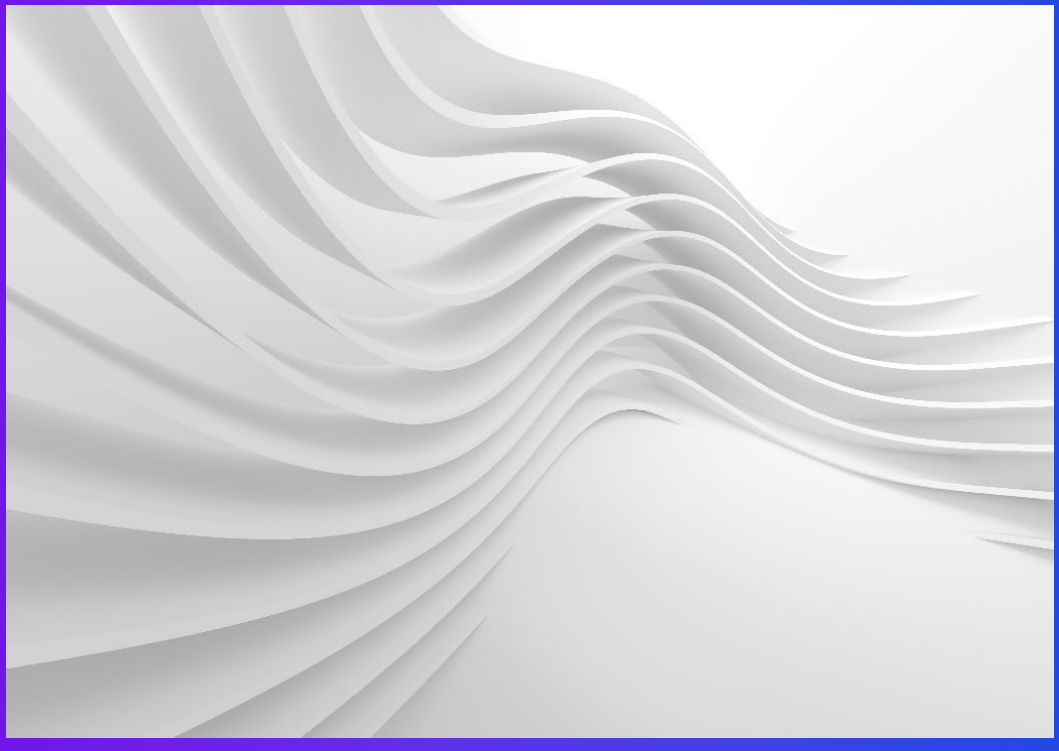
KPMG
毕马威

个人信息保护合规审计管理与应对

毕马威中国

—

2025年3月



kpmg.com/cn

序言

在数字化时代，个人信息保护已成为广大人民群众最切实关心的利益问题之一，也是涉及个人信息处理企业的重要合规义务之一。那么，企业如何保障个人信息处理活动符合国家法律法规的监管要求，而监管机构又如何审查与评价企业的个人信息保护合规情况呢?

作为一项监管对企业个人信息保护的重要“体检”工作，国家已制定法律将企业个人信息合规审计定义为一项基本义务并为其提供了制度框架。我国个人信息保护法第54条和64条明确规定了个人信息处理者的个人信息保护合规审计义务，并将审计分为自行审计与监管审计两种方式。

为进一步细化与落实指导上述个人信息保护法规定的义务工作的开展执行，2023年8月，国家网信办制定并出台了《个人信息保护合规审计管理办法（征求意见稿）》；2025年2月14日《个人信息保护合规审计管理办法》正式发布，并将于2025年5月1日正式生效。

《个人信息保护合规审计管理办法》从适用条件、个人信息处理者的责任等多个方面进行了详细规定，为企业的个人信息保护合规审计工作提供了更多细节性指导，以激励并提升企业个人信息保护能力为构建与执行个人信息保护合规审计工作。

目录

个人信息保护合规审计背景和概述

2017.6

《网络安全法》首次以法律的形式明确提出了个人信息保护的要求

2020

《信息安全技术 个人信息安全规范（GB/T 35273-2020）》首次在我国个人信息保护领域对个人信息控制者提出了“安全审计”的要求

2021.12

《关于推进个人信息保护合规审计的若干建议》，对个人信息审计的审计目标、原则、人员、内容、程序等方面设计了具体的框架

2021.11

《个人信息保护法》首次以法律的形式明确了个人信息保护领域中合规审计的法定义务

2023.8

《个人信息保护合规审计管理办法（征求意见稿）》及附件《个人信息保护合规审计参考要点》发布

2024.7

《数据安全技术 个人信息保护合规审计要求（征求意见稿）》提出了个人信息保护合规审计原则并规定了实施要求

2025.2

2025年2月14日，《个人信息保护合规审计管理办法》及附件《个人信息保护合规审计指引》正式发布

2025.1

《网络数据安全管理条例》提出网络数据处理者应当定期进行合规审计

《中华人民共和国个人信息保护法》

第54条：“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。”

第64条：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……

《网络数据安全管理条例》

第27条：网络数据处理者应当定期自行或者委托专业机构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。

个人信息保护合规审计是所有个人信息处理者的基本合规义务

开展合规审计工作的必要性：

- **遵循法律：**个人信息保护合规审计制度的建立可以完善个人信息安全法律体系，确保企业运营过程中符合相关法律法规，避免罚款和法律诉讼；
- **建立信任：**展示企业对个人信息的保护和合规意识，增强用户和企业的信任感；
- **保障数据安全：**有助于识别并降低安全风险，加强数据安全保障措施，避免数据泄露事件；
- **保护用户权益：**确保企业尊重用户权益，保护个人信息安全，避免滥用和不当使用个人信息；
- **组织规范运营：**引导组织规范运营，符合合规要求，提升整体运营效率和信誉度。

根据《个人信息保护法》，个人信息保护合规审计主要分为以下两种情形：

- **一是定期自行审计，**即个人信息处理者定期自行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；
- **二是专项强制审计，**即履行个人信息保护职责的监管部门在某些特定情形下，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。

因此企业既需要建立自主审计体系也需要考虑潜在的第三方审计可能性：

建立自主审计体系

企业自行定期开展审计：

- 处理个人信息数量超过1000万人：每两年至少开展一次

自行审计既可以由本组织内部机构开展，也可以自行委托专业机构开展。

应对潜在的监管审计

监管强制审计：

- 个人信息处理活动存在严重影响个人权益或者严重缺乏安全措施等较大风险的；
- 个人信息处理活动可能侵害众多个人的权益的；
- 发生个人信息安全事件，导致100万人以上个人信息或者10万人以上敏感个人信息泄露、篡改、丢失、毁损的。

强制审计只能由个人信息处理者委托专业机构进行审计，且个人信息处理者应当按照保护部门*要求选定专业机构，在限定时间内完成个人信息保护合规审计。

*保护部门：国家网信部门和其他履行个人信息保护职责的部门

做好个人信息保护合规基本工作是完成审计的前提条件

国家对个人信息保护的合规要求并非是因《个人信息保护合规审计管理办法》出台而产生的“新”要求，因此，做好个人信息保护的基本合规要求是顺利完成审计的重要前提。如：

01

梳理个人信息处理活动

- ✓ 收集个人信息的种类、范围、数量和频率、收集目的、流转过程以及公司在个人信息处理过程中的角色
- ✓ 梳理的记录应当依法保存

02

开展个人信息保护影响评估

- ✓ **需要进行评估的情形：**处理敏感个人信息，利用自动化决策处理个人信息，委托处理个人信息或向其他个人信息处理者提供个人信息，公开个人信息，向境外提供个人信息等情况下应当进行个人信息保护影响评估
- ✓ **评估内容：**(a) 个人信息的处理目的、处理方式等是否合法、正当、必要; (b) 对个人权益的影响及安全风险; (c) 所采取的保护措施是否合法、有效并与风险程度相适应

03

落实个人信息出境合规管理

- ✓ **应当进行出境安全评估申报的情形：**向境外提供重要数据；公司是关键信息基础设施运营者；自当年1月1日起累计向境外提供100万人以上个人信息（不含敏感个人信息）或者1万人以上敏感个人信息。
- ✓ **其他出境途径：**个人信息保护认证；按照国家网信部门制定的标准合同与境外接收方签订合同并向所在地省级网信部门备案。

04

完善个人信息保护相关协议文件

- ✓ **个人信息保护政策或隐私协议、个人单独同意条款：** 除法定豁免的情况，企业在收集个人信息前，应通过协议方式获得个人信息主体的同意。
- ✓ **数据出境标准合同：**依据网信办标准合同模版制定并签署。
- ✓ **数据处理协议：**个人信息处理者委托处理个人信息，向其他个人信息处理者提供个人信息或共同处理个人信息的，需约定各方在数据保护方面的权利和义务。

05

建立健全个人信息保护的组织、流程和技术防护措施

- ✓ 建立便捷的个人信息主体权利的申请和受理机制
- ✓ 制定内部管理制度和操作规程
- ✓ 建立个人信息保护组织架构
- ✓ 对个人信息进行分类分级管理，采取加密、去标识化等安全技术措施
- ✓ 合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训
- ✓ 制定并组织实施个人信息安全事件应急预案

个人信息保护合规审计要点

企业在做好个人信息保护基本合规工作的同时，也需结合个人信息保护合规审计管理办法所提示的审查重点准备合规审计工作。

审计重点

个人信息处理活动原则

- 合法性
- 取得同意
- 最小必要
- 多项业务功能的自主选择

个人信息处理规则与告知管理

- 个人信息处理规则/隐私声明
- 告知和同意管理

参与个人信息处理活动的第三方

- 委托处理个人信息
- 共同处理个人信息
- 向第三方提供个人信息
- 公开个人信息
- 在合并、重组、分立、解散和被宣告破产时转移个人信息
- 第三方管理

个人信息处理活动的特殊场景

- 处理敏感个人信息
- 向境外提供个人信息
- 利用自动化决策处理个人信息
- 在公共场所安装图像收集或个人身份识别设备
- 处理公开的个人信息
- 通过移动应用程序处理个人信息

个人信息保护治理模型

- 治理架构与运营模式
- 个人信息处理活动记录
- 个人信息保护合规管理
- 个人信息安全意识和培训

隐私管理政策和程序

- 个人信息分类分级和保护
- 个人信息保护影响评估（PIPIA）
- 个人信息合规风险评估
- 个人信息主体权利响应
- 数据泄露事件响应
- 个人信息留存管理
- 个人信息保护安全工程

个人信息保护的技术措施

- 身份鉴别与访问控制
- 日志和监控
- 数据加密和脱敏
- 备份和恢复
- 入侵防御
- 漏洞管理

对特定情形个人信息处理者*的要求

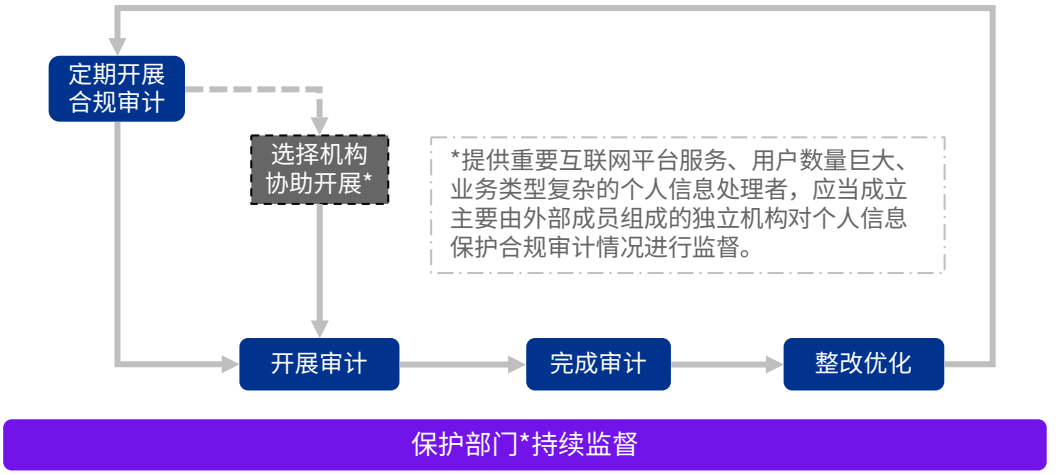
- 平台规则管理
- 社会责任报告管理

*特定情形个人信息处理者：包括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。

个人信息保护合规审计流程概览

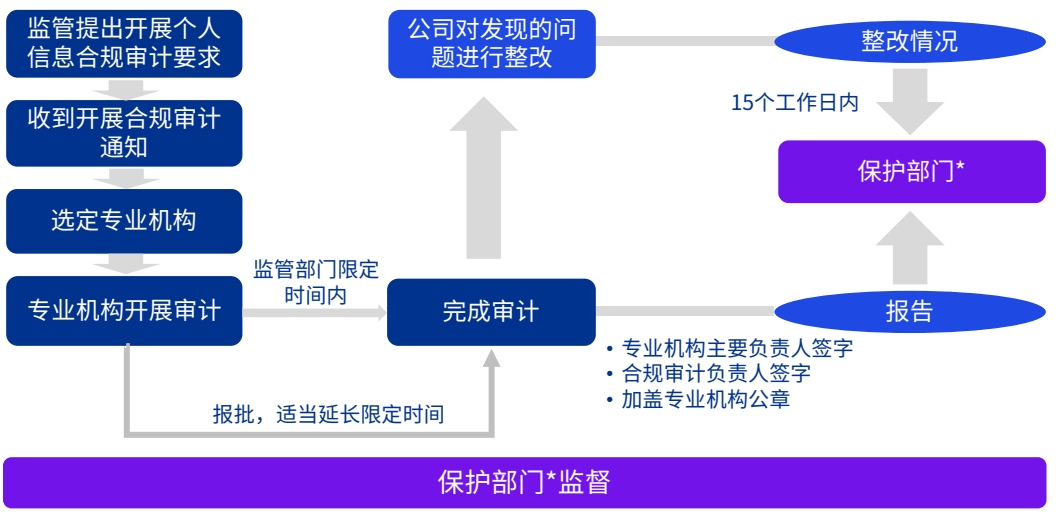
个人信息保护合规自主审计流程

自主审计需要个人信息处理者制定审计相关的内部管理制度和操作规程，设立相应的组织架构，配备人员，并按照个人信息保护法和个人信息保护合规审计参考要点明确审计方法、审计内容、审计流程。



监管强制审计流程

强制监管审计必须由独立第三方专业机构完成，包含**启动检查，开展审计，出具报告，整改落实，成果报送**等阶段。



*保护部门：国家网信部门和其他履行个人信息保护职责的部门

个人信息保护合规审计建议

《个人信息保护合规审计管理办法》为个人信息处理者如何进行合规审计提供了明确的指导。企业应尽早建立个人信息保护合规审计制度，明确合规审计的具体开展流程和负责部门，将审计策略、审计方式、审计问题整改、审计结果跟踪等内容制度化、体系化，以积极应对合规监管，切实提高个人信息管理成熟度，为企业的健康、高速发展保驾护航。

我们建议的个人信息保护合规审计实践路径如下：

个人信息保护合规审计实践路径

01 内部自查

- 企业内部指定个人信息保护负责人，积极开展内部合规审计

02 整改优化

- 根据内部合规审计结果对问题发现进行整改优化

03 外部审计（部分适用）

- 必要时配合第三方专业机构展开审计工作

04 持续改进和定期审计

- 优化内部审计及应审流程
- 定期自行审计

持续风险跟踪、专项审计

- **所有个人信息处理者均应定期开展合规审计（建议至少每三年一次）**
- **处理超过1000万人个人信息的个人信息处理者每两年至少一次全面审计**

企业的实践关注点和建议

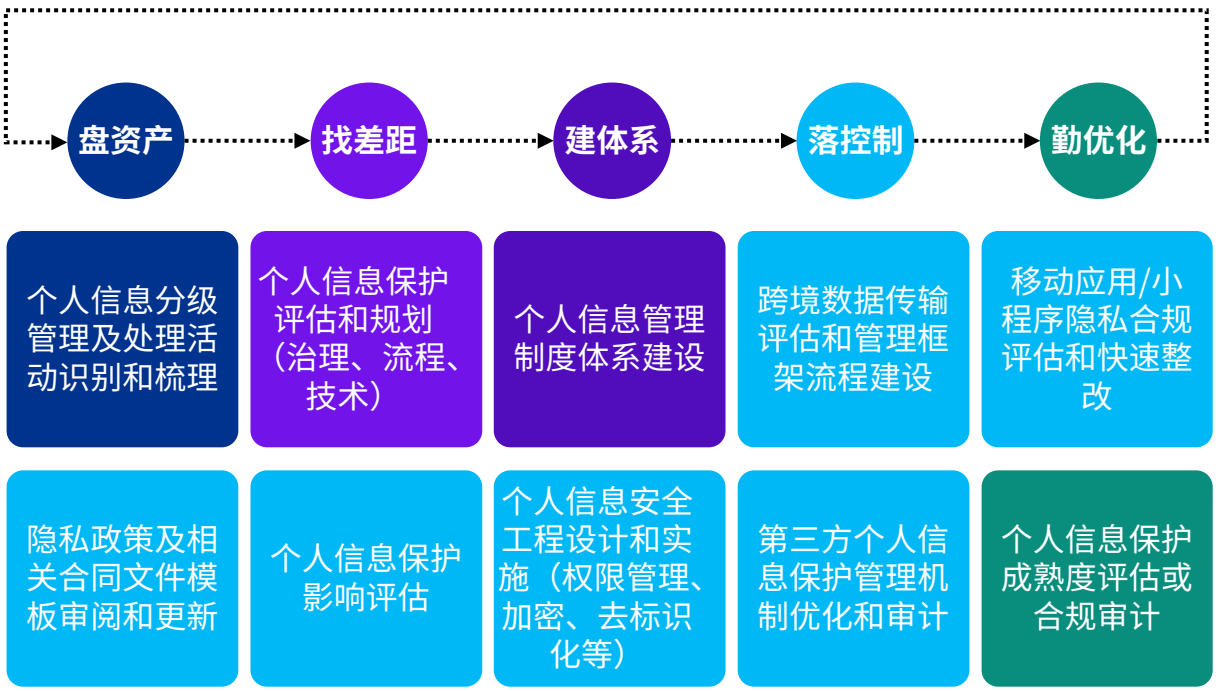
- 建立健全的企业内部个人信息保护合规审计制度，合规审计独立于日常合规管理工作以监督其执行情况和有效性
- 关注行业特定要求，特殊个人信息主体的特定要求，特殊技术、场景的特定要求等，及时履行个人信息保护合规审计义务
- 着眼持续优化和改进，通过定期的合规审计开展自检和管理成熟度评估，以有效规划和提升个人信息保护管理水平

毕马威个人信息保护服务

个人信息保护合规审计服务

外部应审准备	协助企业进行应审准备工作，包括但不限于：协助企业准备应审的文件和材料，配合审计机构进行现场审计工作，协助企业按照整改建议进行整改，以及协助企业准备相关整改情况总结等。
内部审计支持	基于个人信息保护合规审计相关要求，结合企业的业务和技术现状及发展战略，协助企业自行定期开展审计，包括但不限于：制定审计流程和制度，设计审计方案和控制矩阵，协助企业根据监管要求的频率开展个人信息保护合规审计。
个人信息保护优化设计&实施	基于个保法和个人信息保护合规审计相关要求，结合行业标准和最佳实践，协助企业开展个人信息保护管理体系设计，制度流程优化，和技术措施改进工作，协助企业切实保护个人信息和管理相关风险。

个人信息保护服务全景图



联系我们

张令琪
毕马威中国
科技咨询服务
主管合伙人
Tel: +86 (21) 2212 3637
richard.zhang@kpmg.com

郝长伟
毕马威中国
科技咨询技术风险管理服务
主管合伙人
Tel: +86 (10) 8508 5485
danny.hao@kpmg.com

黄芃芃
毕马威中国
科技咨询技术风险管理服务
业务合伙人
Tel: +86 (21) 2212 2355
quin.huang@kpmg.com

周文韬
毕马威中国
科技咨询技术风险管理服务
业务合伙人
Tel: +86 (21) 2212 3149
kevin.wt.zhou@kpmg.com

张倪海
毕马威中国
科技咨询技术风险管理服务
业务合伙人
Tel: +852 2847 5026
brian.cheung@kpmg.com

林海燕
毕马威中国
科技咨询技术风险管理服务
业务合伙人
Tel: +852 2143 8803
lanis.lam@kpmg.com

赫荣科
毕马威中国
科技咨询技术风险管理服务
业务合伙人
Tel: +86 (755) 2547 3398
jason.rk.he@kpmg.com

邬敏华
毕马威中国
科技咨询技术风险管理服务
业务总监
Tel: +86 (21) 2212 3180
fm.wu@kpmg.com

宋智佳
毕马威中国
科技咨询技术风险管理服务
业务总监
Tel: +86 (21) 2212 3306
jason.song@kpmg.com

李振
毕马威中国
科技咨询技术风险管理服务
业务总监
Tel: +86 (10) 8508 5397
jz.li@kpmg.com

kpmg.com/cn/socialmedia

如需获取毕马威中国各办公室信息，请扫描二维码或登陆我们的网站：
https://home.kpmg/cn/zh/home/about/offices.html