

中电金信

金融数据安全治理白皮书



CONTENTS
目 录

1	第一章 金融数据安全治理的含义是什么？	
1.1.	金融数据安全治理的定义	03
1.2.	金融数据安全治理的重要性	03
1.3.	金融数据安全治理发展历程	04
2	第二章 我国金融数据安全法规与监管要求有哪些？	
2.1.	国内数据安全法律法规概览	05
2.2.	金融行业数据安全监管要求	06
2.3.	监管框架下的数据安全治理挑战	08
3	第三章 如何制定并执行金融数据安全治理方案？	
3.1.	金融数据安全治理参考框架	09
3.2.	中电金信数据安全治理框架	10
3.3.	数据安全管理体系	11
3.4.	数据安全技术体系	12
3.5.	数据分类分级	19
3.6.	个人信息保护	21
3.7.	数据安全运营体系	22
3.8.	数据安全监督评价体系	30
3.9.	金融数据安全治理的实施路径	32
4	第四章 如何建立金融数据安全治理的组织保障体系？	
4.1.	明确数据安全治理组织设置原则	36
4.2.	数据安全治理的组织架构设计	37
4.3.	落实数据安全责任与问责机制	38
4.4.	数据安全文化培养	38

CONTENTS 目录

5	第五章 数据安全治理产品应具备哪些功能？	
5.1.	数据安全治理产品概述	39
5.2.	数据安全治理产品典型应用场景	42
5.3.	中电金信数据安全治理产品特色	45
6	第六章 金融数据安全治理有哪些优秀案例？	
6.1.	金融行业内数据安全治理案例	48
6.2.	我们从案例中总结的经验与不足	51
7	第七章 金融数据安全治理未来有哪些发展趋势？	
7.1.	技术创新持续引领安全治理革新	54
7.2.	新技术带来新兴的数据安全威胁	55
7.3.	数据伦理和隐私保护更为重要	56
7.4.	跨境数据流动的安全与合规管理	57
8	第八章 中电金信怎样保障您的数据安全？	
8.1.	中电金信简介	57
8.2.	中电金信金融数据安全治理解决方案优势	58
8.3.	中电金信对于数据安全治理的长期承诺	59
8.4.	中电金信对金融行业数据安全的持续投入与创新	60

序言

金融行业作为数据密集型行业，对数据的依赖日益加深，但数据价值的提升也带来了严峻的数据安全挑战。面对频繁的网络攻击、数据泄露事件以及日益严格的监管法规，金融机构在追求数据价值创造的同时，愈加重视数据安全问题，并积极加大在此领域的投入。

金融数据安全治理不仅关乎客户隐私保护和金融资产安全，还关系到整个金融系统的稳定与发展。因此，金融机构迫切需要全面构建数据安全治理体系，以提升整体防护能力。本白皮书将深入探讨金融数据安全治理的框架和重点内容，分析面临的挑战和未来趋势，旨在为金融机构的数据安全管理提供策略和思路参考。

核心观点

数据安全治理是金融行业数字化转型的保障基石

在金融行业的数字化转型过程中,数据驱动了业务创新、风险管理和决策。数据安全通过各环节的严格措施,确保数据的完整性、可用性和隐私性。数据安全治理则通过系统化的管理,确保这些安全措施得到有效执行,从而支持数字化转型的顺利进行。同时,态势感知和安全运营平台等平台化产品在这一过程中发挥了关键作用。这些平台通过整合各种安全工具和流程,提高了对复杂数字环境中安全事件的处理效率,进一步增强了数据安全治理的能力。

金融行业数据安全治理已经进入深水区

金融行业数据安全治理重点已经从运维层面转向生产环境的安全管理。在生产环境中,金融机构处理大量客户信息和业务应用数据,面临更为严峻的安全风险。因此,当前更注重实时监控、快速响应和动态保护,以确保数据在处理过程中的安全和稳定。

金融行业应在数据全生命周期中实现“数据安全左移”

金融行业应将数据安全要求融入到业务系统开发全流程,系统应满足安全标准。包括在设计、编码、测试、部署和运维各阶段严格实施安全措施,如数据加密、访问控制和数据脱敏等。同时,对开发人员进行安全培训,推广安全编码的规范和最佳实践。