

FINANCIAL INSTITUTION PQC MIGRATION RECOMMENDATIONS

金融机构后量子密码迁移 实施建议

基于 FINMA Guidance 05/2026 的
跨辖区治理与技术路线参考

龚晖 | UCL Institute of Finance & Technology

适用对象：银行、保险、证券、基金、资产管理机构、金融市场基础设施及金融科技服务机构

用途：董事会决策、风险评估、技术选型、迁移计划、试点验收与审计取证

发布基准：2026 年 10 月 1 日 版本：1.4

独立研究 | 中文版公开稿

执行摘要

一页结论

量子风险尚未转化为大规模现实攻击，但金融机构的迁移窗口已经开启。原因并不依赖对“量子计算机何时成熟”的单点预测：需要长期保密的数据正在持续产生，复杂系统升级通常需要数年，外部供应商的产品周期又不完全由金融机构控制。瑞士金融市场监管局（Swiss Financial Market Supervisory Authority, **FINMA**）第 05/2026 号通告将这一问题纳入操作风险和韧性治理；其控制逻辑也可供其他司法辖区参考。

依据 FINMA 第 05/2026 号通告强调的治理方向，本报告建议金融机构在启动后 12 个月内形成经管理层批准的战略与路线图，完成高风险范围的**密码物料清单（Cryptographic Bill of Materials, CBOM）**和关键供应商基线，并启动至少一个**传统密码与后量子密码并行的混合迁移试点**；随后参考 36 至 60 个月的时间框架，按风险波次推进关键流程迁移。上述时间为本报告提出的参考排期，并非 FINMA 统一规定的完成期限。长期目标是建立可持续的**密码敏捷能力**：能够识别、替换、验证和证明密码控制始终有效。

为什么要做

金融机构依赖**Rivest–Shamir–Adleman (RSA)** 公钥算法、**椭圆曲线密码 (Elliptic Curve Cryptography, ECC)** 等机制，保护身份认证、密钥交换、数字签名、软件更新、机构间通信和长期档案。未来，具备现实密码分析能力的量子计算机（**Cryptographically Relevant Quantum Computer, CRQC**）可能使这些公钥机制失去预期安全性。长期敏感数据还面临“**先收集、后解密（Harvest Now, Decrypt Later, HNDL）**”风险：今天被复制的密文，可能在未来被解密。

因此，**后量子密码（Post-Quantum Cryptography, PQC）** 迁移既是安全升级，也涉及业务连续性、客户信任和第三方治理。项目还能立即改善证书管理、密钥治理、技术债识别、供应商透明度和算法撤回速度。

为什么现在做

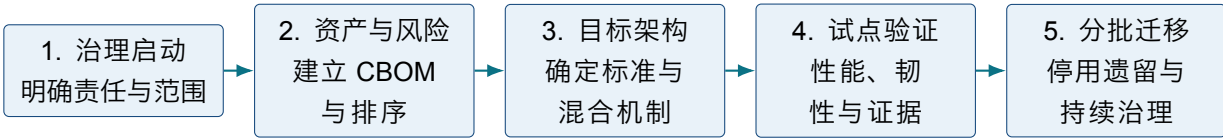
当前事实	对经营与治理的影响	现在可以完成的工作
长期敏感数据已在产生	迁移完成前已被复制的数据，后续升级无法消除其既有暴露	识别数据寿命、传输路径和优先保护对象
大型机构迁移通常需要多年	应用、证书、硬件安全模块、外部接口和供应商版本相互依赖	建立资产清单、依赖图和分阶段迁移波次
首批正式标准已经发布	技术工作已可从研究转入受控试点	验证标准算法与现有协议的兼容性
新系统仍可能增加传统算法依赖	每一次不具备密码敏捷的新采购都会扩大未来改造成本	将 PQC 准备度写入架构、采购和外包要求
监管关注已从观察转向治理	董事会和高级管理层需要证明风险已被识别、排序和持续监督	批准路线图、风险偏好、资源和例外机制

及早行动带来的经营选择权

资产透明：知道哪些数据、系统和供应商真正需要优先处理；**投资可控：**把多年改造拆分为可审批、可验收的波次；**供应链主动：**在续约和采购窗口提出版本、互操作和退出要求；**业务连续：**通过并行验证、受控切换和安全回退降低集中变更风险；**证据完整：**能够向董事会、客户、审计和监管说明风险状态与处置进度。

应当怎样做

建议按以下五个相互衔接的步骤组织实施：



- 1. 治理启动。**董事会或相应最高治理机构批准风险偏好、目标日期和资源；信息安全负责人牵头，业务、技术、数据、采购、法务、风险和审计共同参与。
- 2. 资产与风险。**先建立**CBOM**，再把算法、证书、密钥、数据、业务流程、系统和供应商连接起来。没有这一步，机构无法确定迁移范围，也无法对预算和优先级作出可信判断。
- 3. 目标架构。**针对密钥建立、签名、静态数据和软件供应链分别设计迁移机制。短中期可在适当场景采用**混合机制**；所有新设计应支持**算法可替换、版本可观察、策略可控制**。
- 4. 试点验证。**同时验证功能、性能、互操作、异常处置和业务连续性，并保存可复核证据。
- 5. 分批迁移。**生产迁移按波次发布；旧算法在依赖解除、数据处置、业务签署和观察期完成后正式停用。迁移后的资产更新、算法版本、供应商支持和定期复测纳入常态运营，保持持续升级能力。

参考时间框架

FINMA 建议受其监管的机构最迟在 **2027** 年年中形成路线图。其他司法辖区可把这一日期视为有参考价值的治理标杆，而非自动适用的法定期限。每家机构应根据数据寿命、系统复杂度、供应链约束和所在地监管要求重新校准。

阶段	建议时间	应形成的结果
启动与定界	0-90 天	治理架构、项目章程、适用范围、初始供应商问卷、长期敏感数据清单、试点候选
路线图与基线	3-12 个月	管理层批准的路线图、高风险 CBOM、风险排序、目标架构、预算和采购要求
试点与关键迁移	12-36 个月	混合传输层安全协议（Transport Layer Security, TLS ）或签名试点、关键流程迁移、互操作与容量证据、供应商版本计划
规模化与收尾	36-60 个月	遗留系统处置、弱算法停用、例外关闭、持续监测和常态化报告

目录

执行摘要

1	FINMA 监管通告与跨辖区适用框架	1
1.1	FINMA Guidance 05/2026 的监管要点	1
1.2	监管控制目标的跨辖区适用性	1
1.3	建议的使用者与职责	2
1.4	从监管语言到实施主线	2
1.5	量子风险的时间判断	3
1.6	范围边界与本地化原则	3
2	量子计算如何改变现有密码安全假设	4
2.1	先理解金融系统今天依赖什么	4
2.2	量子算法必须运行在物理设备上吗	4
2.3	Shor 算法：公钥密码的结构性威胁	4
2.4	Grover 算法：对称密码的平方根加速	5
2.5	Shor 与 Grover 的关系及区别	5
2.6	从算法威胁到业务风险	6
2.7	HNDL 与迁移窗口	7
2.8	威胁模型的边界	7
3	后量子密码标准及其数学基础	8
3.1	首批标准化方案的选择依据	8
3.2	格及模格结构	8
3.3	带误差学习与计算困难性	9
3.4	ML-KEM：模格密钥封装机制	9
3.4.1	选择明文与选择密文安全模型	9
3.5	ML-DSA：模格数字签名机制	9
3.6	SLH-DSA：无状态哈希签名机制	10
3.7	传统与后量子密码的混合构造	10
3.8	算法选型与实施约束	10
4	端到端迁移机制与目标架构	11
4.1	迁移生命周期与完整性要求	11
4.2	分层目标架构	11
4.3	传输层协议、API 与机构间通信	12
4.4	数字签名、证书与长期证据	12
4.5	静态数据保护与密钥再封装	12
4.6	身份体系、软件供应链与设备信任	13
4.7	第三方、云与金融市场基础设施	13
4.8	共存、切换与安全回退	13
4.9	密码策略服务与运行可观察性	14
4.10	生产迁移完成判定	14
5	密码资产清单与风险排序	15
5.1	密码资产清单的基础作用	15

5.2	CBOM 的最低字段	15
5.3	发现方法：自动化与人工核实结合	16
5.4	依赖图：从“算法在哪”到“变更会影响谁”	16
5.5	风险评分模型	16
5.6	HNDL 优先队列	17
5.7	可复核的排序流程	18
5.8	清单质量与持续更新	18
6	金融机构后量子密码迁移参考路线图	19
6.1	路线图模型与适用条件	19
6.2	启动阶段：前 90 天	19
6.3	阶段一：治理、基线与路线图（3–12 个月）	19
6.4	阶段二：试点与共性能力（6–18 个月）	20
6.5	阶段三：高风险流程迁移（12–36 个月）	20
6.6	阶段四：规模化、长尾与停用（24–60 个月）	20
6.7	参考时间线	20
6.8	资源与预算口径	20
6.9	跨辖区适用性与本地化核查	21
6.9.1	国际参考时间表与机构排期校准	21
6.10	路线图年度复核	21
7	试点验证、抗扰动与生产验收	22
7.1	试点必须回答的四个问题	22
7.2	试点一：混合 TLS/API	22
7.3	试点二：文件交换或数字签名	22
7.3.1	金融市场基础设施参考案例：Project Leap	22
7.4	抗扰动验证框架	23
7.5	安全回退与失败关闭	23
7.6	实现安全与侧信道	23
7.7	性能与容量模型	24
7.8	生产准入门槛	24
7.9	证据包与观察期	24
8	治理、供应链与持续保证	25
8.1	治理结构	25
8.2	董事会与高级管理层应看到什么	25
8.3	供应商治理与合同要求	26
8.4	例外管理	26
8.5	关键指标	26
8.6	三道防线与独立保证	27
8.7	证据架构	27
8.8	能力成熟度	28
8.9	持续更新与公开沟通	28
8.10	持续密码治理与运营机制	28
A	术语与缩写索引	30
B	数学附录：从传统密码到 PQC	32
B.1	RSA 正确性与 Shor 算法的切入点	32

B.2	Grover 振幅放大的简化推导	32
B.3	LWE 解密正确性的直观推导	32
B.4	KEM 安全: IND-CPA 与 IND-CCA	33
B.5	签名正确性、不可伪造与拒绝采样	33
B.6	混合密钥组合的安全条件	33
C	启动与供应商问卷	34
C.1	内部启动问卷	34
C.2	供应商问卷	34
D	CBOM 字段模板	35
E	实施与验收检查清单	36
E.1	路线图批准前	36
E.2	试点进入生产前	36
E.3	标记“完成迁移”前	36
F	标准与监管资料快照	37
	参考文献	38

FINMA 监管通告与跨辖区适用框架

1.1 FINMA Guidance 05/2026 的监管要点

FINMA 于 2026 年 7 月发布 [Guidance 05/2026：量子计算带来的网络风险](#)。通告并未要求立即完成全量技术替换，也没有对量子计算机成熟日期作确定预测。其监管含义是：金融机构已经拥有足够信息启动治理，不应把时间不确定性作为缺少路线图、资产基线和管理责任的理由。

通告依据 2025 年 11 月至 2026 年 1 月对 60 家瑞士金融机构的调查，覆盖银行、保险、集体资产管理机构和金融市场基础设施。调查显示，**72%** 尚未规划或实施量子安全措施，仅 **8%** 已有具体路线图；已有路线图的机构通常预计关键数据和流程迁移需要 4 至 5 年。另有 76% 认为密码资产清单价值较高、73% 重视密码敏捷、60% 已与供应商联系或计划联系。FINMA 建议受其监管的机构最迟于 **2027 年年中** 形成路线图，并分别设定关键业务流程和完整迁移的目标日期 [1]。

FINMA 所述 2027 年年中是路线图与治理准备的时间节点。路线图需明确责任、优先数据与流程、密码资产、目标架构、供应商安排、资源、验收方式和例外审批；关键流程及全量迁移日期应另行确定。

1.2 监管控制目标的跨辖区适用性

FINMA 通告适用瑞士监管范围，但其核心问题不具有地域特异性。任何数字化金融机构都依赖公钥基础设施、跨机构接口、第三方软件、云服务、长期数据和电子签名；也都需要管理技术替换中的业务连续性。由此可以提炼出五项全球通用的控制目标：

表 1.1: FINMA 要求与全球通用控制目标

FINMA 关注域	通用控制目标	可验证成果
战略与路线图	批准优先级、目标日期、资源和例外机制	决议、风险偏好、路线图和预算
风险分析与清单	定位密码依赖及其业务、数据和供应商关系	CBOM、依赖图、数据寿命及责任人确认
关键数据保护	优先处理长期敏感数据及长期有效签名	HNDL 清单、重加密/重签名、留存规则
密码敏捷	在受控条件下替换算法并观察实际版本	抽象接口、策略服务、自动测试和停用机制
外部服务商	保持对外包密码风险和退出安排的责任	合同条款、供应商路线、审计权和退出方案

这些目标与各地常见的操作风险、技术风险、数据安全、外包管理和业务连续性要求相容。金融机构参考本建议时，应结合所在地法律、密码管理制度、金融监管规则、数据跨境要求和行业标

准。例如，中国境内机构需考虑《密码法》及商用密码、金融数据安全等要求；瑞士受监管机构需对照 FINMA 相关监督要求。控制目标具有共通性，法律依据、算法与产品要求、验收流程和目标日期需本地化。

英国国家网络安全中心（National Cyber Security Centre，**NCSC**）的迁移指导同样将资产评估、密码敏捷、供应商依赖和业务连续性纳入实施安排 [2]。本报告据此把首次迁移与持续治理相衔接；不同来源的时间表及适用范围在第6章分别说明。

1.3 建议的使用者与职责

建议由以下职能共同使用，并由高级管理层指定具有预算和跨部门协调权的负责人：

表 1.2: 主要使用者及其决策问题

使用者	需要作出的决定	主要使用章节
董事会与风险委员会	批准风险偏好、资源、目标日期和重大例外	第 1、6、8 章
高级管理层与安全技术负责人	确定责任、范围、架构及供应商策略	第 1、4、6、8 章
业务与数据负责人	确定优先数据、业务影响和切换条件	第 2、5、7 章
架构、开发与运维	发现依赖、设计机制、测试和发布	第 3、4、5、7 章
采购、法务与第三方风险	落实合同、版本、证据和退出要求	第 6、8 章
内部审计与合规	复核决策、测试、例外和迁移状态	第 7、8 章及附录

1.4 从监管语言到实施主线

实施顺序必须体现依赖关系：先有治理范围，才能定义需要发现的资产；先有资产与数据寿命，才能进行风险排序；先完成目标架构和供应商确认，才适合进入试点；试点通过后，才能按波次进入生产并逐步停用旧机制。

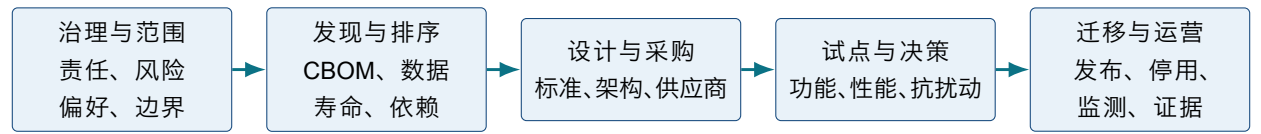


图 1.1: 本建议采用的端到端实施主线

图中箭头表示进入下一阶段所需的最低输入，而不是所有工作必须串行。例如，供应商调查可与资产发现并行，算法测试可在路线图审批前预研；但没有确认资产责任人和业务影响，就不应把试验结果直接推广到生产。

1.5 量子风险的时间判断

机构不需要精确预测量子计算机成熟年份，仍可进行可审计的时间判断。令

$$T_D = \text{数据仍需保密或签名仍需可信的剩余时间}, \quad (1.1)$$

$$T_M = \text{完成发现、设计、采购、测试和迁移所需时间}, \quad (1.2)$$

$$T_Q = \text{能够威胁现有公钥密码的量子能力出现前的时间}. \quad (1.3)$$

当

$$T_D + T_M > T_Q \quad (1.4)$$

时，现有保护周期与迁移周期已超过潜在安全窗口。这一表达常被称为 Mosca 不等式 [18]。其中 T_Q 最不确定，但 T_D 和 T_M 可以通过数据分类、合同期限、系统复杂度和历史改造经验估算。治理重点因此应放在可测量的两个变量上，并对 T_Q 采用情景分析，而不是等待单一预测成为事实。

1.6 范围边界与本地化原则

本建议涉及传输加密、密钥建立、数字签名、身份认证、软件与固件签名、证书体系、静态数据密钥封装、分布式账本和第三方服务。量子密钥分发 (QKD)、量子计算业务应用和一般网络安全控制可作为相邻课题管理，其技术与部署机制不同于 PQC 迁移。

金融机构可形成一份“所在地适用性说明”，至少记录：适用法律与监管、允许使用的算法与产品、数据所在地要求、关键基础设施身份、外包审批、审计留存期、事件报告义务，以及与所在地现行密码体系的兼容策略。实施以所在地强制性规则和正式审批为准。

量子计算如何改变现有密码安全假设

2.1 先理解金融系统今天依赖什么

金融系统中的密码控制承担四类基本任务：机密性保证未经授权者不能读取信息；完整性保证内容未被篡改；真实性确认通信方或签名者身份；不可否认性为交易、合同和软件发布提供可验证证据。

对称密码使用同一秘密密钥加密和解密，例如 AES；公钥密码使用一对相关但不同的密钥，其中公钥可以公开，私钥必须保密。现代金融协议通常把两者结合：先用公钥机制建立会话密钥或验证签名，再用速度更快的对称密码保护大量数据。因而，量子风险首先冲击的不是整个系统的每一个加密步骤，而是密钥建立、数字签名和身份信任所依赖的公钥层。

2.2 量子算法必须运行在物理设备上吗

必须。量子算法是数学步骤，真正获得量子加速需要在量子处理器上执行。现有经典计算机可以模拟小规模量子线路，用于教学、调试和算法验证，但模拟成本会随量子比特数快速增长，不能替代大规模量子硬件。

物理量子比特容易受到噪声、退相干和控制误差影响。要长时间稳定执行复杂算法，通常需要量子纠错：用大量物理量子比特编码少量可靠的逻辑量子比特。因此，判断密码威胁不能只看厂商公布的物理量子比特数量，还要看逻辑量子比特、逻辑错误率、门深度、纠错开销和完整运行时间。

具备现实密码分析能力的量子计算机 (Cryptographically Relevant Quantum Computer, CRQC)，是指能够在可接受时间和成本内对现实使用的密码参数实施有效攻击的容错量子系统。它不是某一固定型号，也不能简单等同于“超过某个物理量子比特数量”。截至本报告发布日，尚不存在公开证实可破解现实 RSA-2048 或主流 ECC 参数的 CRQC。

2.3 Shor 算法：公钥密码的结构性威胁

Shor 算法是 Peter Shor 于 1994 年提出的量子算法。它把整数分解和离散对数问题转化为周期/阶寻找问题，并利用量子傅里叶变换高效提取周期 [13]。RSA 的安全性依赖大整数分解困难；有限域上的 Diffie–Hellman 密钥交换 (DH) 和数字签名算法 (Digital Signature Algorithm, DSA) 依赖离散对数困难；椭圆曲线上的椭圆曲线 Diffie–Hellman 密钥交换 (Elliptic Curve Diffie–Hellman, ECDH) 和椭圆曲线数字签名算法 (Elliptic Curve Digital Signature Algorithm, ECDSA) 依赖椭圆曲线离散对数困难。足够大且可靠的量子计算机运行 Shor 算法后，这些经典困难问题可在多项式时间内求解。

对 RSA，公开模数为 $N = pq$ 。若能找到随机 a 在模 N 乘法群中的阶 r ，即

$$a^r \equiv 1 \pmod{N}, \quad (2.1)$$

且 r 为偶数、 $a^{r/2} \not\equiv -1 \pmod{N}$ ，则

$$\gcd(a^{r/2} - 1, N) \quad \text{和} \quad \gcd(a^{r/2} + 1, N) \quad (2.2)$$

通常可给出 N 的非平凡因子。量子部分负责高效寻找 r ，经典部分完成最大公因数计算。附录B给出更完整推导。

Shor 算法的业务含义不是“量子计算会让所有加密失效”，而是：

- 基于 RSA 的密钥交换、加密和数字签名将失去其数学安全基础；
- 基于有限域离散对数的 DH/DSA 以及基于椭圆曲线离散对数的 ECDH/ECDSA 同样受到结构性影响；
- 单纯增加 RSA 或 ECC 密钥长度不能从根本上解决问题，因为算法复杂度类别已经改变；
- 只有具备足够逻辑量子比特和纠错能力的物理设备，才能对现实参数执行该攻击。

2.4 Grover 算法：对称密码的平方根加速

Grover 算法是 Lov Grover 于 1996 年提出的量子搜索算法。它不利用 RSA 那样的代数结构，而是对候选答案提供一个可判定“是否命中”的量子查询过程。算法先制备候选项的均匀叠加，再交替执行目标相位翻转和关于平均振幅的反射；两步合称一次 Grover 迭代，使目标态的测量概率逐次增加。对一个包含 N 个候选项、只有一个目标的无结构搜索问题，经典穷举平均需要 $O(N)$ 次查询，理想量子条件下约需

$$O(\sqrt{N}) \quad (2.3)$$

次查询 [14]。若目标有 M 个，所需迭代约为 $(\pi/4)\sqrt{N/M}$ ；附录B给出振幅放大的二维几何推导。查询次数并不等于总计算量：每次查询还需可逆地实现一次完整的候选验证，包括密钥调度、加密或哈希计算和错误纠正。

对于 k 位对称密钥，搜索空间 $N = 2^k$ ，理想查询复杂度由 $O(2^k)$ 降为 $O(2^{k/2})$ ：例如 128 位与 256 位密钥分别对应约 2^{64} 和 2^{128} 次理想查询。这不是对 AES 结构的“完全破解”，也不能把哈希原像、碰撞和签名安全问题混为一谈。实际成本还受量子门数、长期串行深度、纠错开销和并行化效率约束。NIST 指出，不能仅凭平方根公式断言 AES-128 现在失效或必须立即全部替换；新系统或长期高敏感场景可根据风险与正式标准选择 AES-256，并按适用规范核对哈希与消息认证参数 [15]。

2.5 Shor 与 Grover 的关系及区别

两者都是量子算法，都需要物理量子设备才能获得真正加速，但解决的问题和安全影响不同。

表 2.1: Shor 算法与 Grover 算法的工程差异

比较项	Shor 算法	Grover 算法
核心问题	整数分解、有限域和椭圆曲线离散对数	无结构搜索与通用穷举加速
主要受影响机制	RSA、DH、DSA、ECDH、ECDSA 等公钥密码	对称密钥搜索、哈希原像搜索等
影响性质	改变底层困难问题的可解性，属于结构性威胁	将理想查询次数降低到平方根量级
典型响应	迁移到 PQC 密钥建立和签名算法	使用更长密钥/哈希并遵循更新后的参数规范
硬件要求	大规模、低逻辑错误率、深线路容错量子计算	同样需要量子硬件；现实资源仍十分可观
二者关系	两者相互独立，均依赖物理量子硬件。Shor 利用特定代数结构；Grover 加速无结构搜索。	

2.6 从算法威胁到业务风险

量子算法只有在硬件能力、脆弱协议、可取得的材料和可利用的业务入口同时成立时，才会形成现实攻击路径。机密性路径是截获受脆弱公钥密钥交换保护的通信及握手信息，在具备相应量子能力后推导共享秘密、重建会话密钥，再解密留存密文；若数据仍在保密期内，就可能造成客户信息或商业秘密暴露。真实性路径是从公开验证密钥求得相应签名私钥，再通过仍接受旧算法的验证端提交伪造指令、证书或软件更新；只有攻击者能进入相应提交流程且验证方接受时，才会进一步产生欺诈或供应链后果。风险并非量子设备一出现就自动发生。

金融机构还应区分攻击风险与迁移风险：升级算法、证书和接口本身可能引入兼容故障、时延和服务中断。因此，业务映射既要说明攻击如何到达资产，也要说明防护变更如何通过试点、容量测试和安全回退进入生产。

表 2.2: 传统密码威胁的业务映射

业务对象	暴露与攻击路径	可能后果与控制重点
API 与机构间通信	留存脆弱密钥交换的握手与密文；或对端继续接受旧证书签名	会话内容泄露或连接方被冒用；验证混合密钥建立、证书链和降级防护
长期档案与备份	外层公钥封装和历史副本可被取得，相关数据密钥可能被推导	保密期内的档案暴露；定位副本、减少收集路径并规划重封装
支付指令与电子合同	验证端仍接受可被伪造的 RSA/ECDSA 签名	伪造指令可能被受理；升级签名并保留可信时间戳与长期验证证据
软件、固件与模型发布	攻击者既能伪造旧算法签名，又能进入更新分发链	恶意更新被旧验证器接受；更新签名链、发布控制和安全启动
客户身份与访问	旧客户端或设备证书仍可在认证入口使用	冒用身份访问接口；缩短旧证书窗口并监测实际算法协商

历史签名并不会仅因未来出现量子设备就自动变成伪造；是否能够证明其在密钥受损前已经存在，取决于可信时间戳、撤销状态和存档证据。类似地，重封装可保护仍受控的数据密钥，却不能追回此前已被第三方复制的密文。这些边界决定了保密性和真实性需要分别排序与验收。

2.7 HNDL 与迁移窗口

先收集、后解密（Harvest Now, Decrypt Later, HNDL）指攻击者今天复制加密通信或存储数据，在未来获得更强计算能力后再解密。它使风险起点前移：对数据寿命长于潜在量子窗口的内容，攻击无需等到 CRQC 出现才开始。

评估优先级时，应同时考虑：数据还需保密多久、是否暴露在可被截获的网络或第三方环境、密钥是否能被重新封装、历史副本能否定位、泄露后对客户和市场的影响，以及迁移需要多长时间。可用第 1 章式(1.4)进行情景判断，而不把 T_Q 当作一个可以精确预测的日期。

2.8 威胁模型的边界

PQC 能够在正确实现和部署的前提下，为密钥建立、数字签名及其所支撑的身份验证和软件发布提供抵御已知量子算法攻击的密码机制。其直接价值是保护未来建立的通信密钥与签名信任链，并为需要长期保密的数据提前升级保护方式。

这一能力有明确边界。PQC 不能恢复已经泄露的明文，不能自动消除过去截获且已可解密的密文风险，也不能修复弱身份验证、私钥泄露、权限配置错误、软件漏洞、侧信道、恶意内部人员或不安全的终端。新实现还可能引入兼容性、性能和实现安全问题。因此，迁移应与密钥管理、漏洞治理、监测响应及业务连续性安排共同实施，并以实际协议和系统测试证明效果。

后量子密码标准及其数学基础

3.1 首批标准化方案的选择依据

美国国家标准与技术研究院（NIST）在 2016 年启动公开的后量子密码标准化程序，经过多轮国际评审、密码分析、实现测试和参数调整，于 2024 年 8 月发布首批三项正式标准：

- **ML-KEM (FIPS 203)**：用于建立共享密钥，取代或补充 RSA/ECDH 密钥建立；
- **ML-DSA (FIPS 204)**：基于格的通用数字签名；
- **SLH-DSA (FIPS 205)**：基于哈希函数的无状态数字签名 [5, 6, 7]。

之所以重点解释这三项，并不是因为 PQC 只有三种算法，也不是因为所有司法辖区都必须直接采用 NIST 标准，而是因为它们为首批完成正式标准化、具有公开规范和广泛实现生态的通用基线。金融机构仍需依据所在地监管、密码许可、行业网络和供应商支持确定生产算法。NIST 标准亦会通过勘误和修订持续维护，实施时必须锁定标准版本、参数集和实现版本。

表 3.1: 从第 2 章威胁到三项 PQC 标准的对应关系

现有功能	量子威胁	PQC 响应	数学安全基础
TLS/VPN/API 密钥建立	Shor 威胁 ECDH、DH 和 RSA	ML-KEM，短中期可与传统机制混合	模格上的带误差学习问题 (Module-LWE)
证书、合同、交易和代码签名	Shor 威胁 RSA/ECDSA/DSA	ML-DSA	Module-LWE 与模格短整数解 (Module-SIS)
高保证或算法多样化签名	同上	SLH-DSA	哈希函数的原像、第二原像和碰撞安全性
对称加密与哈希	Grover 带来平方根级加速	通常调整密钥和输出长度，不由上述三项直接替代	对称密码与哈希安全假设

3.2 格及模格结构

格可以直观理解为由若干基向量的整数线性组合形成的离散点集。给定线性无关的基向量后，格可写为

$$\mathcal{L}(\mathbf{B}) = \left\{ \sum_{i=1}^n z_i \mathbf{b}_i : z_i \in \mathbb{Z} \right\}. \quad (3.1)$$

在高维空间中，寻找最短向量、最近向量或满足特定模关系的短向量被认为十分困难。PQC 并不是直接把业务数据“放在格上”；格困难问题用于构造密钥、密文和签名，使攻击者难以从公开信息恢复秘密。

ML-KEM 和 ML-DSA 使用的是具有环和模结构的模格。这类结构能使运算更紧凑、更快，但也

意味着安全性依赖对结构化格问题的持续密码分析。金融机构无需自行证明底层困难性，却必须采用经标准化的参数和经过审查的实现，不能任意修改噪声分布、压缩方式或采样过程。

3.3 带误差学习与计算困难性

带误差学习（Learning With Errors, LWE）的核心形式为

$$\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \pmod{q}, \quad (3.2)$$

其中 $\mathbf{A}$ 公开， $\mathbf{s}$ 是秘密， $\mathbf{e}$ 是从规定分布采样的小误差。若没有 $\mathbf{e}$ ，攻击者可通过线性代数求解 $\mathbf{s}$ ；加入合适误差后，恢复 $\mathbf{s}$ 与高维格困难问题相关 [16, 17]。

Module-LWE 把标量或普通矩阵元素替换为多项式环中的元素，在效率与安全分析之间取得平衡。这里的“噪声”不是系统故障，而是算法设计的一部分；误差必须足够小，以便合法接收者正确恢复共享秘密，又必须具有足够随机性以隐藏私钥。附录B给出解密正确性的简化推导。

3.4 ML-KEM：模格密钥封装机制

密钥封装机制（Key-Encapsulation Mechanism, KEM）不是直接加密大文件，而是让发送方和接收方建立一个短的共享秘密，再由密钥派生函数生成对称会话密钥。其接口包含：

$$(pk, sk) \leftarrow \text{KeyGen}(), \quad (3.3)$$

$$(ct, K) \leftarrow \text{Encaps}(pk), \quad (3.4)$$

$$K' \leftarrow \text{Decaps}(sk, ct). \quad (3.5)$$

正确执行时 $K' = K$ 。实际数据随后由**认证加密（AEAD）**保护。

ML-KEM 的内部算法由 Kyber 演化而来，使用 Module-LWE 结构、压缩编码和经规范定义的转换，目标是在主动攻击环境中达到选择密文安全。FIPS 203 定义 ML-KEM-512、768 和 1024 三个参数集；参数数字是名称的一部分，不等于密钥位数。金融机构不应仅按“数字越大越安全”选择，而应结合监管安全级别、性能、报文大小、协议支持和供应商互操作性。

3.4.1 选择明文与选择密文安全模型

选择明文攻击（Chosen-Plaintext Attack, CPA）假设攻击者可以选择明文并观察相应密文；安全目标是攻击者仍不能区分目标密文所对应的明文。选择密文攻击（Chosen-Ciphertext Attack, CCA）进一步允许攻击者向解密接口提交选择的密文并观察结果，但不能直接询问目标密文。现实网络协议面临畸形报文、错误响应和主动探测，因此 KEM 通常需要更强的 CCA 安全目标。

ML-KEM 的解封装还要求对无效密文进行一致处理，避免错误消息、时间差或回退行为泄露秘密。工程验收不能只测试“正常情况下双方得到相同密钥”，还要测试畸形密文、重复报文、超时、密钥不匹配和实现侧信道。

3.5 ML-DSA：模格数字签名机制

数字签名提供真实性和完整性。签名者使用私钥产生签名，验证者使用公钥检查：

$$\sigma \leftarrow \text{Sign}(sk, m), \quad (3.6)$$

$$\{0, 1\} \leftarrow \text{Verify}(pk, m, \sigma). \quad (3.7)$$

ML-DSA 由 Dilithium 演化而来，安全基础主要关联 Module-LWE 和 Module-SIS。Module-SIS 可简化描述为：在给定公开矩阵 $\mathbf{A}$ 时，寻找非零且足够短的 $\mathbf{z}$ ，使

$$\mathbf{Az} \equiv \mathbf{0} \pmod{q} \quad (3.8)$$

仍然困难。

签名过程中使用拒绝采样，以防签名值泄露私钥相关信息：候选值若不满足规定分布和界限，就被丢弃并重新采样。这解释了为什么签名耗时会有轻微波动，也说明实现必须谨慎处理随机数、采样和时间侧信道。FIPS 204 定义 ML-DSA-44、65 和 87 三个参数集。选择时要同时考虑签名大小、验证吞吐量、设备能力、证书链膨胀和长期验证需求。

3.6 SLH-DSA：无状态哈希签名机制

SLH-DSA 由 SPHINCS+ 演化而来，不依赖格困难问题，而是组合一次性签名、少次签名和 Merkle 树，通过哈希函数把大量临时公钥承诺到一个较短的根值。其安全依据更保守、数学依赖更少，可形成与格密码不同的算法多样性。

直观地说，签名者沿一棵哈希树提供认证路径，验证者逐层计算并确认最终根值与公钥一致。多层树和地址化设计防止不同节点或不同用途之间发生混淆。SLH-DSA 的主要代价是签名较大、签名速度通常低于 ML-DSA；优势是只依赖成熟哈希假设、无需维护有状态计数器，并提供多个安全级别及“小签名/快速签名”参数族。

金融机构可把 SLH-DSA 视为以下场景的候选：根证书或固件等签名频率较低但要求长期可信的对象；需要与格密码形成算法多样性的高保证场景；或所在地标准和供应商生态明确支持的场景。它不是默认优于 ML-DSA，也不适合未经容量评估直接用于高频交易消息。

3.7 传统与后量子密码的混合构造

混合密码机制在一次协议执行中组合传统算法与 PQC 算法，使最终安全性不完全依赖其中单一机制。例如，混合密钥协商可将 X25519 与 ML-KEM-768 产生的两个共享秘密输入密钥派生函数：

$$K = \text{KDF}(K_{\text{classical}} \parallel K_{\text{PQC}}, \text{context}). \quad (3.9)$$

IETF RFC 10024 规定了 TLS 1.3 中的若干传统/PQ 混合密钥协商组合 [9]。

混合机制的价值在于过渡期风险分散和互操作演进，但它不是把两个算法名称拼接即可。安全性取决于组合构造、上下文绑定、降级防护、错误处理和实现质量。签名混合尤其需要明确“两个签名都必须有效”还是其他验证策略，以及证书、协议和业务系统如何表达该策略。

3.8 算法选型与实施约束

算法选择应遵循四层约束：第一，所在地正式标准和监管要求；第二，协议标准与行业网络支持；第三，关键供应商的生产级实现和维护承诺；第四，机构自身的性能、硬件和业务连续性验证。实验代码、候选算法、草案协议和供应商预览版可用于实验室评估，但不能替代生产审批。

截至本报告发布日，FIPS 203、204 和 205 均为正式标准；NIST 已对标准文件发布勘误或修订提示。上线前应复核最新公告，保留标准版本、参数集、软件库、编译选项和测试向量。第 4 章进一步说明这些算法如何进入 TLS、签名、静态数据和身份体系。

端到端迁移机制与目标架构

4.1 迁移生命周期与完整性要求

一个完整迁移必须覆盖发现、分类、设计、共存、验证、切换、观察、停用和取证。如果只替换密码库而忽略证书链、密钥设备、对端系统、历史数据和失败回退，机构可能在“使用了 PQC”的同时产生新的可用性或降级风险。

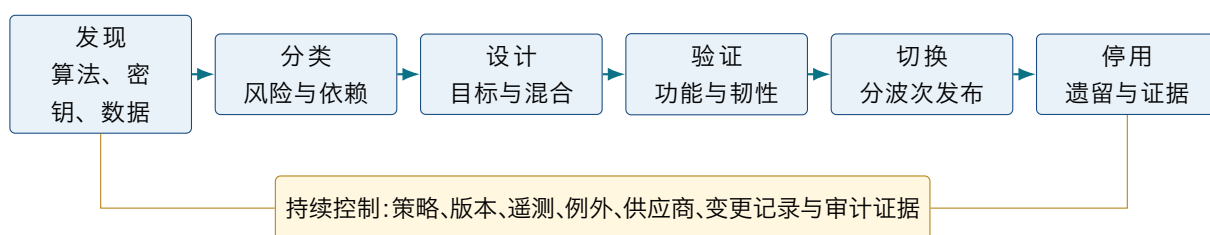


图 4.1: PQC 迁移的完整生命周期

每一阶段都应有明确进入和退出条件。特别是“切换成功”不等于“迁移完成”：只有旧密钥和旧证书已妥善处置、所有依赖已解除、观察期满足、业务责任人签署且证据归档后，旧机制才可停用。

4.2 分层目标架构

表 4.1: 目标架构分层及核心职责

层次	核心能力	设计要求
业务与数据层	数据分类、签名有效期、交易和监管流程	明确机密性/真实性期限、业务中断容忍度和责任人
应用与协议层	TLS、API、文件交换、签名、身份与代码发布	不在业务代码中硬编码算法；支持双轨验证和版本协商
密码服务层	KEM、签名、AEAD、证书、密钥派生与策略	经批准的算法目录、统一接口、上下文绑定和失败关闭
密钥与硬件层	KMS、HSM、密钥生命周期、随机数和备份	确认 PQC 密钥/签名大小、固件支持、导入导出和高可用
治理与证据层	CBOM、配置基线、遥测、例外、测试和审计	每个版本可追踪、每次切换可解释、每项例外有到期日

密码敏捷（**cryptographic agility**）贯穿五层：机构能够在不大规模重写业务流程的条件下，更换算法、参数、证书和实现；同时保证变更经过授权、测试、监测并可在安全边界内恢复。它不是“允许任何算法自由切换”，而是受策略约束的可替换性。

4.3 传输层协议、API 与机构间通信

TLS 迁移通常先处理密钥建立，再处理证书签名。推荐的过渡路径为：

1. 识别客户端、服务端、负载均衡、网关、服务网格和对端机构的 TLS 版本、密码套件与证书链；
2. 在隔离环境启用经标准化的传统/PQ 混合密钥协商，例如 RFC 10024 定义的 X25519MLKEM768；
3. 测量握手报文大小、CPU、内存、连接建立时延、失败率、重传和中间设备兼容性；
4. 通过特性开关或策略分组进行灰度发布，并监测实际协商结果；
5. 在 PQC 签名证书生态成熟后，再规划证书链、客户端信任库、OCSP/CRL 和硬件设备升级。

协议必须防止降级攻击。服务端不得因异常报文或攻击者干预而静默回到不符合政策的较弱算法。允许的兼容回退应限定对端、时间、数据范围和监测条件；涉及高敏感数据时，无法协商合规机制应优先阻断连接并告警。

例如，资产管理机构与托管机构每日交换估值文件时，应分别核查传输通道的密钥协商、文件自身的加密或签名，以及网关和批处理程序的证书依赖。试点可先在双方隔离环境复现日终批量负载，记录旧链路 with 混合链路的握手成功率、文件完整性、传输时延和失败恢复时间；生产发布还需双方共同批准兼容窗口与应急流程。

4.4 数字签名、证书与长期证据

签名迁移比密钥建立更复杂，因为签名可能需要多年后仍被验证。机构应区分：

- 在线短寿命签名：交易消息、会话令牌或短期授权，可随协议版本快速更新；
- 长期业务签名：合同、指令、监管档案和审计证据，需要时间戳、撤销状态和长期验证材料；
- 信任根签名：根证书、代码、固件、模型和设备启动链，迁移失败可能影响大范围系统。

迁移策略可以包括双签名、并行证书链、重新签名或为历史证据增加新的可信时间戳。选择取决于法律效力、验证方能力和存档期限。任何双签名方案都必须明确验证逻辑：是否要求两个签名均有效，旧签名何时停止被接受，验证失败如何记录，以及旧算法退出后历史证据如何复核。

以投资指令或电子合同为例，迁移对象不仅是签名算法，还包括签发机构、验证软件、时间戳、撤销记录和档案检索系统。试点应抽取跨年份样本，在旧版与新版验证器上分别测试签发、验证、撤销及长期复核，并记录不同对手方是否能识别新证书。只有在法律、业务和技术验证链条均闭合时，才适合扩大应用范围。

4.5 静态数据保护与密钥再封装

大型数据集通常由对称数据加密密钥（**DEK**）加密，再由密钥加密密钥（**KEK**）或公钥机制封装 DEK。若数据内容的对称加密仍满足安全要求，迁移可以优先更换“包裹密钥”的外层，而不必立即解密和重写全部数据：

1. 定位数据副本、DEK、封装元数据、备份和恢复流程；

2. 在受控环境解封旧 DEK 并使用新的 PQC/混合机制重新封装；
3. 保持内容密文不变，验证恢复、轮换、灾备和历史版本；
4. 在观察期后停用旧封装密钥并更新销毁证明。

这种“重封装”不能解决已经外泄的密文，也不能自动覆盖离线备份、导出文件或第三方副本。HNDL 风险较高的数据还应减少外部暴露、缩短留存、强化访问控制，并评估是否需要重新加密或重新生成。

对医疗研究数据、客户档案和长期合同，机构应先确定保密期限、所有副本的位置和密钥来源，再区分“仅更新外层封装”与“内容重新加密”。后一种方案涉及更高的计算、存储与业务协调成本；前一种方案则必须确认原始密文和备份并未在此前暴露。两种方案都需要执行恢复演练，并保留密钥轮换和数据可读性的证据。

4.6 身份体系、软件供应链与设备信任

机器身份、客户端证书、代码签名、容器镜像、软件包、固件和安全启动通常拥有不同的更新周期。迁移前要确认：

- 身份提供者、目录、网关、终端和设备固件是否支持新密钥与签名格式；
- 构建系统、制品库、CI/CD、更新服务和终端验证器是否实施相同策略；
- HSM、智能卡、安全元件或可信平台模块是否容纳更大的密钥和签名；
- 离线设备、分支终端和长期不联网设备如何安全升级与撤销。

根信任更新必须先于依赖它的软件或设备更新。否则，新的 PQC 签名可能无法被旧终端识别，而旧信任根又过早停用，形成大范围不可用。

移动应用与长期运行的终端尤其需要分批验证：客户端更新率、旧版本最低支持期限、离线验证行为和证书撤销的传播时间都可能决定实际切换日期。软件发布链应以测试制品验证双签名和版本回退，确保旧设备仍可安全升级，同时避免攻击者利用兼容期接受未经授权的旧制品。

4.7 第三方、云与金融市场基础设施

机构即使没有源代码控制权，仍需对外包系统中的密码风险负责。供应商应提供：支持的算法与参数、产品版本和日期、协议互操作范围、HSM/KMS 依赖、性能数据、漏洞与勘误处理、回退机制、日志证据和退出安排。对支付网络、托管机构、交易场所、清算系统等双边或多边连接，迁移日期必须联合规划，不宜由单一机构单方面切换。

新合同和续约应优先购买具备密码敏捷的产品，而不是只承诺“未来支持 PQC”。承诺必须转化为可验收的版本、接口、测试窗口和服务水平。无法提供时间表的关键供应商，应进入集中风险清单并设置替代、隔离或退出计划。

4.8 共存、切换与安全回退

迁移期不可避免地存在多算法、多版本和多证书共存。机构应把每个迁移单元建模为状态机：

传统基线 → 混合试点 → 混合生产 → PQC 优先 → 传统机制停用。 (4.1)

每次状态转换都要定义技术门槛、业务签署、监测窗口和恢复动作。回退必须是预先批准、限时、可观察且不低于最低安全底线的操作。若回退会重新暴露已被判定不可接受的风险，应停止相关通道或切换至备用业务流程，而不是静默降级。

4.9 密码策略服务与运行可观察性

建议把允许的算法、参数、证书和最低版本集中到密码策略服务或等效控制面，由应用通过稳定接口调用。遥测至少记录：实际协商算法、参数集、证书链、软件/固件版本、失败原因、降级尝试、调用量、时延和责任系统。日志不得记录私钥、共享秘密或敏感明文。

密码敏捷只有在“能看见实际使用了什么”时才成立。否则，配置上允许 PQC 并不代表生产连接真正使用 PQC；同样，升级了密码库也不代表所有静态链接、容器镜像和第三方组件已同步更新。

4.10 生产迁移完成判定

一个系统只有同时满足以下条件，才可标记为完成迁移：

- 资产清单、数据寿命、依赖和责任人已经确认；
- 目标算法、参数、协议、产品版本和标准版本获得批准；
- 功能、性能、安全、互操作、灾备和抗扰动测试通过；
- 生产遥测证明目标机制被实际使用，异常处置经过演练；
- 旧密钥、证书、代码路径和供应商依赖已处置或纳入有期限例外；
- 业务、技术、风险和审计所需证据完整归档。

密码资产清单与风险排序

5.1 密码资产清单的基础作用

金融机构无法迁移未知的依赖。一个面向客户的 API 可能在网关使用 ECDH，在后端服务调用中使用另一套 TLS，在证书服务中依赖 RSA 签名，又通过 HSM 保护私钥；其软件包、容器、灾备站点和外包运维可能各有不同版本。仅从服务器配置或证书台账出发，会漏掉嵌入代码、静态链接库、设备固件和第三方服务中的密码使用。

因此，密码物料清单（**Cryptographic Bill of Materials, CBOM**）是路线图的事实基础。它记录“什么算法、在哪里使用、保护什么、由谁负责、依赖谁、何时更新”。本章主要供安全架构、资产管理、开发运维、数据治理、采购和业务责任人共同使用；内部审计用其复核完整性，高级管理层用汇总视图监督风险与进度。

5.2 CBOM 的最低字段

CBOM 不应成为一张无法维护的超宽表。建议采用关系型结构，将业务、数据、系统、密码对象和供应商分表管理，通过唯一标识关联。管理层视图只展示关键字段，详细技术字段保留在底层记录。

表 5.1: CBOM 核心字段与用途

字段组	核心字段	用于回答的问题
业务与责任	业务流程、服务、责任人、关键等级、恢复目标	中断会影响谁，谁批准迁移和例外
数据与期限	数据分类、保密/签名有效期、留存期、所在地、外部暴露	是否存在 HNDL 风险，需保护多久
密码对象	算法、用途、参数、协议、证书、密钥类型、库与版本	具体使用了什么，是否量子脆弱或已过时
技术位置	应用、主机、容器、网关、HSM/KMS、环境、接口	依赖位于哪里，如何测试和发布
供应链	厂商、产品、合同、支持状态、升级日期、退出能力	外部路线能否满足机构目标日期
迁移状态	风险等级、目标机制、波次、测试、例外、计划日期	何时改、当前进度、还有哪些阻塞
证据与时间	发现来源、扫描时间、人工确认、版本、审批记录	记录是否可信、是否需要重新验证

附录D提供可直接建立表单或数据库的字段模板。

5.3 发现方法：自动化与人工核实结合

单一扫描工具无法覆盖全部密码使用。建议把以下来源合并，并为每条记录保留发现证据：

表 5.2: 密码资产发现来源

方法	擅长发现	主要局限与补充
证书与密钥平台导出	证书链、算法、有效期、密钥位置和责任域	难发现应用内自带库；结合代码和运行时扫描
代码与依赖分析	API 调用、密码库、静态依赖、硬编码算法	可能误报或漏掉动态配置；需要开发者复核
配置与镜像扫描	TLS、SSH、VPN、容器、网关和中间件配置	只反映扫描时配置；需关联部署环境与版本
网络与协议观测	实际协商的协议、算法、证书和对端	加密流量可见度有限；不得以拦截方式扩大风险
HSM/KMS 与云清单	托管密钥、使用策略、轮换和调用日志	无法自动解释业务用途；需关联应用和数据
供应商问卷与证明	SaaS、设备、闭源软件和升级路线	自报信息需通过测试、合同与版本证据验证
业务访谈与数据目录	长期数据、法律期限、手工流程和影子系统	依赖人员知识；应形成签署并定期刷新

覆盖率应分别按资产类型衡量。不能因为服务器扫描覆盖 90%，就声称业务流程、移动端、外包和历史档案也覆盖 90%。高风险对象需要人工确认，未知项本身应作为风险进入跟踪。

5.4 依赖图：从“算法在哪”到“变更会影响谁”

清单记录单个对象，依赖图解释对象之间的关系。建议至少建立以下节点和边：

业务流程 → 数据 → 应用/接口 → 协议/算法 → 密钥/证书 → 平台/供应商。

例如，替换一个网关的密钥协商机制，可能影响移动客户端、合作机构、防火墙、硬件负载均衡和监控探针。依赖图应标识方向、版本和责任人，并允许从高价值数据反向追踪到所有保护机制。迁移波次的基本原则是：共同依赖应共同规划，上游信任能力应先于下游业务切换。

5.5 风险评分模型

评分模型用于排序，不替代专家判断。可为资产 i 定义：

$$R_i = 100 (0.24D_i + 0.18E_i + 0.18C_i + 0.14A_i + 0.14X_i + 0.12M_i), \quad (5.1)$$

其中各变量归一化到 $[0, 1]$ ： D 为数据寿命与敏感度， E 为外部暴露， C 为业务关键性， A 为算法脆弱性， X 为依赖与供应商集中度， M 为迁移难度。权重只是参考，机构应通过风险偏好和历史事件校准。

表 5.3: 风险因子的可解释评分示例

因子	高分情形	需要的证据
D 数据	保密期超过 10 年、客户/交易/生物或战略数据	数据目录、法律留存期、业务签署
E 暴露	公网、跨机构、云边界或可长期被截获	数据流、网络架构、第三方位置
C 关键性	中断影响核心服务、结算、监管或大量客户	BIA、RTO/RPO、关键业务认定
A 算法	RSA/ECC 用于长期机密性或长期签名	CBOM、证书与协议观测
X 依赖	多个对端、单一供应商、设备升级周期长	依赖图、合同、产品路线图
M 难度	无源码、无测试环境、硬件限制或停机窗口极少	架构评估、测试条件、历史变更

建议把高风险阈值与行动绑定，而不只生成颜色：例如 $R_i \geq 75$ 要求进入首批迁移或形成高级管理层批准的限时例外； $50 \leq R_i < 75$ 进入下一波次并完成供应商确认；低于 50 仍需纳入持续监测。任何关键数据存在已知外部可收集路径时，可直接上调优先级。

5.6 HNDL 优先队列

对机密性数据，可进一步计算简化时间缺口：

$$G_i = T_{D,i} + T_{M,i} - T_Q. \quad (5.2)$$

$G_i > 0$ 意味着在所设量子情景下已经进入迁移窗口。由于 T_Q 不确定，建议至少设置“加速、基准、延后”三个情景，并观察资产排序是否稳定。无论哪个情景都位于前列的资产，应优先处理；只在极端情景下上升的资产，可通过降低暴露、缩短留存或提升迁移准备度进行缓释。

计算时， $T_{D,i}$ 是从评估日起数据剩余的保密年限， $T_{M,i}$ 是该资产完成可验证迁移所需的年限， T_Q 是从同一天起算的情景化量子威胁时间；三者必须采用相同单位和起点。例如，某档案尚需保密 10 年、迁移预计 3 年，若加速情景假设 8 年后出现相关能力，则 $G_i = 10 + 3 - 8 = 5$ 年。这不是“5 年后必然泄露”的预测，而是说明当前排期无法覆盖该情景下的保密需求。

队列不能只按 G_i 从高到低排列。应先筛选可被持续截获、复制或由第三方长期保存的数据流，再叠加保密期限、客户影响、可用替代方案和供应商交付时间。对所有情景均为正值且暴露高的资产，立即进入首批保护或迁移；仅在加速情景为正值资产，先降低收集面、缩短不必要的留存并准备试点；负值资产仍纳入清单和年度复核。已被外部复制的密文不能靠后续重封装消除既有暴露，

应另行评估通知、调查和数据治理措施。本节时间缺口主要用于机密性排序；长期签名应按有效期、可信时间戳和验证链独立评估。

5.7 可复核的排序流程

以下伪代码强调数据质量和人工复核，而非追求自动给出最终结论：

```
for each asset in CBOM:
    validate owner, data_lifetime, algorithm, exposure, dependencies
    if required_field_missing:
        create remediation_task(asset)
        increase uncertainty_score(asset)
    score = risk_model(asset)
    if long_lived_data(asset) and externally_exposed(asset):
        score = max(score, HNDL_PRIORITY_FLOOR)
    assign provisional_wave(asset, score)

for each migration_wave:
    resolve shared dependencies and vendor dates
    review with business, security, architecture and risk owners
    approve wave or record a time-bound exception
```

第一轮产生的是暂定排序。随后必须检查共同供应商、共同证书链、网络对端和业务高峰等约束，避免把技术上相邻的组件拆到不同波次。每次人工调整都记录理由、批准人和复核日期，使风险模型既可自动计算，又不掩盖专业判断。

5.8 清单质量与持续更新

CBOM 应纳入配置管理和变更流程，而不是项目结束时的静态附件。最低质量指标包括：关键业务覆盖率、必填字段完整率、责任人确认率、记录新鲜度、供应商证明覆盖率、未知算法数量和已到期例外数量。新系统上线、证书签发、密码库升级、供应商版本变更和并购整合都应触发更新。

建议每季度刷新高风险范围，每半年对关键供应商重新确认，每年至少进行一次全范围复核；重大标准勘误、算法漏洞或量子风险情景变化时立即触发专项更新。

金融机构后量子密码迁移参考路线图

6.1 路线图模型与适用条件

本章提供一套 60 个月参考模式。它把 FINMA 建议的治理动作、NIST 标准成熟度和大型金融机构常见技术依赖组合在一起，但不构成任何司法辖区的统一法定期限。参考本建议的机构可将自身启动日设为第 0 天，结合数据寿命、监管要求、技术规模、供应商窗口和年度变更冻结期重新排程。

路线图有两个不同终点：关键流程目标日期，表示高风险数据和核心业务完成迁移；完整迁移目标日期，表示供应商长尾、遗留系统和已批准例外基本关闭。二者不应被压缩成一个无法执行的日期。

6.2 启动阶段：前 90 天

1. 第 0–30 天：指定高级管理层发起人和项目负责人；批准章程、范围、风险假设和工作组；冻结新增长期 RSA/ECC 依赖，确有必要的进入架构例外。
2. 第 31–60 天：确定 CBOM 字段和发现方法；识别首批长期敏感数据、关键流程与关键供应商；发出供应商问卷；选择两个候选试点。
3. 第 61–90 天：形成初始风险热图、依赖图和目标架构原则；估算 36–60 个月资源；向治理委员会提交路线图草案和试点立项建议。

90 天完成的不是全量资产盘点，而是建立能够持续扩展的治理、数据结构和决策节奏。管理层应在此时确认：项目是否覆盖所有必要职能，资产记录是否有责任人，试点是否代表真实依赖，以及供应商是否进入正式沟通。

6.3 阶段一：治理、基线与路线图（3–12 个月）

目标是形成管理层批准的实施依据：

- 完成关键业务和高风险数据范围的 CBOM，建立数据寿命与依赖关系；
- 对关键供应商获得书面版本路线、协议支持、HSM/KMS 约束和测试窗口；
- 批准目标算法目录、混合机制原则、密码敏捷要求和最低安全底线；
- 建立多情景风险模型和迁移波次，明确关键流程与完整迁移目标日期；
- 形成预算、人员、采购、测试环境、变更窗口和审计证据计划。

退出条件是“能够解释并批准”，而不是“所有技术问题都已经解决”。路线图必须列明未知项及关闭日期，不能用模糊的“持续关注”替代行动。

6.4 阶段二：试点与共性能力（6–18 个月）

建议至少选择一个密钥建立场景和一个签名场景。典型组合是外部 API/机构间 TLS 混合密钥协商，以及文件交换/代码签名双轨验证。同步建设共性能力：算法目录、策略接口、测试向量、遥测、版本台账、证书实验链和自动化证据采集。

试点目标不是证明某算法在实验室中“能够运行”，而是验证端到端业务在高峰负载、异常网络、密钥故障、证书错误和回退条件下仍满足安全与服务要求。第 7 章给出验收方法。

6.5 阶段三：高风险流程迁移（12–36 个月）

优先迁移 HNDL 风险高、外部暴露强、长期签名重要或供应商窗口明确的流程。每个波次包括：

范围确认 → 设计批准 → 预生产验证 → 灰度发布 → 观察 → 旧机制处置。

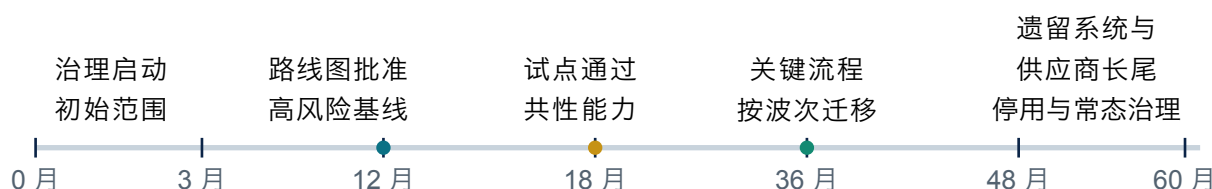
应避免按组织部门机械分批。更有效的波次通常围绕共同协议、共同信任链、共同供应商或共同数据域设计，以减少重复测试和跨波次依赖。

6.6 阶段四：规模化、长尾与停用（24–60 个月）

该阶段处理分支终端、移动端、设备固件、收购系统、离线档案、长期合同和缺少厂商支持的遗留产品。可采用替换、隔离、前置网关、缩短留存、降低暴露或限时例外等策略。无法迁移且风险不可接受的系统应制定退出日期，不应无限期留在“待观察”状态。

同时把 PQC 能力转入常态运营：新项目默认采用批准的密码策略，CBOM 由变更流程自动更新，供应商定期证明，管理层季度查看风险和迁移指标，算法勘误或实现漏洞触发快速替换流程。

6.7 参考时间线



图中的月份从机构正式启动日计算。阶段允许重叠：例如供应商沟通贯穿全程，试点可在部分 CBOM 仍扩展时开始；但生产切换必须满足第 4 章定义的完整门槛。

6.8 资源与预算口径

预算应按能力和迁移波次编制，而不是只列“采购 PQC 软件”。主要成本包括：

- 资产发现、数据治理和依赖建模；
- 密码库、PKI、HSM/KMS、网关、终端和监测工具升级；
- 供应商版本、许可证、专业服务和联合测试；
- 开发、架构、测试、运维、业务参与及变更窗口；
- 独立安全评估、性能测试、审计取证和培训；

- 遗留系统替换、例外缓释及双轨运行期间的额外容量。

年度拨款可与阶段门槛挂钩：基线批准、试点通过、关键波次上线、旧机制停用和例外关闭。这样既保留多年投入承诺，又避免在技术或供应链条件变化时一次性锁定全部方案。

6.9 跨辖区适用性与本地化核查

FINMA 通告提供了可借鉴的治理结构，但其中的监督范围和时间要求只直接适用于相应瑞士受监管机构。其他地区的金融机构可以参考其控制目标，再依据所在地法律、监管要求、行业网络和供应链条件形成自己的实施计划。下表是本地化核查框架，而非对不同辖区成熟度作高低排名。

表 6.1: 跨辖区实施路线图的本地化核查框架

层级	核查事项	形成的证据
国际标准	核对算法标准、协议规范、参数集与供应商实现版本	标准映射及互操作测试记录
本地监管	核对密码、金融数据、网络安全、外包与产品准入要求	法规适用性清单与审批路径
行业基础设施	确认支付、清算、托管、交易和身份网络	对手方接口清单与协同计划
跨境业务	明确数据传输、合同、外部服务与审计证据的属地要求	数据流图与合同条款
内部治理	由风险、业务、技术和审计共同确定预算、里程碑与例外	经批准的路线图和定期报告

国际标准有助于技术选型和互操作，但并不自动替代所在地的正式标准、检测认证或监管程序。不同地区的实施日期也不宜直接照搬；共同的基础仍是资产清单、风险排序、供应商协同、测试证据与可执行的路线图。

6.9.1 国际参考时间表与机构排期校准

NCSC 提出的英国参考节点为：**2028** 年完成发现、评估和初始迁移规划；**2031** 年完成最高优先级迁移并完善后续计划；**2035** 年完成 PQC 迁移 [2]。这些节点属于英国指导语境；FINMA 提出的 2027 年年中节点针对路线图准备，两者对应的交付阶段不同。

金融机构可以将自己的资产基线、试点、高风险流程迁移及遗留机制停用分别映射到相关参考节点，再按所在地要求、数据保护期限和供应商版本重新排程。本报告的 60 个月模式以机构启动日为起点，不能据此推导全球统一的完成年份。对于保护窗口已收窄的长期敏感数据，可先落实优先控制；对于尚未具备成熟协议或产品支持的场景，应明确依赖、临时控制和复核日期。

6.10 路线图年度复核

路线图至少每年重估一次，在以下事件发生时立即专项复核：正式标准修订或勘误、算法或实现出现重大漏洞、监管要求变化、关键供应商延期、并购或云迁移、重大数据分类变化，以及量子硬件能力出现可信跃迁。复核应记录假设变化如何影响优先级、预算和目标日期。

试点验证、抗扰动与生产验收

7.1 试点必须回答的四个问题

金融机构的 PQC 试点应选择真实协议、真实产品版本和代表性负载，在隔离或预生产环境中回答：

1. 安全性：采用的算法、参数、组合方式和失败处理是否符合批准标准？
2. 可用性：业务功能、对端互操作、容量和恢复目标是否满足要求？
3. 韧性：网络、密钥、证书、设备或供应商服务发生扰动时，系统能否受控阻断、告警、恢复且不静默降级？
4. 可运营性：配置、版本、实际协商、例外和证据是否能够持续管理？

“完成一次成功握手”只能证明最基本功能，不能作为生产上线依据。

7.2 试点一：混合 TLS/API

选择一个边界清晰、可重复压测且具有真实对端的 API 或机构间接口。建立传统 TLS 基线后，测试批准的混合密钥协商组合。测试矩阵至少覆盖：

- 不同客户端、服务端、网关、负载均衡和密码库版本；
- 完整握手、会话恢复、连接复用、并发峰值和大报文；
- 握手时延、CPU、内存、带宽、失败率、重传率和最大并发；
- 证书链、SNI、代理、服务网格、入侵检测和日志平台兼容；
- 允许组合、禁止组合、未知组合和主动降级尝试。

基线和 PQC 测试必须使用相同硬件、网络条件、数据集和负载曲线。结果既报告平均值，也报告 P95/P99 尾部时延和错误分布；只看平均时延可能掩盖高峰期队列和超时。

7.3 试点二：文件交换或数字签名

选择合同、投资指令、监管报文、软件制品或机构间批量文件。测试 ML-DSA 或经批准方案的签名、验签、时间戳、归档和审计链。若采用双签名，明确两个签名的验证策略及过渡日期。

重点指标包括签名与验证吞吐量、签名/证书大小、存储增长、批量处理窗口、HSM/KMS 兼容、无效签名拒绝、密钥轮换、撤销、历史证据复核和灾备恢复。长期档案还应执行“未来验证演练”：在独立环境使用归档的公钥、算法标识、标准版本、证书状态和时间戳重建验证过程。

7.3.1 金融市场基础设施参考案例：Project Leap

国际清算银行（Bank for International Settlements, **BIS**）于 2025 年 12 月发布 Project Leap 第二阶段报告。在欧元体系 T2 支付系统的隔离测试环境中，项目验证了流动性划拨报文的抗量子签名、功能、性能及互操作，并发现处理性能差异和组件改造需求 [3]。

该实验采用早期 Dilithium 版本，尚未测试最终 ML-DSA 标准；测试以软件密钥文件替代物理

硬件安全模块，且未覆盖全部生产链路。因此，案例支持受控验证的可行性，生产部署仍需补足当前标准、密钥托管及全链路测试。

参考这一经验，机构可从一条可重复测试的报文或文件链路入手，同时确定发送方、接收方、网络服务商和验签组件的责任；把标准版本、密钥保护、报文容量、异常拒绝和峰值负载列入试点范围。试点成果应沉淀为可复用的接口、测试用例与交付文件，后续波次再逐项验证各自差异。

7.4 抗扰动验证框架

抗扰动不是泛泛的“稳定性测试”，而是验证系统面对可预期异常时仍遵循安全策略。建议从六类扰动设计故障注入：

表 7.1: PQC 迁移的抗扰动测试

扰动类型	测试注入	预期安全行为
网络与报文	延迟、丢包、乱序、分片、重复、截断和超大握手报文	有界重试、无状态混淆、无资源耗尽；超过阈值受控失败并告警
算法协商	删除 PQC 组合、伪造不支持、重复扩展、参数错配	检测并阻断未授权降级；仅按批准兼容策略回退
证书与签名	过期/撤销/未知证书、错误签名、超长链、算法标识不一致	严格拒绝、统一错误处理、保留事件证据，不绕过验证
密钥与随机数	密钥缺失、HSM 不可用、轮换中断、随机数源异常	不复用不安全密钥；切换高可用或停止服务，触发高优先级告警
容量与资源	峰值并发、CPU/内存压力、队列拥塞、日志写满	限流和隔离，维持关键服务；不得因压力自动启用弱算法
部署与供应商	版本回滚、部分节点升级、云区域故障、对端版本漂移	识别配置漂移，按波次隔离/恢复，保持状态一致和可追踪

每个测试用例要写明前置条件、注入方式、期望结果、最大恢复时间、停止条件、证据位置 and 责任人。涉及生产镜像或外部对端时，需事先批准并设定不影响真实客户和资金的边界。

7.5 安全回退与失败关闭

安全回退不是“恢复到任何能工作的旧版本”。应预先定义三种结果：

- 恢复到批准的上一安全状态：适用于新实现缺陷但旧机制在限定期限和数据范围内仍符合风险偏好；
- 切换备用安全通道：例如专线、离线签名或人工复核流程；
- 失败关闭：当回退会低于最低安全底线时暂停连接或交易，并启动业务连续性流程。

回退包应包含配置、证书、密钥引用、应用版本、数据库变更和依赖服务的一致恢复步骤。演练不仅验证“回得去”，还要验证回退后没有双重处理、状态丢失、未授权降级或审计断点。

7.6 实现安全与侧信道

PQC 数学安全不等于实现安全。测试应覆盖：

- 常数时间实现、缓存和分支行为，防止时间及微架构侧信道；
- 解封装失败、签名拒绝和解析错误是否产生可区分响应；
- 随机数、采样、密钥生成和敏感内存清理；
- 畸形公钥、密文和签名的输入验证与模糊测试；
- 密码库来源、软件物料清单、构建链、签名和漏洞响应；
- HSM 或硬件加速的固件版本、认证边界和密钥不可导出属性。

高风险实现宜接受独立代码审查、渗透测试或实验室评估。测试报告应区分算法标准符合性、协议符合性、实现安全和业务验收，避免用一类测试替代另一类。

7.7 性能与容量模型

对场景 j ，可估算额外容量：

$$\Delta C_j = N_j(\Delta c_{\text{cpu}} + \Delta c_{\text{mem}}) + B_j \Delta s_{\text{wire}} + S_j \Delta s_{\text{store}}, \quad (7.1)$$

其中 N_j 为操作量， B_j 为握手或报文量， S_j 为签名/证书存储量。模型只用于初始规划，最终应以峰值压测和生产遥测校准。除了平均资源，还要评估 HSM 队列、证书链放大、网络 MTU/分片、移动端电量和灾备容量。

7.8 生产准入门槛

建议把以下条件作为统一准入门槛：

1. 标准、算法、参数、软件和固件版本已记录并经架构/安全批准；
2. 业务功能、互操作、性能、容量、故障注入和灾备测试通过；
3. 未关闭的高危漏洞为零，中低风险缺陷有责任人和期限；
4. 遥测能证明实际协商与配置一致，告警已接入运营流程；
5. 回退或失败关闭经过演练，最低安全底线不可被静默绕过；
6. 业务、技术、风险和变更管理完成签署，证据包可复核。

7.9 证据包与观察期

每个试点和生产波次应形成统一证据包：范围与架构、资产快照、标准版本、配置、测试数据摘要、用例及结果、缺陷和整改、性能基线、扰动记录、回退演练、供应商证明、批准记录和生产遥测。敏感信息按最小权限保存，但证据索引应允许审计人员确认其存在、版本和责任人。

上线后设置与业务风险相匹配的观察期。期间监测协商算法、失败与回退、P95/P99 时延、错误率、CPU/内存、HSM 队列、证书异常、配置漂移和客户影响。只有观察期达标，旧机制处置和业务签署完成后，迁移状态才从“已上线”转为“已完成”。

治理、供应链与持续保证

8.1 治理结构

PQC 迁移跨越多年且涉及核心系统，建议纳入现有技术风险和业务韧性治理，而不是建立脱离日常管理的临时委员会。董事会或其风险委员会监督风险偏好、目标日期、重大投资和高风险例外；高级管理层指导委员会负责跨部门取舍；项目办公室维护路线、依赖、预算和证据。

表 8.1: 关键活动的责任分配

活动	业务	安全	技术	风险	说明
数据寿命与业务影响	A/R	C	C	C	业务责任人确认保护期限和中断后果
CBOM 与依赖图	C	A	R	C	技术团队发现，安全负责控制口径
目标架构与算法目录	C	A/R	R	C	法务、采购和本地密码专家参与咨询
试点和生产验收	A	R	R	C	业务对可用性签署，安全对最低底线签署
风险例外	R	C	C	A	高风险/长期例外升级至高级管理层
审计与保证	C	C	C	R	内部审计保持独立评价

表中 A 为最终负责，R 为执行负责，C 为咨询参与。实际机构可将角色映射到既有三道防线和委员会体系，但每项关键决定只能有清晰的最终责任人。

8.2 董事会与高级管理层应看到什么

季度报告应控制在能够支持决策的范围，而非罗列全部算法。建议包括：

- 高风险业务和长期敏感数据的覆盖率、趋势和未识别范围；
- 关键流程迁移进度、下一波次、重大阻塞和目标日期偏差；
- 关键供应商支持状态、合同缺口和替代/退出准备；
- 试点及生产中的安全、性能、业务影响和重大缺陷；
- 高风险例外数量、金额/客户影响、剩余期限和批准层级；
- 预算、资源、技能与年度里程碑是否足以支持路线图。

管理层不需要判断具体多项式参数，但需要确认风险是否在可接受期限内下降，以及资源和供应链是否与承诺日期匹配。

8.3 供应商治理与合同要求

供应商问卷至少覆盖：产品和版本中的密码算法、PQC 支持状态、目标日期、混合协议、证书/HSM 依赖、性能影响、升级方式、兼容范围、漏洞响应和停用计划。问卷不是最终证据，关键声明需要由版本说明、实验测试、第三方评估或合同承诺支撑。

新采购和续约可纳入以下条款：

- 提供并持续更新相关密码组件和 PQC 路线；
- 在约定日期提供生产级版本、互操作环境和迁移支持；
- 对算法、实现或标准重大变化及时通知，并提供修复时限；
- 支持机构获取配置、日志、测试证据和必要审计权；
- 明确升级、双轨运行、数据导出和退出成本；
- 分包商和云依赖遵守同等要求，责任不得因转包而失去可追踪性。

8.4 例外管理

例外应是有期限的风险决定，而不是技术积压的另一种名称。每项例外记录资产、数据、原因、风险评分、补偿控制、业务影响、供应商依赖、责任人、批准人、到期日和退出计划。出现以下情形之一应升级审批：涉及长期敏感数据或核心业务；需要低于最低密码策略运行；期限超过一个年度；供应商没有可信路线；或多个系统依赖同一例外。

补偿控制可以包括网络隔离、减少数据留存、限制对端、提高监测、使用安全网关、缩短密钥周期或人工复核，但这些措施不能被描述为已经完成 PQC 迁移。

8.5 关键指标

建议同时使用领先指标和结果指标：

表 8.2: PQC 迁移的建议指标

类别	指标示例	解释
资产质量	关键业务 CBOM 覆盖率、必填字段完整率、责任人确认率、记录新鲜度	反映决策基础是否可信
风险减少	HNDL 高风险数据流数量、量子脆弱关键接口数量、风险加权暴露值	反映风险是否实质下降
交付进度	波次按期率、试点通过率、旧机制停用率、例外关闭率	反映路线图执行力
供应链	关键供应商书面路线覆盖率、互操作完成率、合同条款覆盖率	反映外部依赖可控程度
运行质量	PQC/混合协商占比、失败/降级率、尾部时延、重大事件和回退次数	反映生产真实状态
能力建设	密码敏捷接口采用率、自动化测试覆盖、已培训关键岗位比例	反映长期可持续性

覆盖率必须有明确分母。若资产总量仍未知，应同时披露估算方法和不确定性，避免用快速增长的扫描数量制造虚假进展。

8.6 三道防线与独立保证

第一道防线由业务、技术和运营团队实施并维护控制；第二道防线由信息安全、技术风险、合规和第三方风险职能制定政策、挑战评估并监督例外；第三道防线由内部审计独立评价治理、资产完整性、测试质量和报告真实性。

三道防线应在同一迁移波次中形成不同责任，而不是重复签字。第一道防线提供资产清单、代码和配置版本、业务测试及上线后协商日志，并对业务连续性作出验收；第二道防线独立挑战范围遗漏、参数选型、供应商声明和安全回退是否满足风险偏好，对超出政策底线的例外升级审批；第三道防线不代替项目团队实施或批准技术方案，而是评价前两道防线的决策与证据是否可信。

独立保证可采用双向抽样：从关键业务反向追踪到数据、接口、算法、密钥、供应商和测试证据，检查是否有未列入清单的依赖；再从 CBOM 抽取记录，正向验证生产配置、实际协商结果和责任人。对样本重算风险评分、重演关键异常与受控回退，核对旧机制是否停用或纳入有到期日的例外。高风险流程和重大切换应提高抽样比例，并在上线后观察期复核遥测；发现清单与生产不符、未经批准的降级或缺失证据时，应要求整改、重新测试，并向相应风险委员会报告。仅审阅项目汇报不足以证明控制有效。

8.7 证据架构

建议按“决策、资产、设计、测试、发布、运营、例外、供应商”八类建立证据索引。每项证据包含唯一编号、对象、版本、日期、责任人、批准状态、保管位置、保留期和访问等级。证据内容可以分散在配置库、工单、测试平台、合同系统和日志平台，但索引必须统一并可检索。

表 8.3: 最低证据集合

证据域	核心材料	证明的问题
治理与决策	战略、路线图、风险偏好、预算、会议决议	风险是否由适当层级知悉并批准
资产与风险	CBOM 快照、依赖图、数据寿命、评分与复核	范围和优先级是否有事实依据
架构与标准	算法目录、版本、ADR、威胁模型、供应商证明	为什么选择该机制，适用边界是什么
测试与发布	用例、结果、缺陷、容量、扰动、回退和签署	生产变更是否经过充分验证
运营与例外	遥测、事件、配置漂移、例外、关闭和停用证明	目标机制是否持续有效，遗留风险是否受控

8.8 能力成熟度

机构可用五级成熟度衡量进展：

1. 认知：形成风险共识和初始责任；
2. 可见：关键范围拥有 CBOM、数据寿命和供应商基线；
3. 可验证：目标架构、实验环境、测试和证据机制运行；
4. 可迁移：关键流程按波次上线，回退和运营能力成熟；
5. 可持续：密码敏捷成为新系统默认要求，清单、监测和算法替换进入常态治理。

成熟度应按业务域分别评价。机构整体达到较高级别，不代表某个收购系统、分支网络或外包平台已经满足同样水平。

8.9 持续更新与公开沟通

PQC 路线会随标准、实现和监管变化。项目结束后仍需保留算法观察、供应商复核、资产刷新、漏洞响应和年度演练。对客户、合作机构或投资者的外部表述应准确区分“制定路线图”“完成试点”“关键流程迁移”和“全量完成”，不得把支持某种算法表述为全部数据已经量子安全。

8.10 持续密码治理与运营机制

密码资产会随应用发布、证书轮换、云服务调整和供应商升级发生变化。机构应在项目向运营移交时，明确持续管理的责任人、预算、工具和升级路径，使首次迁移形成的资产清单、策略与测试能够继续发挥作用。

e23 在 2026 年 5 月的企业观点文章中，以其自有的 Triple-A 框架组织密码发现、敏捷调整和自动化治理 [4]。本节借鉴其对持续管理的关注，结合金融机构的变更与风险管理提出以下运营安排：算法与产品选型仍以适用标准和批准策略为依据。

1. 资产刷新与变更闭环。将扫描结果、应用发布、证书及密钥管理记录与 CBOM 关联。新接口、密码库升级、证书续期或外包变更触发差异检查；发现新增传统算法依赖、未知版本或责任人

缺失时，生成工单并指定关闭期限。清单保存发现来源、确认时间和版本，便于复核变化。

2. 策略审批与算法生命周期。分别记录允许使用、试点使用、限期兼容和禁止使用的算法、参数与实现版本，并确定启用、替换和停用条件。自动化工具执行经批准的策略，重大算法撤回、信任根更新和生产切换经过变更审批；紧急处置使用事先授权的预案，并保留操作及复核记录。
3. 实际使用监测与回归测试。同时检查传输密钥建立、身份认证和数字签名的实际机制，避免把其中一项升级视为整条链路完成保护。密码库、网关、对端或证书链变化后，重跑受影响的互操作、异常及性能用例；发现未授权降级、配置漂移或错误率上升时，按预案阻断、告警和恢复。
4. 运营节奏与服务交接。可按月复核资产变化、故障与证书到期，按季度报告风险、供应商支持与例外，按年评估路线图并开展恢复演练；频率由业务风险校准。依托外部服务时，合同应明确更新范围、响应时限、复测证据、数据保管与退出安排，机构保留策略审批和风险责任。

这一机制把资产发现、受控替换、复测和证据更新贯穿于系统生命周期。迁移成效既看旧依赖是否关闭，也看后续变更能否在合理时间和成本内完成。长期维护能力由实际运行记录、整改时效及可复核测试支撑。

术语与缩写索引

本索引既给出简明定义，也指向正文的详细说明。页码在最终编译时自动更新。

术语	简明定义	页码
FINMA	Swiss Financial Market Supervisory Authority，瑞士金融市场监管局；本报告引用其第 05/2026 号通告作为治理参考。	1
NCSC	National Cyber Security Centre，英国国家网络安全中心；其 PQC 迁移指导提供英国参考时间表和组织实施方法。	1
BIS	Bank for International Settlements，国际清算银行；Project Leap 为金融支付场景的抗量子技术验证案例。	22
PQC，后量子密码	在经典计算机上运行、旨在抵御已知经典与量子攻击的密码算法；不等于量子通信或量子计算。	8
CRQC	能够在现实时间和成本下攻击实际密码参数的容错量子计算机。	4
HNDL	“先收集、后解密”；攻击者今天收集密文，未来获得能力后再解密。	7
RSA	安全性基于大整数分解困难的公钥密码，可用于加密、密钥传输和签名。	4
ECC	椭圆曲线密码，包括 ECDH 密钥协商和 ECDSA 签名，安全性依赖椭圆曲线离散对数。	4
DH	Diffie–Hellman 密钥交换；基于有限域离散对数，在通信双方之间建立共享秘密。	4
DSA	Digital Signature Algorithm，数字签名算法；基于有限域离散对数。	4
ECDH	Elliptic Curve Diffie–Hellman，椭圆曲线密钥交换；基于椭圆曲线离散对数。	4
ECDSA	Elliptic Curve Digital Signature Algorithm，椭圆曲线数字签名算法。	4
Shor 算法	在足够可靠的量子计算机上高效求解整数分解和离散对数。	4
Grover 算法	对无结构搜索提供平方根级量子加速，影响对称密钥和哈希参数选择。	5
ML-KEM	NIST FIPS 203 标准化的模格密钥封装机制，用于建立共享秘密。	9
ML-DSA	NIST FIPS 204 标准化的模格数字签名算法。	9
SLH-DSA	NIST FIPS 205 标准化的无状态哈希数字签名算法。	10

术语	简明定义	页码
KEM	密钥封装机制；使用接收方公钥建立短共享秘密，再派生对称密钥。	9
CPA	选择明文攻击；攻击者可选择明文并观察密文。	9
CCA	选择密文攻击；攻击者可提交选择的密文并观察解密行为。	9
LWE / Module-LWE	带误差学习及其模格版本；ML-KEM 和 ML-DSA 的重要困难问题。	9
Module-SIS	模格短整数解问题；ML-DSA 安全分析的重要组成。	9
CBOM	密码物料清单；记录算法、协议、密钥、证书、位置、用途、责任人和依赖。	15
SBOM	软件物料清单；记录软件组件及版本，可为发现嵌入式密码库提供输入。	16
密码敏捷	在受控、可观察和可验证条件下替换算法、参数、证书和实现的能力。	11
混合密码	在同一协议中组合传统与 PQC 机制，以降低过渡期对单一算法的依赖。	10
TLS	Transport Layer Security，传输层安全协议；用于保护网络连接的机密性和完整性。	12
PKI	公钥基础设施；管理证书签发、信任链、撤销和验证。	12
HSM	硬件安全模块；在受保护边界内生成、保存和使用密钥。	11
KMS	密钥管理系统；管理密钥生成、授权、轮换、备份和销毁。	12
AEAD	认证加密；同时提供机密性与完整性，例如 AES-GCM。	9
DEK	数据加密密钥；直接加密数据内容的对称密钥。	12
KEK	密钥加密密钥；用于封装或保护 DEK。	12
RTO / RPO	恢复时间目标 / 恢复点目标，用于衡量业务连续性要求。	15
QKD	量子密钥分发；使用量子通信建立密钥，与软件可部署的 PQC 不同。	3

数学附录：从传统密码到 PQC

B.1 RSA 正确性与 Shor 算法的切入点

RSA 选择大素数 p, q ，令 $N = pq$ ，并计算

$$\varphi(N) = (p-1)(q-1). \quad (\text{B.1})$$

选择 e 使 $\gcd(e, \varphi(N)) = 1$ ，再求 d 满足

$$ed \equiv 1 \pmod{\varphi(N)}. \quad (\text{B.2})$$

对满足条件的消息 m ，加密 $c = m^e \bmod N$ ，解密为

$$c^d = m^{ed} = m^{1+k\varphi(N)} \equiv m \pmod{N}, \quad (\text{B.3})$$

其中最后一步来自欧拉定理（对与 N 不互素的情形可用中国剩余定理分别证明）。只要不知道 p, q ，经典攻击者难以获得 $\varphi(N)$ 和 d 。

Shor 算法不直接“猜测私钥”，而是对随机 a 寻找最小正整数 r 使 $a^r \equiv 1 \pmod{N}$ 。若 r 为偶数，则

$$(a^{r/2} - 1)(a^{r/2} + 1) \equiv 0 \pmod{N}.$$

在非平凡条件下， $\gcd(a^{r/2} \pm 1, N)$ 给出因子。量子傅里叶变换使阶寻找可在多项式资源下完成，这正是 RSA 安全假设被结构性改变的原因。

B.2 Grover 振幅放大的简化推导

设搜索空间有 N 个元素，其中一个目标态 $|w\rangle$ 。均匀叠加态可写为

$$|s\rangle = \frac{1}{\sqrt{N}}|w\rangle + \sqrt{\frac{N-1}{N}}|w^\perp\rangle. \quad (\text{B.4})$$

令 $\sin \theta = 1/\sqrt{N}$ 。一次 Grover 迭代由目标相位翻转和关于 $|s\rangle$ 的反射组成，在二维子空间内把状态向 $|w\rangle$ 旋转约 2θ 。执行 t 次后，成功振幅约为

$$\sin((2t+1)\theta). \quad (\text{B.5})$$

当 $(2t+1)\theta \approx \pi/2$ 时成功概率最大，因此

$$t \approx \frac{\pi}{4}\sqrt{N}. \quad (\text{B.6})$$

这是平方根级查询复杂度的来源，但实际门数、纠错和并行成本可能远大于查询次数本身。

B.3 LWE 解密正确性的直观推导

考虑简化公钥关系 $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \pmod{q}$ 。发送方选择短随机向量 $\mathbf{r}$ ，形成

$$\mathbf{u} = \mathbf{A}^\top \mathbf{r} + \mathbf{e}_1, \quad (\text{B.7})$$

$$v = \mathbf{b}^\top \mathbf{r} + e_2 + \lfloor q/2 \rfloor m, \quad (\text{B.8})$$

其中 $m \in \{0, 1\}$ 。接收方计算

$$v - \mathbf{s}^\top \mathbf{u} = (\mathbf{A}\mathbf{s} + \mathbf{e})^\top \mathbf{r} + e_2 - \mathbf{s}^\top (\mathbf{A}^\top \mathbf{r} + \mathbf{e}_1) + \lfloor q/2 \rfloor m \quad (\text{B.9})$$

$$= \mathbf{e}^\top \mathbf{r} + e_2 - \mathbf{s}^\top \mathbf{e}_1 + \lfloor q/2 \rfloor m \pmod{q}. \quad (\text{B.10})$$

若总误差绝对值远小于 $q/4$ ，结果接近 0 或 $q/2$ ，从而恢复 m 。安全性来自攻击者无法在未知短秘密和噪声下从公开样本恢复 $\mathbf{s}$ ；正确性来自合法运算后噪声仍在解码阈值内。真实 ML-KEM 使用模格、多项式、压缩和规范化转换，不能由该简化式自行实现。

B.4 KEM 安全：IND-CPA 与 IND-CCA

不可区分性游戏用于表达“攻击者不能区分真实秘密与随机值”。在 IND-CPA 游戏中，攻击者可获得公钥并调用封装/加密能力；挑战阶段收到真实或随机结果，优势定义为

$$\text{Adv} = \left| \Pr[b' = b] - \frac{1}{2} \right|. \quad (\text{B.11})$$

若对所有可行攻击者该优势可忽略，则方案具有选择明文安全。IND-CCA 游戏进一步给攻击者解封装/解密查询能力，但禁止直接查询挑战密文。真实协议会接收攻击者构造的报文，因此 KEM 通常要求 IND-CCA 级安全。

标准 KEM 通过经证明的转换把较基础的加密原语提升到 CCA 安全。实现必须严格执行重新加密检查、密文比较和失败秘密生成；若对无效密文返回可区分错误或时间差，数学证明的前提会被破坏。

B.5 签名正确性、不可伪造与拒绝采样

数字签名要求

$$\Pr[\text{Verify}(pk, m, \text{Sign}(sk, m)) = 1] \approx 1. \quad (\text{B.12})$$

安全目标通常是自适应选择消息攻击下的存在性不可伪造：攻击者可以请求多个消息的签名，但仍难以为一个未签过的新消息产生有效签名。

格签名中的候选值常与秘密量相加。若直接输出，其分布可能泄露私钥信息。拒绝采样通过只接受满足特定分布或范数界限的候选值，使最终签名分布基本独立于秘密。实现因此要保护随机采样、拒绝次数和时间行为，并遵守标准规定的界限与编码。

B.6 混合密钥组合的安全条件

若传统机制产生 K_1 ，PQC 机制产生 K_2 ，不能简单截取或异或而不分析上下文。推荐由标准协议定义的提取/扩展函数组合：

$$K = \text{HKDF-Extract}(\text{salt}, K_1 \parallel K_2), \quad (\text{B.13})$$

并在后续派生中绑定协议、角色、算法标识和握手转录。组合设计希望在至少一个组成机制安全时仍保持目标性质，但这一结论依赖具体构造、输入独立性、失败处理和认证方式，不能从公式外观自动推出。

启动与供应商问卷

C.1 内部启动问卷

1. 哪些业务数据需要保密超过 5 年、10 年或更久？哪些签名必须长期有效？
2. 哪些外部接口、文件传输、备份或云服务可能使密文被长期收集？
3. 哪些系统使用 RSA、DH、ECDH、DSA 或 ECDSA？来源证据是什么？
4. 哪些证书、密钥或密码调用由 HSM/KMS 托管，哪些嵌入应用或设备？
5. 哪些关键流程依赖同一证书机构、网关、核心供应商或硬件设备？
6. 现有测试环境能否复制真实对端、峰值负载、灾备和异常情况？
7. 新系统是否经过密码架构审查，是否禁止新增不可替换依赖？
8. 谁批准算法目录、风险例外、生产切换和旧机制停用？

C.2 供应商问卷

1. 当前产品各版本使用哪些算法、协议、证书和密码库？
2. 是否支持 ML-KEM、ML-DSA、SLH-DSA 或所在地正式 PQC 标准？具体版本与发布日期是什么？
3. 是否支持标准化混合 TLS/密钥协商？与哪些客户端、HSM、KMS 和网关完成互操作？
4. 密钥、密文、签名和证书大小会对容量、网络、数据库和设备产生什么影响？
5. 算法是否可配置和替换？如何防止降级，如何记录实际协商？
6. 如何处理标准勘误、实现漏洞、侧信道和紧急算法撤回？
7. 升级是否需要硬件更换、停机、数据迁移或许可证变更？
8. 是否提供测试环境、测试向量、证据、技术支持和退出/数据导出能力？

CBOM 字段模板

字段组	建议字段	填写说明
标识	记录 ID、发现日期、来源、环境	唯一编号；注明生产/灾备/测试及自动或人工来源
业务	流程、服务、责任人、关键等级	对应业务目录和业务影响分析
数据	分类、保密期、签名期、留存期、所在地	区分机密性、完整性、真实性和法律期限
系统	应用、组件、主机/容器、接口、对端	记录版本和部署位置，关联资产管理编号
算法	功能、算法、参数、协议、密码库版本	区分密钥建立、签名、对称加密、哈希和随机数
密钥证书	密钥 ID、证书链、HSM/KMS、轮换、有效期	不在 CBOM 存储私钥或共享秘密
依赖	上下游、网关、PKI、硬件、供应商	标识共同依赖和迁移先后顺序
风险	HNDL、暴露、影响、脆弱性、迁移难度、评分	保留输入值、模型版本和人工调整理由
计划	目标机制、波次、负责人、日期、阻塞	关联项目、工单、预算和供应商里程碑
验证	用例、结果、缺陷、签署、证据索引	记录测试环境和标准/软件版本
状态	传统/混合/PQC 优先/停用/例外	状态变更必须带日期、批准人和证据

实施与验收检查清单

E.1 路线图批准前

- ☐ 高级管理层发起人、项目负责人和跨部门责任已明确。
- ☐ 本地法律、监管、密码标准和数据要求已形成适用性说明。
- ☐ 关键业务、长期敏感数据和外部供应商已进入初始范围。
- ☐ CBOM 字段、发现方法、质量指标和责任人已批准。
- ☐ 关键流程与完整迁移分别设定目标日期。
- ☐ 多年预算、技能、环境和供应商测试窗口已评估。

E.2 试点进入生产前

- ☐ 算法、参数、标准、协议、软件和固件版本已批准。
- ☐ 功能、互操作、峰值容量、灾备和长期验证已测试。
- ☐ 六类扰动、降级防护、安全回退或失败关闭已经演练。
- ☐ 高危缺陷清零，其余缺陷有责任人和关闭日期。
- ☐ 遥测、告警、工单和运营手册已经接入。
- ☐ 业务、安全、技术、风险和变更管理完成签署。

E.3 标记“完成迁移”前

- ☐ 生产观察期达标，实际协商与批准策略一致。
- ☐ 所有上下游、灾备、备份和第三方依赖已确认。
- ☐ 旧密钥、证书、代码路径和配置已停用或进入限时例外。
- ☐ CBOM、依赖图、风险评分和供应商状态已更新。
- ☐ 证据包完整、可检索并满足留存要求。
- ☐ 业务责任人确认风险下降与服务水平符合预期。
- ☐ 运营责任人、资产更新触发条件、算法生命周期和复测安排已确认。
- ☐ 持续维护合同或内部服务安排明确响应、证据保管及退出要求。

标准与监管资料快照

本快照以 2026 年 10 月 1 日为基准；正式实施前应从发布机构核对最新版本和勘误。

表 F.1: 核心资料及实施用途

资料	状态/主题	实施用途
FINMA Guidance 05/2026	2026 年 7 月监管通告	战略、路线图、清单、关键数据、密码敏捷和第三方治理
NCSC PQC 迁移指导	2025 年 3 月；英国参考时间表	发现评估、优先迁移、业务连续性 & 排期校准
BIS Project Leap 第二阶段	2025 年 12 月；支付系统测试报告	签名迁移、互操作、性能与试点边界
NIST FIPS 203	ML-KEM 正式标准	密钥封装、参数和合规实现基线
NIST FIPS 204	ML-DSA 正式标准	通用数字签名基线
NIST FIPS 205	SLH-DSA 正式标准	哈希签名和算法多样性基线
NIST SP 800-227	KEM 使用建议	KEM 接口、使用与安全考虑
IETF RFC 10024	TLS 1.3 PQ/传统混合密钥协商	混合 TLS 组合和互操作依据
NIST NCCoE SP 1800-38 草案	密码发现与 PQC 迁移实践	清单、工具、测试和迁移方法
CISA/NSA/NIST Quantum-Readiness	组织量子准备建议	路线图、清单、供应链和迁移准备
中国密码与金融数据规则	《密码法》、商用密码及金融数据安全制度	中国境内本地适用性、产品服务和验收约束

参考文献

- [1] FINMA. [Guidance 05/2026: Cyber risks associated with quantum computing](#). 2026.
- [2] NCSC. [Timelines for migration to post-quantum cryptography](#). 20 March 2025. 英国实施参考。
- [3] BIS Innovation Hub. [Project Leap: Quantum-proofing payment systems, Phase 2](#). 11 December 2025. 金融场景测试报告。
- [4] e23. [The Great Cryptographic Reset: The Rise of Quantum Safe Financial Infrastructure](#). 19 May 2026. 企业观点文章；持续治理参考。
- [5] NIST. [FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard](#). 2024.
- [6] NIST. [FIPS 204: Module-Lattice-Based Digital Signature Standard](#). 2024.
- [7] NIST. [FIPS 205: Stateless Hash-Based Digital Signature Standard](#). 2024.
- [8] NIST. [SP 800-227: Recommendations for Key-Encapsulation Mechanisms](#). 2025.
- [9] IETF. [RFC 10024: Post-Quantum Traditional Hybrid Key Agreement Mechanisms for TLS 1.3](#). 2026.
- [10] NIST NCCoE. [Migration to Post-Quantum Cryptography Project and SP 1800-38 Drafts](#). Current project materials.
- [11] CISA, NSA and NIST. [Quantum-Readiness: Migration to Post-Quantum Cryptography](#). 2023.
- [12] ETSI. [TR 103 619: Migration Strategies and Recommendations to Quantum Safe Schemes](#). 2020.
- [13] Peter W. Shor. [Algorithms for Quantum Computation: Discrete Logarithms and Factoring](#). 1994.
- [14] Lov K. Grover. [A Fast Quantum Mechanical Algorithm for Database Search](#). 1996.
- [15] NIST. [Post-Quantum Cryptography: Frequently Asked Questions](#), 关于 Grover 算法与 AES 密钥长度的说明。
- [16] Oded Regev. [On Lattices, Learning with Errors, Random Linear Codes, and Cryptography](#). 2009.
- [17] Chris Peikert. [A Decade of Lattice Cryptography](#). 2016.
- [18] Michele Mosca and Marco Piani. [Quantum Threat Timeline Report](#). Global Risk Institute, 2018.
- [19] 国家密码管理局. [中华人民共和国密码法](#).
- [20] 国家市场监督管理总局、国家密码管理局. [商用密码管理条例](#). 2023.
- [21] 国家密码管理局等. [关键信息基础设施商用密码使用管理规定](#). 2025.
- [22] 国家金融监督管理总局. [银行保险机构数据安全管理办法](#). 2024.

从路线图到可验证的 量子安全迁移能力

看得见资产，解释得清风险，
控制得住切换，证明得了结果。

龚晖 | UCL Institute of Finance & Technology

版本 1.4 | 2026 年 10 月 1 日 | 公开发布稿

