数据安全法解读系列（二）
《数据安全法》解读

（来源：安永微信公众号，2021-07-21）

一、数据安全的监管环境

（一）立法背景

2021 年 6 月 10 日，第十三届全国人民代表大会常务委员会第二十九次会议通过《中华人民共和国数据安全法》（以下简称“数据安全法”），在经历了三次审议后最终决定于 2021 年 9 月 1 日起施行。

《数据安全法》是数据领域的第一部基础性法律，将与《中华人民共和国网络安全法》和计划颁布的《中华人民共和国个人信息保护法（草案）》共同构建我国的数据和网络安全的法律保护体系，体现了国家对数字化经济发展的决心。

（二）金融行业数据安全现状

金融行业内部系统错综复杂，设备类型多样，数据具有多元复杂、高价值、高敏感、数据类型和保护等级定义不清、流转过程复杂等特性，也因此，金融行业的数据安全将成为国家和多头监管机构（人民银行、银保监、证监会、公安部等）的重点管控领域。

数据安全相关的法律、国家标准和行业标准的体系建立与完善，将指导金融机构建立企业内部数据安全体系，规范管控和技术标准，明确数据全生命周期安全要求，以解决数据安全治理、管理、技术、基础支撑各层次的历史难题。

重要法规及标准发布时间一览		
2016/11/7	**《中华人民共和国网络安全法》**	**人大常委**
2018/5/21	《银行业金融机构数据治理指引》	银保监
2019/5/28	《数据安全管理办法（征求意见稿）》	网信办
2019/4/10	《互联网个人信息安全保护指南》	公安部
2019/6/13	《个人信息出境安全评估办法(征求意见稿)》	网信办
2019/8/30	《信息安全技术 数据安全能力成熟度模型》	信安标委
2019/8/30	《信息安全技术 大数据安全管理指南》	信安标委
2020/2/13	**《个人金融信息保护技术规范》**	**金标委**
2020/3/6	《信息安全技术 个人信息安全规范》	信安标委
2020/9/23	**《金融数据安全 数据安全分级指南》**	**金标委**
2021/4/8	**《金融数据安全数据生命周期安全规范》**	**金标委**
2021/4/26	**《个人信息保护法(草案）》二审**	**人大常委**
2021/6/10	**《中华人民共和国数据安全法》**	**人大常委**

二、金融机构面临的挑战

（一）数据泄漏难以溯源——金融机构需持续完善数据安全管控精细度和技术应用

金融行业具有业务主体多样、信息系统繁多、数据形式复杂、价值定义困难等特点，进而导致数据资产盘点难度较大，数据泄露途径复杂，数据保护难度较高。

近年来源于金融机构内部数据安全管控不足而发生的数据安全事件在社会产生不良影响和舆论，如未经授权查询与贩卖个人信息、未经授权的个人财务信息披露等，严重危害金融机构的声誉。《数据安全法》中已明确要求企业应加强数据全生命周期的安全建设，所以，如何有效加强全生命周期的安全管控，明确数据收集、存储、使用、加工、传输、提供、公开、销毁等各个阶段的安全要求，以保证数据安全管控体系的持续优化，是金融机构在当前必须面对的一项重要挑战。

同时，源于系统及技术漏洞、外部攻击及威胁的数据安全事件也频频发生，如服务器或云环境下的错误配置引发的数据泄露、利用人工智能新兴技术的漏洞而产生的数据泄漏、瞄准个人财务帐号的移动银行木马等等，批量的数据泄漏或丢失，将对数据的可用性、机密性与完整性造成极大危害，严重影响金融行业的业务运营。

因此，金融机构迫切需要发现自身安全防护的薄弱点，平衡安全的整体投入资源，切中要点的提升纵深安全防御技术能力，**量身定制符合自身业务体量的、健壮的数据安防技术体系及架构**，从而高效且精准的应用加密、脱敏、防泄漏、追踪溯源等数据安全技术。

（二）安全评估及技术检测流于表面——金融机构需提升安全风险检测能力

对 IT 环境的定期安全评估和技术测试虽已成为科技及安全部门的一项重要工作，**但执行方式多陷于被动的、以合规为导向的“头病医头，脚病医脚”困境**，无法深入分析且解决技术检测结果背后的根本原因，所以导致评估工作范围大、负担重、投入资源多，但却重复性较高，效果不足。《数据安全法》中已明确要求企业应对数据安全风险进行评估，那么基于法律强制要求的背景下，金融机构需重新审视安全评估工作的执行效果及效率问题，考虑如何有效发现数据安全漏洞和管控薄弱点，如何分析并解决根源痛点而不是流于表面。

（三）数据安全能力建设和文化熏陶——金融机构需建立数据安全培养机制

完善的数据安全管控策略和健壮的数据安防技术，如果不能被科技部门、数据管理部门、数据使用部门等相关方深入理解，则无法被有效执行和应用到工作当中，这将产生安全资源投入充足，但无法达

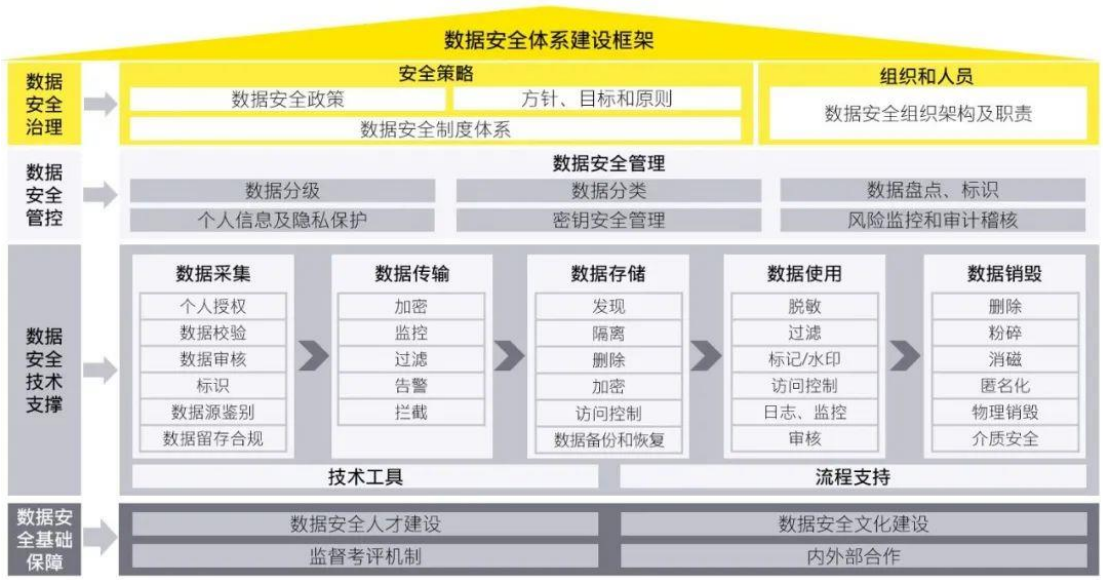
到预期效果的困境。

然而，目前大多金融机构的数据安全文化、培训及能力培养并不充足：高层对数据安全的重视程度仍需提升，专业人员的数据安全能力培养机制尚未完善，全员的数据安全文化氛围尚未成型。《数据安全法》中已明确要求企业应组织开展数据安全教育培训且增强数据安全专业能力。

那么，如何**针对不同受众，设计多场景、多层次的安全宣贯、培训及能力培养计划**，开展既包括管理策略又涉及技术手段的数据安全培训，提升人员的素质能力和安全意识，当成为数据安全工作开展的重要支撑。

三、安永助力赋能

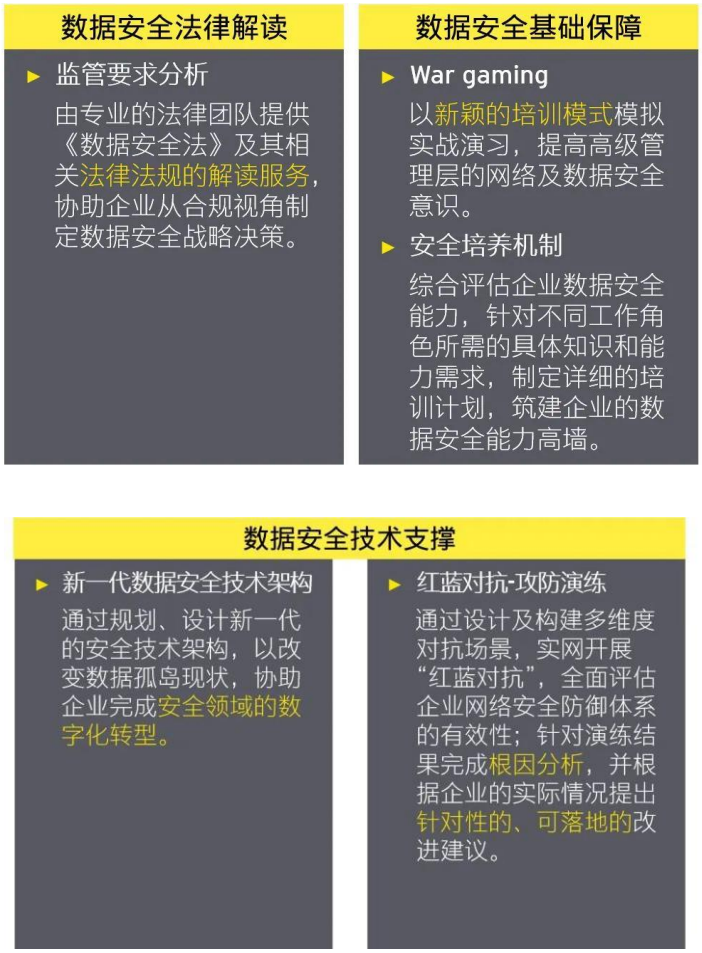
安永数据安全体系框架



安永数据安全服务

在大数据涌入的今日，数据已成为企业的基础和战略资源，而安全是其业务健康且持续发展的基础。为协助金融机构解决数据安全体系的治理、管理、技术及基础保障等合规和实践难题，安永将为客户

提供**数据安全解决方案**：



原文链接：https://mp.weixin.qq.com/s/yGiGkswxBgL4nWOoVNmmdg ，转载请注明。