个人信息保护合规审计探究

任昊源　王　颖

2022年我国数字经济规模为50.2万亿元，占GDP的比重达到41.5%[①]。数字经济在创造巨大经济价值的同时，也带来了日益严峻的数据安全问题，引发了全社会的广泛关注。为保护个人信息权益，促进个人信息的合法合规使用，我国于2021年8月20日审议通过了《个人信息保护法》，自2021年11月1日起实施。《个人信息保护法》第54条和第64条均明确提出对个人信息处理者[②]开展个人信息保护合规审计的要求，以评价和监督个人信息处理活动，降低个人信息保护合规风险。本文以《个人信息保护法》实施为背景，对我国个人信息保护合规审计的研究现状进行梳理，分析个人信息保护合规审计的重点内容和程序。同时针对个人信息保护合规审计在实务开展中面临的困境，提出相应的建议。

一、文献回顾

个人信息保护属于跨学科研究问题，学者主要从法学和计算机科学等视角对其展开广泛探讨，但对个人信息保护合规审计的研究还比较少。本文拟从个人信息保护和个人信息保护合规审计两个方面进行文献回顾。

（一）个人信息保护研究

本文在CNKI中国学术期刊网络出版总库（CAJD）中以“个人信息保护”为关键词，对1997~2022年收录于北大核心、CSSCI和CSCD的期刊进行检索，共获得文献资料1574篇。对个人信息保护的研究总体分为三个阶段。

第一个阶段为探索期（1997~2002年）。这一阶段表现出两个趋势。一是不断加强对国外个人隐私保护政策的介绍。例如：贝内特（1997）在对加拿大《魁北克68号法案》和《电子通讯法案》进行介绍的基础上，对加拿大个人隐私保护政策的要点进行了总结；周建（2001）对美国《隐私权法（1974）》中政府机构采集、使用、公开个人记录的规定进行了详细介绍，认为《隐私权法（1974）》更多的是以限制政府公开个人记录的方式来保护个人信息。二是开始对个人信息隐私保护技术进行探索。例如，孔令飞和王义刚（2000）对用于个人信息保护的密钥算法进行探索，形成了一种便于记忆、具有容错性的个人信息保护方案。第二个阶段为发展期（2003~2020年）。随着网上购物带来的消费者个人隐私泄露事件的频繁发生，学者开始关注消费者隐私泄露的法律保护问题。以郑成思（2003）为代表的法学学者基于21世纪初我国信息网络发展趋势及电子商务中面临的隐私保护问题，呼吁对个人信息保护进行立法。此后学者对个人信息保护的立法模式（杨佶，2012；侯富强，2015）、立法路径（姬蕾蕾，2017；李美艳，2018）等问题进行了深入研究。经过多年的立法探索，我国于2020年发布《个人信息保护法（草案）》，并向社会公开征求意见。但在个人信息保护的立法实践上欧美走在前列。美国于2015年发布《消费者隐私权利法案（草案）》，欧盟于2016年颁布《通用数据保护条例》。第三个阶段为繁荣期（2021年至今）。随着2021年《个人信息保护法》在我国正式实施，学者对《个人信息保护法》的解读（彭桂兵和丁奕雯，2021；王利明和丁晓东，2021）及其在实践应用中的具体法律问题（周光权，2021；朱荣荣，2022）展开广泛探讨，这助推我国的个人信息保护研究进入繁荣阶段。

（二）个人信息保护合规审计研究

现有文献较少对个人信息保护合规审计进行专门研究，相关研究大多集中在与个人信息保护相关的数据合规审计领域。在立法层面，目前国内外均对数据合规审计做出相关要求。欧盟于2016年正式颁布《通用数据保护条例》，英国信息专员办公室于2021年发布《数据审计指南》，法国数据保护局于2020年发布《审计程序指南》，均对数据合规审计提出具体要求。我国除2021年正式实施的《个人信息保护法》外，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）》，以指导个人信息保护合规审计的有效开展。

从审计需求来看，陈智敏（2022）认为推进个人信息保护合规审计不仅是保障个人信息安全的需要，也是维护社会安全稳定和推进数字中国建设的需要。从审计主体来看，传统领域的合规审计主体更多的是政府审计和内部审计（郑石桥等，2019），而与个人信息保护相关的数据合规审计，由于直接涉及社会公众的个人信息权

① 2023年4月27日，国家网信办发布《数字中国发展报告（2022年）》。

②《个人信息保护法》第73条第1款规定：个人信息处理者，是指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。

益，除政府审计和内部审计发挥作用外，还需要市场化程度更高的社会审计参与其中，以发挥其第三方独立评价职能（闫夏秋，2023）。从审计内容来看，敬力嘉（2022）认为个人信息保护合规审计不仅要审查个人信息保护合规体系的完整性，也要关注企业是否具备应对违法违规处理个人信息行为的能力，同时不能忽略对员工行为合规性的审查。从审计程序来看，贾丹等（2022）认为个人信息保护合规审计除包括传统审计程序外，还应增加审计跟踪阶段，以形成有效的闭环管理。

（三）研究述评

综上所述，为有效保障个人信息权益，学者从多学科视角对个人信息保护进行了有益的探索，推动我国《个人信息保护法》实现立法，促进我国个人信息保护进入新的阶段。但鲜有文献对个人信息保护合规审计进行系统研究，这与《个人信息保护法》对个人信息保护合规审计的要求存在较大差距。因此，本文拟结合《个人信息保护法》的具体规定系统分析个人信息保护合规审计的重点内容，在参考合规审计一般要求和个人信息保护特殊性的基础上分析个人信息保护合规审计的程序，并在深入分析个人信息保护合规审计困境的基础上提出应对策略。

二、个人信息保护合规审计的内容

（一）个人信息保护合规审计的概念界定

2022年8月国务院国资委发布《中央企业合规管理办法》，对“合规”提出三个层面的要求：一是在企业规章层面，要求企业经营管理行为及员工履职行为要符合企业章程和规章制度的要求；二是在行业监管层面，要求企业经营管理行为及员工履职行为要符合法律法规、监管规定和行业准则的要求；三是在国际公约层面，要求企业经营管理行为及员工履职行为要符合国际条约和国际规则的要求。个人信息保护的合规管理同样要遵循上述三个层面的合规要求。

为有效防范个人信息保护合规风险，将审计嵌入个人信息保护合规管理的评价和监督中，就形成了个人信息保护合规审计。个人信息保护合规审计是指审计机构和审计人员以个人信息保护的相关法律、规则及准则为依据，对被审计单位及其员工的个人信息保护行为是否合规所实施的一种监督活动。由于个人信息兼具私有属性和公共属性的特征，个人信息保护合规审计要实现双重目标：从个人信息的私有属性出发，个人信息保护合规审计要实现监管型目标，规范个人信息处理活动，防范侵害个人信息权益事件的发生；从个人信息的公共属性出发，个人信息保护合规审计要实现服务型目标，促进个人信息社会价值和使用价值的发挥。

（二）个人信息保护合规审计的重点内容

《个人信息保护法》重点对个人信息处理者的义务、个人信息主体的权利实现方式、个人信息处理活动和个人信息跨境提供活动提出了合规要求。因此在开展个人信息保护合规审计时，应重点审计以下四个方面的内容。

1. 对个人信息处理者义务的合规审计。个人信息处理者的义务是指为确保个人信息处理活动符合法律法规的要求，同时防止个人信息泄露、篡改、丢失以及未经授权访问，个人信息处理者应履行的安全保障义务。审计的重点内容包括：一是重点审计个人信息保护合规制度的建设情况，重点关注个人信息处理者是否按照法律法规的要求建立个人信息保护的内部管理制度和操作流程。二是重点审计个人信息保护合规制度的遵守情况，重点关注个人信息处理者是否按照法规要求并结合自身业务特点进行个人信息的分类管理，是否采取网络安全等基础安全控制措施和加密等安全技术措施，是否定期对员工开展个人信息保护安全培训，是否制定个人信息安全事件应急预案并定期进行应急演练。三是如果对提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者进行个人信息保护合规审计，还应关注其是否成立主要由外部成员组成的独立机构对个人信息保护情况进行监督，是否按照公开、公平、公正的原则明确平台的个人信息保护规范和义务，是否定期发布个人信息保护社会责任报告等。

2. 对个人信息主体权利实现方式的合规审计。个人信息主体的权利是指个人信息主体在个人信息处理活动中所享有的知情权、决定权、查阅权、复制权、转移权、更正权、补充权、删除权、要求解释权和代行使权。在进行个人信息主体权利实现方式的合规审计时，审计的重点内容是个人信息处理者是否有效响应个人信息主体的各项权利，以及是否为个人信息主体行使各项权利提供对应的申请受理和处理机制等。

3. 对个人信息处理活动的合规审计。个人信息处理活动包括个人信息的收集、存储、使用、加工、传输、提供、公开和删除等活动。审计的重点内容包括：一是在个人信息收集活动的合规审计中，重点关注个人信息收集是否获得授权同意，收集方式是否具有合法正当性，收集目的是否明确且合理，收集范围是否存在超范围收集情况，收集频率是否为所必需的最低频率，收集数量是否为所必需的最小数量。二是在个人信息存储活动的合规审计中，重点关注存储期限是否为所必要的最短时间，存储地点是否存在境内存储的要求，存储技术是否采用加密和去标识化等安全措施，存储设置是否

具有备份和恢复策略。三是在个人信息使用和加工活动的合规审计中，重点关注是否超范围使用个人信息，是否对个人敏感信息进行脱敏展示，是否对个人信息查询进行授权管理，是否对个人信息加工处理过程进行防泄露管控。四是在个人信息传输活动的合规审计中，重点关注是否对个人信息传输进行分级管控，是否进行传输前的授权批准，是否对个人信息进行校验，是否采用入侵检测等安全技术进行传输安全保障。五是在个人信息提供活动的合规审计中，重点关注个人信息提供活动是否向信息主体尽到告知义务，提供范围是否超出个人同意范畴，是否和信息接收方签署责任协议并约束接收方行为。六是在个人信息公开活动的合规审计中，重点关注公开披露是否得到信息主体的单独同意、是否存在适当的信息保护措施、是否存在披露规则并进行准确记录。七是在个人信息删除活动的合规审计中，重点关注是否具有受理个人信息删除诉求的途径，是否按照法规要求主动删除个人信息或按照信息主体要求删除个人信息等。

4. 对个人信息跨境提供活动的合规审计。个人信息跨境提供活动是指个人信息处理者将在中国境内运营中收集和产生的个人信息向中国境外提供的行为。在进行个人信息跨境提供活动的合规审计时，应重点关注跨境提供个人信息是否满足安全评估、个人信息保护认证、标准合同签约等基本条件，是否在跨境提供前进行个人信息保护影响评估，是否在跨境提供前向信息主体尽到告知义务并获取同意，是否经过中国主管机构批准后向境外司法和执法机构提供，是否存在向列入限制或者禁止清单的境外组织和个人提供个人信息的情形，是否对跨境提供的数据提供安全保障措施等。

三、个人信息保护合规审计程序

个人信息保护合规审计既可以由个人信息处理者的治理层发起[③]，也可以由履行个人信息保护职责的政府监管部门发起[④]。不同发起主体下个人信息保护合规审计的程序存在差异。由个人信息处理者治理层发起的个人信息保护合规审计属于个人信息处理者内部组织开展的审计，审计程序要遵循内部审计准则的相关要求。由履行个人信息保护职责的政府监管部门发起的个人信息保护合规审计要遵循政府部门发布的关于个人信息保护合规审计相关的管理规范。

（一）个人信息处理者治理层发起的个人信息保护合规审计程序

由个人信息处理者治理层发起的个人信息保护合规审计既可以委托内部审计部门实施，也可以委托社会审计中的第三方独立审计机构实施，在审计程序上要遵循内部审计准则的要求。按照中国内部审计协会发布的《第1101号——内部审计基本准则》的规定，完整的审计程序包括审计计划、审计准备、审计实施、审计报告和审计整改。具体如图1所示。此外，在个人信息处理者治理层委托第三方独立审计机构实施个人信息保护合规审计时，还应遵循《第2309号内部审计具体准则——内部审计业务外包管理》的相关规定。内部审计部门或第三方独立审计机构在实施个人信息保护合规审计过程中，要对个人信息处理者的治理层负责，将审计报告及整改结果向个人信息处理者治理层报告。

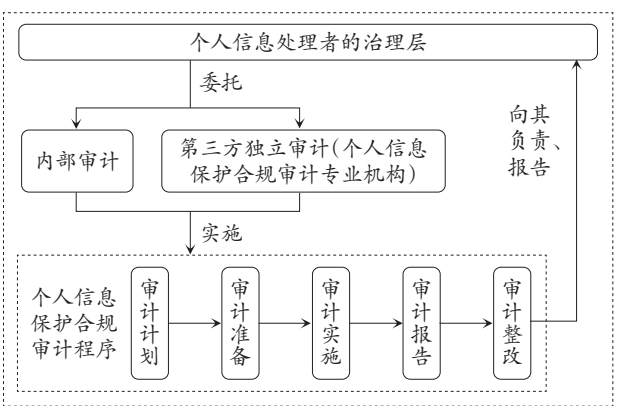

图1　个人信息处理者治理层发起的个人信息保护合规审计程序

1. 审计计划阶段。在审计计划阶段，个人信息保护合规审计既要制定中长期的审计规划，也要编制年度审计计划和项目审计方案。首先，将个人信息保护合规审计纳入总体审计规划。结合外部法律法规和监管政策的要求，参考同行业侵害个人信息权益的违法违规事件，考虑内部管理对个人信息保护机制的建设需求，合理制定个人信息保护合规审计的中长期审计规划。其次，基于审计规划的结果，编制个人信息保护合规审计的年度计划。在个人信息保护合规风险评估基础上，结合审计资源配置情况，确定个人信息保护合规审计的年

③《个人信息保护法》第54条规定：个人信息处理者应当定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。

④《个人信息保护法》第64条规定：履行个人信息保护职责的部门在履行职责中，发现个人信息处理活动存在较大风险或者发生个人信息安全事件的，可以按照规定的权限和程序对该个人信息处理者的法定代表人或者主要负责人进行约谈，或者要求个人信息处理者委托专业机构对其个人信息处理活动进行合规审计。个人信息处理者应当按照要求采取措施，进行整改，消除隐患。

度目标、拟实施的审计项目、实施时间，并确定是否需要委托第三方独立审计机构以及委托实施的具体审计项目。最后，编制具体项目的个人信息保护合规审计方案。根据个人信息保护合规审计年度计划确定的审计项目，制定具体项目的审计方案。审计方案内容包括审计项目的基础信息、审计目标与重点、审计程序与方法、审计资源的分配、对外部信息技术专家及法律专家的利用等。在委托第三方独立审计机构时，个人信息处理者治理层等相关方还需与第三方独立审计机构沟通个人信息保护合规审计方案，确保其符合个人信息保护监管政策要求。

2. 审计准备阶段。在审计准备阶段，要为个人信息保护合规审计项目的具体实施提供所需的条件。一是开展审前调查。通过现场查看、面谈交流、资料分析、书面描述、实施分析性程序等方法总体把握个人信息保护合规审计项目的基本情况。二是明确审计内容和范围。在审前调查基础上，结合个人信息使用场景、个人信息处理活动和保护措施现状等，确定具体项目的审计内容和审计范围。三是确定合规审计的开展方式。结合审计资源的投入情况、审计工具的使用情况和审计专业能力情况，灵活选择专项审计方式、持续审计方式或在其他审计项目中协同开展个人信息保护合规审计的方式。四是确认内外部资源支持情况。对开展个人信息保护合规审计所需的人力资源、财务资源、技术资源、信息情报资源以及外部专家资源等的准备情况进行确认，以确保审计工作的顺利开展。此外，在委托第三方独立审计机构时，个人信息处理者应为第三方独立审计机构开展个人信息保护合规审计提供所必需的工作条件和权限，确保第三方独立审计机构能够顺利开展审计工作。

3. 审计实施阶段。在审计实施阶段，为确保审计目标的实现，可综合使用多种审计方法。一是访谈法。可通过线上或线下方式对授权访问个人信息的人员进行访谈，了解个人信息处理活动的基本状况。二是文件检查法。对个人信息安全管理制度、隐私政策、合同协议、运行文档、留存日志等资料进行查阅检查。三是实地检查法。对个人信息的处理场景、个人信息处理活动的相关设备运行情况进行实地检查。四是穿行测试。通过追踪个人信息在信息系统中的全部处理过程，以了解个人信息处理活动的全部业务流程。五是渗透测试。必要时，在计算机系统中对处理个人信息的信息系统平台进行授权模拟攻击，以测试信息系统平台的安全性。六是控制测试。评价是否存在与个人信息处理活动相关的控制，以及这些控制是否得到有效执行，以确认个人信息保护措施是否有效，是否达到个人信息保护的目的。七是实质性程序。在控制测试基础上，对发现的与个人信息处理有关的问题进行进一步核对和确认，收集合规审计证据。在委托第三方独立审计机构时，个人信息处理者治理层等相关方应定期或不定期听取第三方独立审计机构的汇报，了解项目实施的进度，协助解决审计过程中遇到的问题，确保审计项目的顺利实施。

4. 审计报告阶段。在审计报告阶段，审计机构应在与被审计单位进行问题沟通、意见反馈的基础上，出具正式审计报告。鉴于个人信息保护合规审计的特殊性，除与专业部门沟通外，还需与法务部门、合规部门、大数据部门、舆情部门、信息技术部门等进行沟通，确认是否符合实际情况。正式审计报告的内容通常包括：审计概况、审计依据、审计结论、审计发现、审计意见和审计建议。个人信息保护合规审计报告既要注重对合规问题的事实、定性、原因、影响的说明，给出恰当的审计结论和审计处理意见，以满足监管型审计目标的要求；同时，也要注重对合规问题原因的剖析，并给出有价值的建议，促进个人信息的合理利用，实现服务型审计的目标。在委托第三方独立审计机构时，个人信息处理者治理层等相关方应对第三方独立审计机构提交的审计报告初稿进行复核并提出意见，确保个人信息保护合规审计报告的质量符合监管政策要求。

5. 审计整改阶段。审计整改阶段是审计闭环管理的最后环节，对跟踪审计发现问题和落实审计意见执行具有监督作用。一是确认个人信息保护合规审计问题的整改情况。重点关注是否对个人信息处理的业务、运营、管理等活动存在的控制缺陷进行整改，是否优化业务处理流程和操作，是否完善个人信息保护管理制度，是否修订个人信息保护的隐私政策等，以确认审计整改是否达到预期效果。二是发现审计意见执行过程中出现的问题。重点关注是否存在审计意见不符合当前实际情况的情形，是否出现个人信息保护法规政策变化等新情况，进行复查后，重新做出审计决定。在委托第三方独立审计机构时，个人信息处理者治理层等相关方可就审计整改结果与第三方独立审计机构进行沟通，征求第三方独立审计机构的意见。

（二）政府监管部门发起的个人信息保护合规审计程序

由履行个人信息保护职责的国家网信办等政府监管部门发起的个人信息保护合规审计，针对的通常是在个人信息保护领域存在较大风险或发生风险事件的个人信息处理者，其程序如下页图2所示。个人信息处理

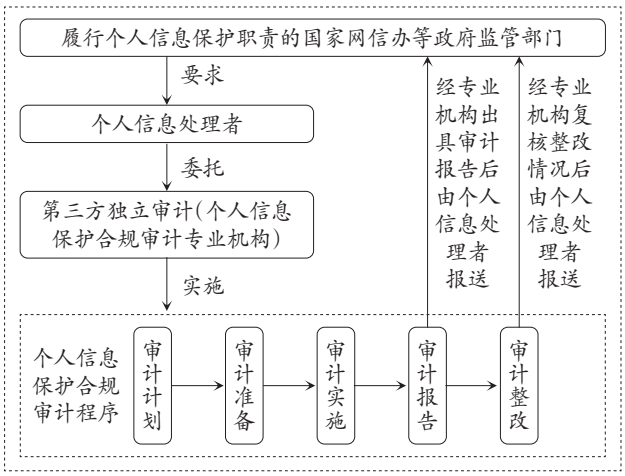

图2　政府监管部门发起的个人信息保护合规审计程序

者应按照履行个人信息保护职责的政府监管部门的要求,委托第三方独立审计机构开展个人信息保护合规审计。在审计程序上要遵循国家网信办等政府监管部门发布的相关规定。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)》,对第三方独立审计机构实施个人信息保护合规审计有专门要求。在第三方独立审计机构的选择上,政府监管部门在开展定期动态评价的基础上,向个人信息处理者发布个人信息保护合规审计专业机构推荐目录,并鼓励个人信息处理者优先选择。由于存在已经评估评价并优先推荐的个人信息保护合规审计专业机构,因此,在审计程序上,监管政策更注重对审计实施、审计报告和审计整改环节的要求,而在审计计划和审计准备环节以专业机构的自我管理为主。以下就审计程序各阶段的特殊内容进行阐述。

1. 审计计划阶段。在审计计划阶段,个人信息保护合规审计专业机构要与个人信息处理者签订审计业务约定书,明确双方的权利与义务,确认双方对业务约定条款不存在误解。同时,个人信息保护合规审计专业机构应做好审计方案的编制,并与个人信息处理者沟通方案内容,确保其符合监管政策要求。

2. 审计准备阶段。 在审计准备阶段,个人信息保护合规审计专业机构除做好通常情形下的审计准备工作外,要重点确认个人信息处理者是否为其开展审计工作提供必要的工作权限。必要的工作权限包括:能够访谈与个人信息处理活动相关的人员,能够观察场所内发生的个人信息处理活动,能够检查个人信息处理活动相关设备设施,能够调查个人信息处理活动及所依赖的信息系统,能够查阅个人信息处理活动的数据和信息等。

3. 审计实施阶段。在审计实施阶段,个人信息保护合规审计专业机构面临审计实施时间和实施质量的双重要求。从审计实施时间来看,现有的监管政策要求个人信息保护合规审计专业机构必须在限定时间内完成审计工作,这既是有效利用审计资源以提升审计工作效率的要求,也是防范风险暴露过长时间导致个人信息保护风险事件向社会外溢的需要。从审计实施质量来看,个人信息保护合规审计专业机构应以科学有效的审计方法和充分可靠的审计证据来保障审计质量,不能因刻意追求审计质量而恶意干扰个人信息处理者的正常经营活动。

4. 审计报告阶段。在审计报告阶段,个人信息保护合规审计专业机构应在保障审计报告质量的同时,及时出具审计报告。在审计报告质量保障方面,个人信息保护合规审计专业机构在实施必要的合规审计程序的基础上,如实出具审计报告。若存在虚假出具或不实出具报告情形,除面临剔除出个人信息保护合规审计专业机构推荐目录的风险外,还面临因违反《个人信息保护法》而被追究法律责任的严重后果。在审计报告报送时间方面,个人信息保护合规审计专业机构应及时出具审计报告,并由个人信息处理者在规定时间内报送履行个人信息保护职责的政府监管部门。

5. 审计整改阶段。在审计整改阶段,个人信息处理者不仅要履行整改义务,还要履行整改情况的报送义务。首先,个人信息处理者应按照专业机构给出的整改建议进行整改,弥补个人信息保护合规风险漏洞。其次,在整改完成后,个人信息处理者应将经专业机构复核后的整改情况报送履行个人信息保护职责的政府监管部门。政府监管部门将其作为监管并评价个人信息处理者的重要依据。

四、个人信息保护合规审计面临的困境

(一)个人信息保护合规审计的实践不足

我国个人信息保护合规审计实践不足,主要表现在两个方面。一是在标准制定层面,尚未形成可供参考的个人信息保护合规审计规范。目前无论是《国家审计准则》《中国注册会计师审计准则》还是《中国内部审计准则》,都未将个人信息保护合规审计纳入其中。二是在实务工作层面,个人信息保护合规审计的审计方式尚在摸索中。在面对海量多维数据的审计场景时,个人信息保护合规审计在审计范围确定、审计要点设计和审计测试深度等问题上面临诸多挑战。

我国个人信息保护合规审计实践不足的原因主要包括两个方面。从外部要求来看,我国个人信息保护法于2021年立法,立法时间较晚,导致个人信息保护合规

审计在较长时间内处于法定合规审计范围之外。从内在动因来看，一方面实施个人信息保护合规审计需要个人信息处理者投入大量的人、财、物等审计资源，增加了个人信息处理者的财务负担。另一方面，实施个人信息保护合规审计限制了个人信息处理者通过违规收集、使用、加工、传输个人信息获取经济利益的机会。因此，个人信息处理者缺少内在动力实施个人信息保护合规审计。

（二）个人信息保护合规审计的协同机制缺失

个人信息保护合规审计既涉及个人信息处理者的内部审计部门，又涉及第三方独立审计机构，还涉及承担个人信息保护职责的政府部门。因此，开展个人信息保护合规审计需要多主体的协同。但是，从审计主体来看，在国家审计中，审计机关尚未将个人信息保护政策跟踪审计作为审计重点，对承担个人信息保护职责的政府部门的政策跟踪审计参与度较低。在社会审计中，会计师事务所的业务范围较少拓展至个人信息保护合规审计领域，对个人信息保护合规行为的第三方独立评价和监督作用发挥不足。在内部审计中，内部审计部门还局限于传统的审计领域，对个人信息保护合规管理的评价和服务职能发挥有限。总体来看，我国个人信息保护合规审计的协同联动机制尚未建立起来，未发挥出最大效力。

（三）数字化审计辅助工具应用不足

个人信息保护合规审计涉及的审计场景通常包括App、微信小程序、微信公众号、云平台以及企业信息系统等。这些审计场景产生的数据具有数据量级大、模态多的特点。传统的人工检查方式在响应时间、灵活性和处理业务量上存在局限性，导致查阅、复核、测试等程序带来繁重的工作量和高昂的审计成本，还会因为审计抽样方法的局限性导致抽样风险的发生。因此，在面对存在海量数据的个人信息保护合规审计场景时，有必要引进数字化审计辅助工具。但是数字化审计辅助工具开发的专业性和复杂性，以及不同审计场景的特殊性，导致数字化审计辅助工具在个人信息保护合规审计中应用较少。

（四）个人信息保护合规审计专业人才缺乏

个人信息保护合规审计对审计人才的要求具有特殊性，不仅要求审计人员必须具备专业的审计知识和审计技能，熟悉数据安全与隐私保护相关的法律、行政法规和行业监管政策，还要具备数据业务流程、数据治理和信息系统等专业知识，以对被审计单位的个人信息处理活动及相关的内部控制、风险管理的合规性、适当性和有效性进行专业判断。但现阶段，无论是国家审计、社会审计，还是内部审计，审计人才均以财务会计专业为主，个人信息保护合规审计人才缺口较大。

（五）保障审计建议落地的资源不足

个人信息保护合规审计建议的执行，对管理资源、财务资源和技术资源等存在较强依赖性。首先，企业内部数据分布于不同的职能部门，其权责归属复杂，对审计建议的落实，不仅涉及数据业务流程的优化，还涉及组织结构的调整，需要投入较多的管理资源。其次，对涉及个人信息处理的相关软件系统进行改造，不仅周期长，而且需要投入大量的财务资源。最后，涉及个人信息处理的相关软件系统通常只适合特定业务场景，具有专用性，需要企业投入特定的技术资源进行改造。而企业的总体资源是有限的，在管理资源、财务资源和技术资源需求量较大的情况下，很难保障资源投入的充足性。

（六）适格审计主体的认定标准缺失

个人信息保护合规审计对第三方独立审计机构存在更高要求。首先，个人信息保护合规审计涉及公众利益，要求审计机构以维护社会公众的个人信息权益为目标，对审计机构的职业能力和职业道德有更高要求；其次，个人信息保护合规审计涉及海量的个人数据，要求审计机构具备数字化审计能力。但对于审计机构具备什么样的条件，才能够从事个人信息保护合规审计，却没有统一的认定标准。这一方面导致个人信息保护合规审计的执业质量参差不齐，另一方面也削弱了第三方独立审计机构从事个人信息保护合规审计业务的意愿。

五、有效实施个人信息保护合规审计的对策建议

（一）加强个人信息保护合规审计实践

加强个人信息保护合规审计实践的着力点主要在两个方面。一是大力发展研究型审计，加强个人信息保护合规审计规范的研究。现有的审计准则尚未形成可供参考的个人信息保护合规审计规范，因此，可将个人信息保护合规审计纳入内部审计具体准则的制定范畴，通过审计专家和实务工作者的共同参与，制定《内部审计具体准则——个人信息保护合规审计》，并向社会颁布，指导审计实践的开展。二是强化典型个人信息保护合规审计案例的研究和推广。由于个人信息保护合规审计实践尚处于初期探索中，可通过对已有典型案例的研究，总结个人信息保护合规审计实务中好的经验做法，并向社会推广，为个人信息保护合规审计实践提供借鉴。

（二）建立个人信息保护合规审计的协同联动机制

个人信息保护合规审计的协同联动需要多主体的参与，既需要个人信息处理者内部的治理层、管理层和内部审计部门的参与，又需要个人信息处理者外部的履行个人信息保护职责的政府监管部门、国家审计部门和第三方独立审计机构的参与。具体的协同联动方式见下页图3。

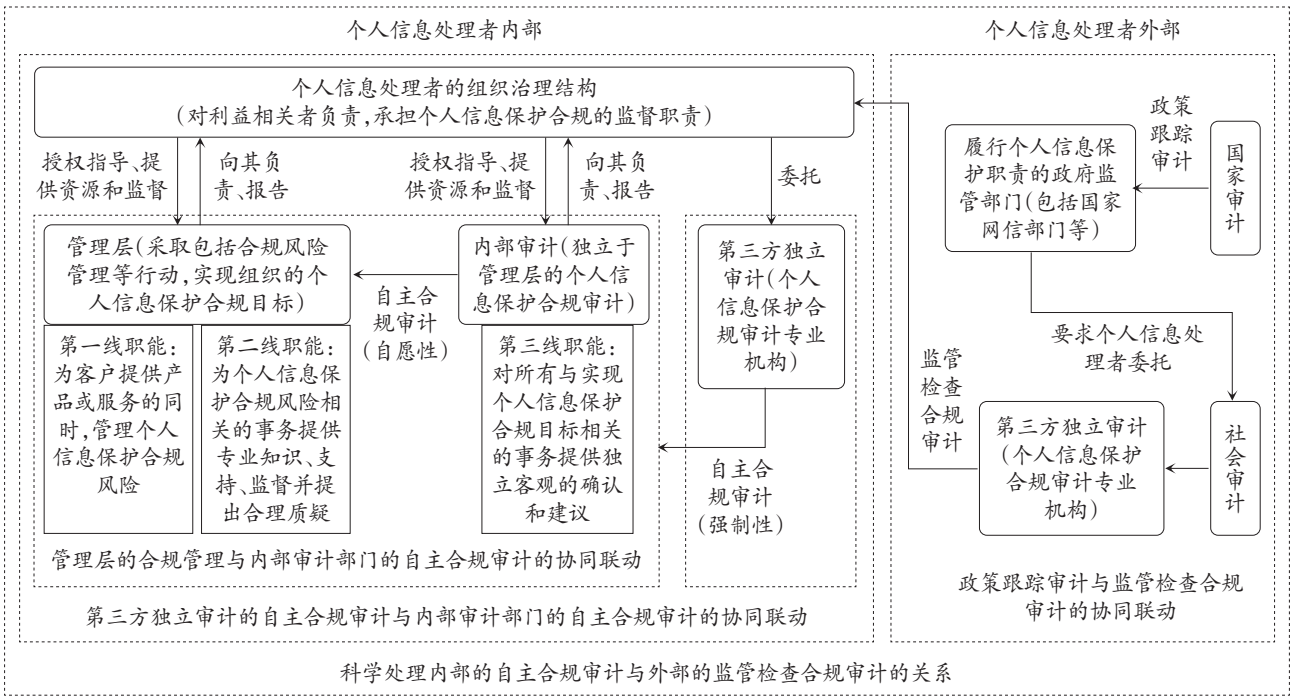

图3　个人信息保护合规审计的协同机制

首先，在个人信息处理者内部，实现管理层实施的个人信息保护合规管理与内部审计部门开展的自主合规审计（自愿性）的协同联动。为实现组织的合规管理目标，个人信息处理者有必要引进“三线模型”。其中，管理层履行第一线和第二线的职能。第一线和第二线的职能并行运行，第一线负责管理个人信息保护合规风险，第二线负责为合规风险相关事务提供补充性的专业知识，发挥支持和监督作用，两条线相互协同，以实现组织的个人信息保护合规管理目标。第三线为独立于管理层的内部审计部门，职能是为所有与实现个人信息保护合规管理目标相关的事务提供独立客观的确认和建议。内部审计部门在日常活动中提供个人信息保护合规审计时，要充分发挥服务型内部审计的职能，在发现和纠偏个人信息保护合规管理中存在问题的同时，要与管理层做好沟通协调，为个人信息保护合规管理的改进和优化提供咨询与建议，实现管理层的个人信息保护合规管理与内部审计部门的自主合规审计的协同联动。

其次，在个人信息处理者内部，实现第三方独立审计机构定期开展的自主合规审计（强制性）与内部审计部门在日常活动中开展的自主合规审计（自愿性）的协同联动。在个人信息处理者内部，自主合规审计包括两个层次。一是由治理层委托第三方独立审计机构定期开展的自主合规审计，主要为满足《个人信息保护法》第54条中定期开展合规审计的法定要求，这种法定要求虽是强制性义务，但更强调个人信息处理者通过合规审计方式进行定期自查。二是由治理层委托内部审计部门在日常活动中开展的自主合规审计，主要为满足内部管理需要，对组织内部个人信息保护合规管理情况进行独立客观的确认和提出建议。为有效降低个人信息保护合规风险，第三方独立审计机构定期开展的自主合规审计与内部审计部门在日常活动中开展的自主合规审计可在多方面实现协同。一是实现审计计划的协同共商，例如通过共同协商审计范围，在确保审计监督涵盖个人信息处理全部活动的同时，又能突出敏感个人信息等重要风险领域，最大化利用审计资源，提升审计效率。二是实现信息资源的协同共用，虽然不同审计方式获取信息的来源不同，但可以通过召开沟通会等形式实现信息资源的共享共用，以减少个人信息保护合规风险的监管盲区。三是实现合规问题的协同整改，将第三方独立审计的权威性和严肃性与内部审计的积极性和灵活性结合起来，两者形成合力，推进审计问题的有效整改。

再次，在个人信息处理者外部，实现政策跟踪审计和监管检查合规审计的协同联动。承担个人信息保护职责的政府监管部门，肩负着个人信息保护的法定职责。因此，通过对承担个人信息保护职责的政府监管部门实施个人信息保护政策跟踪审计，有利于压实国家网

信办等政府监管部门个人信息保护的责任。国家网信办等政府监管部门通过有效履行职责,对在个人信息保护领域存在较大风险或发生风险事件的个人信息处理者,要求其委托第三方独立审计机构实施监管检查合规审计,并对发现的个人信息保护安全问题进行整改。通过自上而下、层层监督的方式,实现个人信息保护政策跟踪审计和监管检查合规审计的协同联动。

最后,科学处理自主合规审计和监管检查合规审计的关系。内部的自主合规审计由个人信息处理者治理层委托发起,个人信息处理者可以自主决策,具有主动性和增值性的特点。外部的监管检查合规审计由履行个人信息保护职责的政府监管部门发起,个人信息处理者只能被动接受,具有被动性和问责性的特点。内部的自主合规审计与外部的监管检查合规审计之间具有相互转换、此消彼长的关系。如果个人信息处理者消极对待自主合规审计,则会导致组织面临较大的个人信息保护合规风险,甚至发生个人信息保护安全事件,从而带来外部监管检查合规审计更严厉的检查,并承担相应的法律责任和民事赔偿。反之亦然。因此,科学处理两者关系的关键在于,个人信息处理者要积极主动开展自主合规审计,在防范合规风险和满足监管要求的基础上,发挥个人信息的社会价值和使用价值,避免外部监管检查合规审计带来的责任赔偿和信誉损失。

(三)加强数字化审计辅助工具的开发和应用

数字化审计辅助工具是有效开展个人信息保护合规审计的利器。数字化审计辅助工具的开发和利用可以采用"现场+远程+云端"相结合的工作方式。现场审计重在总结数据业务流程的规律,选择合适的审计信息技术(例如非结构化数据转换技术、代码分析技术等),编写相应的审计脚本工具,为开发数字化审计辅助工具奠定基础。远程审计重在固化审计模型,将现场审计总结出的审计规律及开发的脚本工具固化为特定业务场景下的审计模型,并嵌入数字化审计辅助工具中,即使远离审计现场,只要能获取相关数据,就能通过开发的审计模型实现远程审计。云端审计重在对存储在云端的海量数据通过固化在数字化审计辅助工具中的审计模型进行高效处理,以发现可疑的个人信息操纵行为。在数字化审计辅助工具的开发和应用中,遵循边审计、边开发、边利用、边改进的研究型模式,以实现个人信息保护合规审计和业务场景的紧密融合。

(四)培养个人信息保护合规审计人才

随着国家、企业以及社会公众对个人信息保护重视程度的不断提升,培养个人信息保护合规审计人才势在必行。个人信息保护合规审计人才的培养要充分实现审计技能、个人信息保护合规知识体系和信息技术的融合。首先,加强在岗的个人信息保护合规审计人才的继续教育,将研究型审计思维运用于个人信息保护合规审计工作中。在审计前,注重对个人信息保护合规监管政策的学习,强化基于信息技术的审计方法研究。在审计中,注重审计技术、审计方法与特定个人信息保护场景的融合,构建并固化审计模型,以实现自动化审计。在审计后,注重个人信息保护合规审计实务案例的总结,建立个人信息保护合规审计案例库,提升审计工作效率。其次,加强高校个人信息保护合规审计人才培养体系建设。建议相关高校在审计人才培养过程中,在夯实审计知识的基础上,增设合规管理、数据分析、信息技术等选修课程,以加强对复合型审计人才的培养。

(五)保障促进审计建议落地的资源

个人信息保护合规审计建议的落地对管理资源、财务资源和技术资源等具有较高的依赖度。在管理资源保障上,个人信息处理者在治理结构层面,强化董事会对个人信息保护合规管理的职责,成立跨部门的个人信息保护合规管理团队,对涉及个人信息保护的跨部门业务流程优化和组织结构调整问题进行协调和处理。在财务资源保障上,个人信息处理者可以根据个人信息保护风险的评估情况,合理计提个人信息保护专项储备基金,在保障审计建议落地的同时,也可为发生的个人信息保护法律赔偿提供资金支持。在技术资源保障上,个人信息处理者可以综合运用全职聘用和兼职聘用,引进具有专业技术背景的人才,以防范专业技术能力不足的问题。

(六)合理制定适格审计主体的认定标准

适格审计主体认定标准的制定应由承担个人信息保护职责的政府监管部门(如国家网信办等)牵头,这样可以将个人信息保护的相关监管要求融入标准制定中。在标准制定过程中,除了要考虑审计机构的组织形式、成立年限、净资产、从业人员数量等一般标准,还要充分考虑个人信息保护合规审计的特殊要求。例如:要考虑审计机构的历史执业质量情况,是否存在行政、刑事处罚事项,是否存在违反职业道德的事项;要考虑审计机构从业人员的数字化审计能力,从业人员是否具备数字化审计的教育经历或数字化审计的职业资格(如CISA认证)等。

作者简介:任昊源,西京学院会计学院;王颖,西京学院商学院。

原载《财会月刊》(武汉),2024.2.78~85