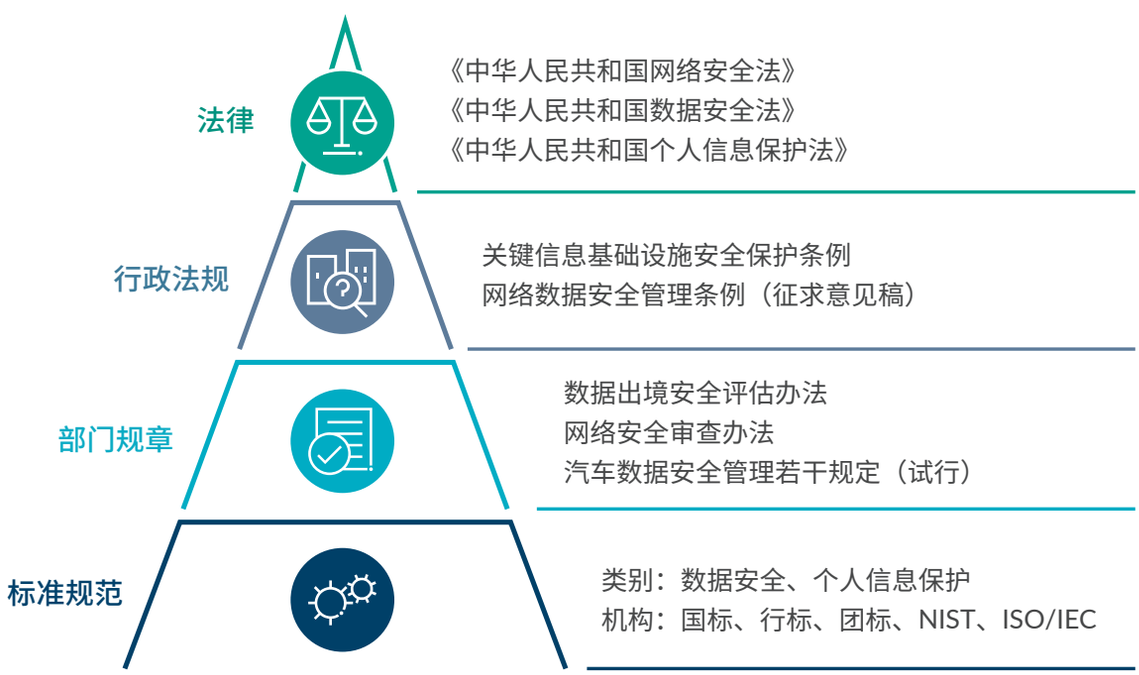
protiviti®
Global Business Consulting
甫瀚

数据安全合规工作开展思路

敏于知

随着我国《网络安全法》、《数据安全法》、《个人信息保护法》、《网络数据安全管理条例（征求意见稿）》、《数据出境安全评估办法》等法律法规的发布与施行，我国数据安全监管框架已基本形成，相关数据安全标准也逐步发布，对法律法规涉及的不同条款进行细化支撑。

图 1：标准对法律、行政法规、规章制度的支撑



随着数据安全监管要求的日益增多和加深，企业要如何达成数据安全合规目标也同时被提上议程。然而面对种种问题，企业常常困惑于应采取怎样的行动和措施才能够达成合规目标。于本文，甫瀚咨询将基于企业困惑，对数据安全合规建设的思路与方法进行阐述。

数据安全标准总览

我们通过下图列举了已发布和在研的相关数据安全国家标准，包括数据安全保护法律法规的要求。这些标准，从总体方向上可分为个人信息保护类与通用数据安全类；从用途上可分为安全要求、实施指南、检测评估类。企业可根据不同场景，使用图中的相关标准对标自身数据安全建设，判断其数据安全合规情况。

图 2：数据安全标准总览

	个人信息保护方向	数据安全方向
安全要求类	***已发布：*** • GB/T 35273-2020 个人信息安全规范 • GB/T 41391-2022 移动互联网应用程序 (APP) 收集个人信息基本要求	***已发布：*** • GB/T 35274-2017 大数据服务安全能力要求 • GB/T 37932-2019 数据交易服务安全要求 • GB/T 39477-2020 政务信息共享 数据安全技术要求 • GB/T 41871-2020 汽车数据处理安全要求 • GB/T 40660-2021 生物特征识别信息保护基本要求 • GB/T 41479-2022 网络数据处理安全要求 • GB/T 42016-2022 网络音视频服务数据安全要求 • GB/T 42017-2022 网络预约汽车服务数据安全要求 • GB/T 41807-2022 声纹识别数据安全要求 • GB/T 42012-2022 即时通信服务数据安全要求 • GB/T 42013-2022 快递物流服务数据安全要求 • GB/T 42014-2022 网上购物服务数据安全要求 • GB/T 42015-2022 网络支付数据安全要求 • GB/T 41773-2022 步态识别数据安全要求 • GB/T 41806-2022 基因识别数据安全要求 • GB/T 41819-2022 人脸识别数据安全要求
	在研： • 个人信息跨境传输认证要求 • 基于个人信息的自动化决策安全要求 • 移动互联网应用程序 (APP) 软件开发工具包 (SDK) 安全要求 • 智能手机预安装应用程序基本安全要求 • 敏感个人信息处理安全要求 • 大型互联网企业内设个人信息保护监督机构要求	***在研：*** • 网络数据分级分类要求 • 重要数据处理安全要求 • 政务数据处理安全要求 • 公共数据开放安全要求
实施指南类	***已发布：*** • GB/T 37964-2019 个人信息去标识化指南 • GB/T 41817-2022 个人信息安全工程指南 • GB/T 41574-2022 公有云中个人信息保护实践指南 • GB/T 42574-2023 个人信息处理中告知和同意的实施指南	***已发布：*** • GB/T 37973-2019 大数据安全管理指南 • GB/T 39725-2020 健康医疗数据安全指南 • GB/T 42447-2023 信息安全技术电信领域数据安全指南
	在研： • 移动互联网应用程序 (APP) SDK 安全指南 • 应用商店的移动互联网应用程序 (APP) 个人信息处理规范性审核与管理指南 • 移动智能终端的移互联网应用规动 (APP) 个人信息处理活动管理指南	***在研：*** • 重要数据识别指南
检测评估类	***已发布：*** • GB/T 39335-2020 个人信息安全影响评估指南 • GB/T 42460-2023 个人信息去标识化效果评估指南	***已发布：*** • GB/T 37988-2019 数据安全能力成熟度模型
	在研： • 移动互联网应用程序 (APP) 个人信息安全测评规范	***在研：*** • 数据安全风险评估方法 • 数据出境安全评估指南 • 数据安全评估机构能力要求

注：标准全称省略信息安全技术

合规难点与诉求

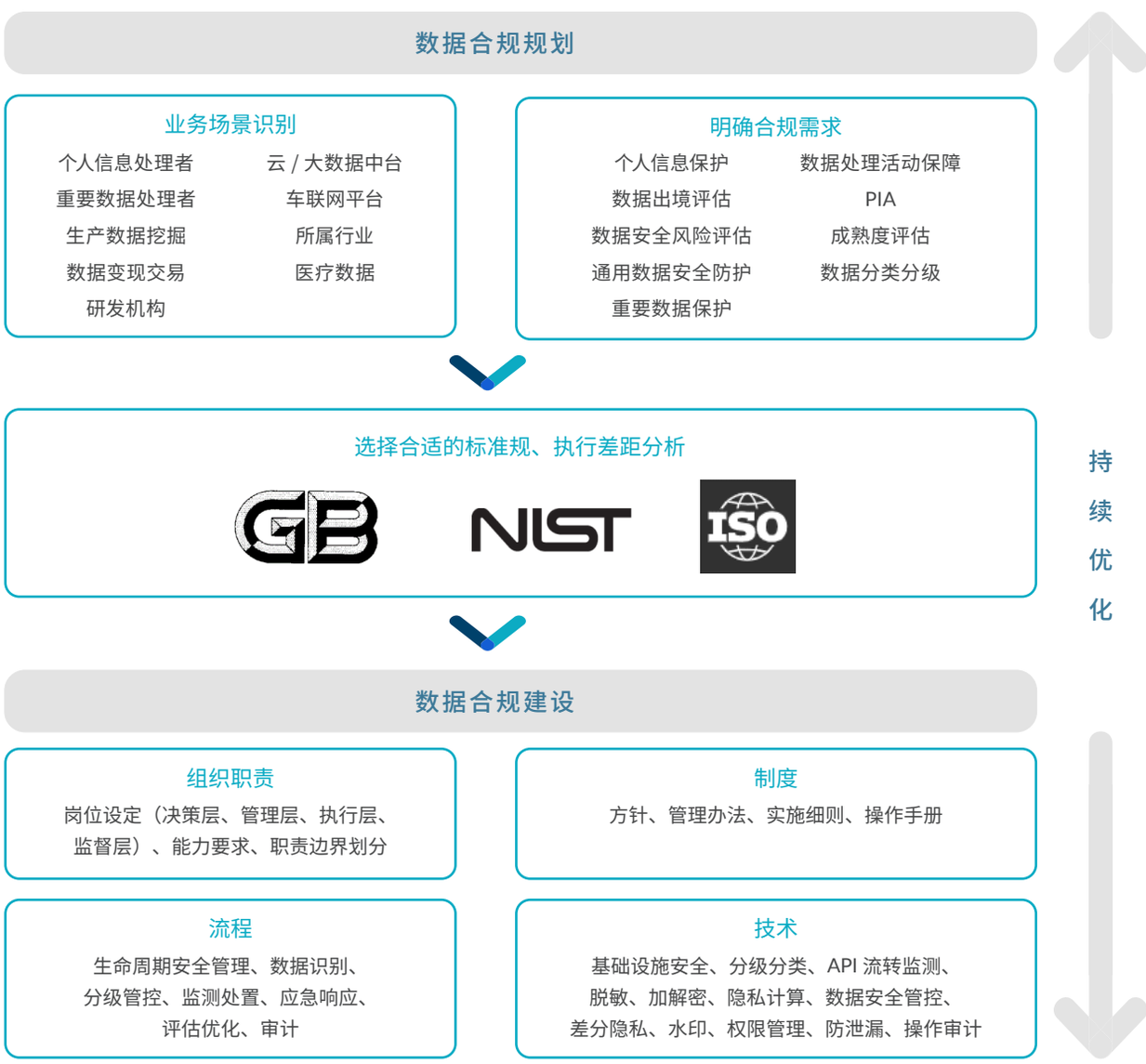
面对不同种类的数据安全标准，企业 IT 与安全团队常常会有如下困惑：

- 有那么多标准，具体哪项适用于企业的业务？
- 企业现有的数据安全成熟度如何，距离相关要求差距多少？
- 企业应采用什么措施以满足标准中的相关条款，从而不会被主管机构处罚？
- 怎样通过一次性建设同时满足企业涉及的多个标准，以避免重复投资？
- 数据安全是由安全团队还是业务部门负责，应该如何推进开展？

数安合规建设思路

甫瀚咨询认为，数据安全合规建设需要遵循体系化建设的原则，通盘设计规划。于下文，我们基于“数据安全合规建设思路”（图 3）对数据合规建设的思路与方法步骤进行进一步阐述。

图 3：数据安全合规建设思路



1. 数据合规规划

- **业务场景识别：**不同的业务场景有不同的建设要点，合规建设的第一步是对目标场景与数据处理者的角色属性进行判断。如其所属具体行业，所处理数据类别是个人信息或重要数据，数据处理场景是数据交易变现、医疗数据、网约车联网平台、生产数据挖掘或研发代码开发平台等；基础设施环境是云平台或大数据中台等。本步骤是后续标准选择及差距分析的基础。

- **明确合规需求：**在业务场景识别完成后，就需要明确其所需的合规目标，如个人信息保护建设、通用数据安全防护、个人隐私影响评估、重要数据保护、数据出境安全评估、成熟度评估、数据安全风险评估、数据处理活动保障及数据分级分类等诉求。

- **选择合适的标准、执行差距分析：**在完成场景梳理并明确合规需求后，企业需要结合其业务属性，按照其所属的监管机构选择合适的标准，如行标、国标、ISO 或是 NIST 标准，依据不同条款在实际数据处理场景中的适用情况进行差距分析，确定出待建设内容。

2. 数据合规建设

建设方需要结合其现状，将目标数安标准相关条款结合并融入到企业组织职责、制度、流程机制、技术等不同方面中。

- **组织与职责：**数据安全与业务耦合度较大，需要内部明确相应的组织与职责才可以系统地推进开展数据安全建设。人员搭建一般需要覆盖决策层、管理层、执行层、监督层，同时需要规定不同人员需承担的职责，以便有相应的人员可以承担数据安全建设工作与任务。

- **制度：**制度可以有效牵引数据安全建设，完善的制度需要至上而下覆盖方针、管理办法、实施细则与操作手册不同层面。方针可以定义组织开展数据安全建设的总体原则；管理办法可定义不同领域数据安全建设方法，对制度形成有效支撑；实施细则可用于指导具体业务场景数安工作开展；操作手册是具体操作层面的指引。几者相辅相成。

- **流程机制：**企业需要完善的流程机制覆盖并保障数据安全。如从采集、传输、存储、使用、删除、销毁等不同生命不同阶段落实数据安全建设；再如对全局资产进行分级分类识别，并根据结果进行分级保护；对数据安全风险进行持续化监测，在数据安全事件发生时，及时启动应急响应机制；建立数据安全风险评估机制，形成相关报告，并采取合适的措施对发现的弱点进行及时缓解；操作动作需要进行留存审计。

- **技术：**数据安全建设在落地过程中需要技术手段进行支撑，以便与管理手段形成有机结合。基础设施侧网络安全是数据安全建设的基础，针对性数据安全需要聚焦所属业务场景，在合适的场景中选择数据资产分级分类、API 接口流转监测、数据脱敏、加解密、隐私计算、数据安全集中管控、差分隐私、水印、权限管理、防泄漏、操作审计等技术工具解决对应的问题。

3. 持续优化

数据安全建设是持续性过程，需要在同步建设、同步运营中发现问题并不断纠正与优化，并迭代到规划中。

相关数据安全参考标准

- GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型
- GB/T 37973-2019 信息安全技术 大数据安全管理指南
- GB/T 37932-2019 信息安全技术 数据交易服务安全要求
- GB/T 35273-2020 信息安全技术 个人信息安全规范
- GB/T 39335-2020 信息安全技术 个人信息安全影响评估指南
- GB/T 41479-2022 信息安全技术 网络数据处理安全要求
- GB/T 41817-2022 信息安全技术 个人信息安全工程指南
- GB/T 41574-2022 信息安全技术 公有云中个人信息保护实践指南
- 信息安全技术 网络数据分级分类要求（在研）
- 信息安全技术 重要数据识别指南（在研）
- 信息安全技术 数据安全风险评估方法（在研）
- 信息安全技术 个人信息跨境传输认证要求（在研）

达于行

甫瀚咨询可提供的服务

甫瀚咨询可以在不同阶段为不同成熟度的用户提供不同类别数据安全合规咨询服务，包括并不限于以下内容：

- **数据处理活动场景梳理：**帮助用户梳理现网业务场景、数据流向、访问交互关系，以便对环境中数据处理活动相关情况完成摸底。
- **基于场景的数据安全合规整改建设咨询：**基于场景与用户所属行业的合规目标进行分析与定义，并针对不同成熟度的用户提供相应整改建议，以便其可以满足主管机构合规要求。
- **数据安全风险评估：**可从不同角度提供评估服务，如个人信息保护影响评估、成熟度评估、数据跨境安全评估、数据安全风险评估、重要数据处理风险评估、APP 个人信息保护测评等，以便度量数据安全现状。
- **数据安全组织建设：**基于组织现状为不同规模公司搭建数据安全团队，设计不同团队职责，协同数据安全工作在组织内的推进与开展。
- **数据安全制度制定：**帮助用户制定相应数据安全方针、管理办法、实施细则、操作手册等，指引数据安全建设落地。
- **数据安全流程优化设计：**制定相关数据安全流程，覆盖不同阶段数据安全需求。
- **数据安全技术工具交付实施：**可针对不同数据安全需求提供技术工具选型、部署、使用、策略优化服务与建议。
- **数据安全培训意识教育：**可针对不同角色能力需求，针对性地进行技能、知识、意识培训。

关于甫瀚咨询

甫瀚咨询是一家全球性的咨询机构，为企业带来领先的专业知识、客观的见解、量身定制的方案和卓越的合作体验，协助企业领导者们充满信心地面对未来。透过甫瀚咨询网络和遍布全球超过25个国家的逾85家分支机构和成员公司，我们为客户提供财务、信息技术、运营、数据、数字化、环境、社会及管治、治理、风险管理以及内部审计领域的咨询解决方案。

甫瀚咨询荣膺2023年《财富》杂志年度最佳雇主百强，我们为超过80%的财富100强及近80%的财富500强企业提供咨询服务，亦与政府机构和成长型中小企业开展合作，其中包括计划上市的企业。甫瀚咨询是Robert Half International Inc. (纽约证券交易所代码: RHI) 的全资子公司。RHI于1948年成立，为标准普尔500指数的成员公司。

联系我们

赵欣
经理
Xin.Zhao@protiviti.com

曹雪峰
经理
Xuefeng.Cao@protiviti.com

金岳阳
高级咨询顾问
Yueyang.Jin@protiviti.com

康妮佳
高级咨询顾问
Ada.Kang@protiviti.com

公司地址

北京
朝阳区建国门外大街 1 号
国贸写字楼 1 座 718 室
电话: (86.10) 8515 1233

上海
徐汇区陕西南路 288 号
环贸广场二期 1915-16 室
电话: (86.21) 5153 6900

深圳
福田区中心四路 1 号
嘉里建设广场 1 座 1404 室
电话: (86.755) 2598 2086

香港
中环 干诺道中 41 号
盈置大厦 9 楼
电话: (852) 2238 0499

protiviti 甫瀚