人力资源管理所必需”豁免出境申报义务的情形尤为常见。据我们所知，目前监管部门倾向于将“个人信息出境活动是否落入豁免情形”的问题交由企业自行判断，但在个保合规审计中审计人员是否认可该等判断结果可能存在不确定性。因此，我们建议，拟依赖出境申报程序豁免场景的企业，应当对豁免的适用性进行充分论证，采取必要的合规措施夯实豁免的适用性，并通过相关书面记录留存合规分析，作为支持企业对豁免结论的判断。

（三）落地数据合规治理体系

企业内部数据合规治理体系为个保合规审计的核心审计内容之一。《审核要求》列明的要点包括内部组织架构、个人信息保护合规机制制定和执行情况、安全技术措施实施情况、个人信息主体权利保障

情况等。其中，《审核要点》提及的“个人信息保护合规机制”包括个人信息保护影响评估（**“影响评估”**）、个人信息安全事件应急预案、个人信息分类分级、安全教育和培训等，均为《个保法》项下的强制要求。

其中需要提示的是，《个保法》要求在开展对个人权益具有重大影响的个人信息处理活动前应当开展影响评估，并以书面形式留存影响评估报告。《审计要求》明确将影响评估报告作为前述个人信息处理活动中待查验的审计证据之一，并要求对影响评估报告的具体内容进行查验。然而，实践中，许多企业目前仅重点关注对个人信息出境活动的影响评估。鉴于《审计要求》明确将个人信息保护合规机制执行情况作为审计内容之一，我们建议企业全面执行《个保法》项下合规机制，确保不留死角。

（四）延申数据处理链条的合规管理

除企业内部处理情况外，《审计要求》的审计范围也涵盖企业合作伙伴的个人信息处理行为，例如受企业委托开展个人信息处理的受托人是否严格按照委托合同的约定处理个人信息以及是否存在转委托情况、从企业处接收个人信息的其他个人信息处理者是否在约定的范围内处理个人信息、因发生合并、重组、分立等继承企业个人信息处理行为的接收方是否继续履行企业的个人信息处理义务等。

这也意味着，个保合规审计范围实质上覆盖企业个人信息处理全链路，除企业自身外，审计对象也扩展至链路上的其他各类参与者，包括企业的受托人、个人信息接收方等。因此，企业应当加强对合作伙伴处理活动的监督，并完善与合作伙伴的数据处理协议，确保可以根据协议要求合作伙伴配合企业开展个保合规审计，包括配合进行测试或按照企业的要求提供相关的支持性文件等。

三、结语

《个保法》已出台近三周年，随着相关配套文件的陆续发布，个人信息保护要求在实践中逐步明确并开始落地实施。《审计要求》虽然不具有强制性，但考虑到个保合规审计在中国还是一项全新的事物，其对审计开展仍具有重要的指导和参考价值。为此，我们建议企业未雨绸缪，全面审视现有流程，优化个人信息处理操作实践，完善内部数据合规治理体系，做好合规留痕，确保企业在面对审计时能够从容应对。

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：

李珺

电话： +86 21 6080 0981
Email： jun.li@hankunlaw.com