DNV
CYBER

Practical PQC Migration

Part 3 – Planning and executing migration

Tor Helge Kristiansen, DNV Cyber

28 October 2025

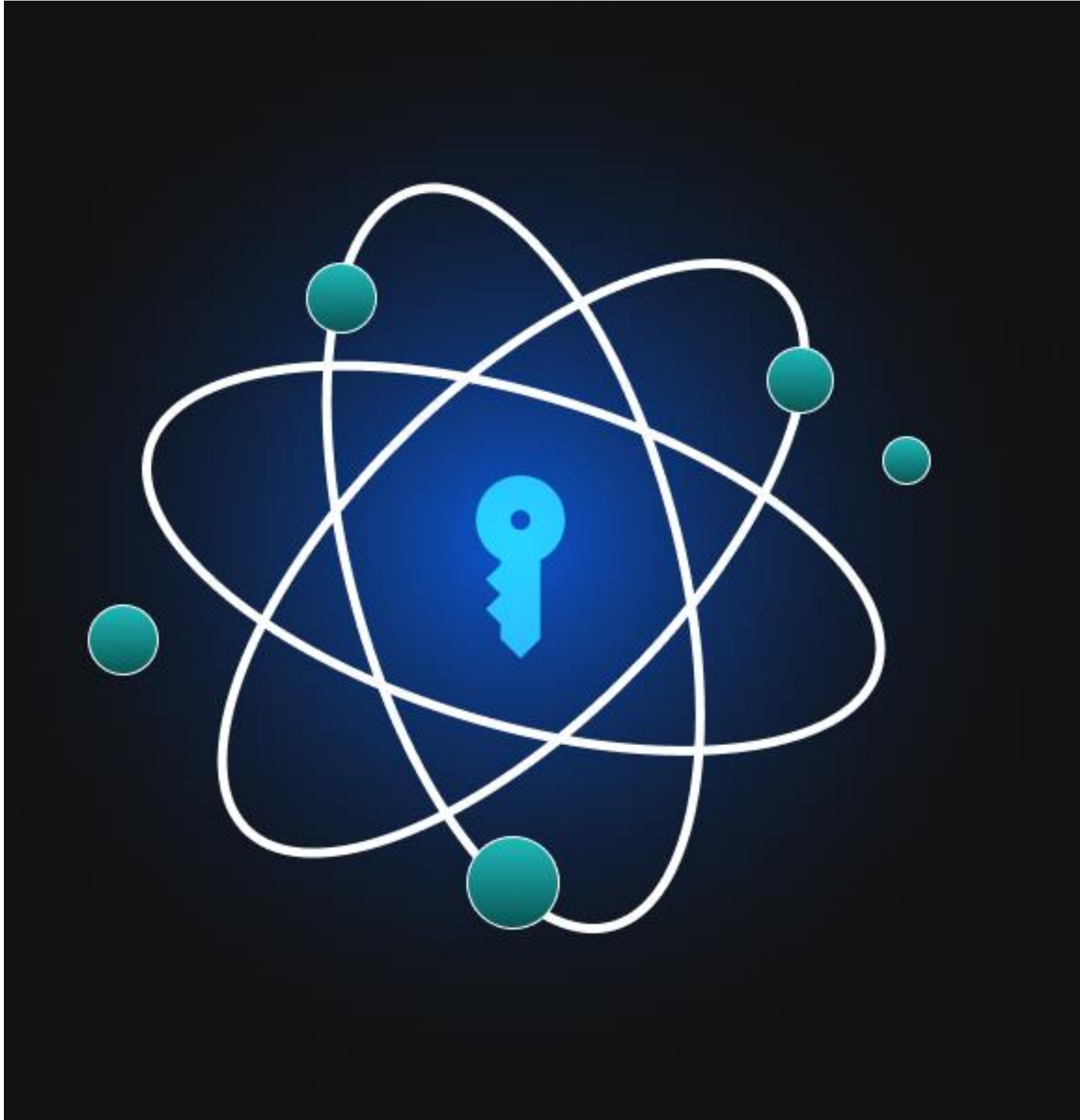
Agenda

01 Planning and Execution

02 Monitoring and Evaluation

03 PQC Migration Challenges

04 Group Exercise



The PQC Migration Roadmap provides a four-phase framework to transition to quantum-safe cryptography

Obtaining a clear overview of the organization's PQC migration objectives	**Gathering a comprehensive understanding of the organization's cryptographic landscape**	**Collaborating with external system vendors and internal system owners to ensure that post-quantum solutions are acquired or developed and implemented effectively**	**Tracking progress against defined goals and establishing a process for ongoing reassessment of cryptographic security as quantum capabilities evolve**

DNV CYBER

Planning and Execution

DNV
CYBER

Practical PQC migration

Obtaining a clear overview of the organization's PQC migration objectives	Gathering a comprehensive understanding of the organization's cryptographic landscape	**Collaborating with external system vendors and internal system owners to ensure that post-quantum solutions are acquired or developed and implemented effectively**	Tracking progress against defined goals and establishing a process for ongoing reassessment of cryptographic security as quantum capabilities evolve
• Identify PQC relevancy • Assign leadership and scope • Identify and engage stakeholders	• Establish or refine data inventory • Develop an inventory of cryptographic assets • Conduct risk assessment and determine urgency	• Select PQC algorithms and solutions • Prepare migration plan • Develop (internal) or acquire (external) solutions • Perform incremental roll-out	• Validate proper implementation • Track migration progress • Review and adapt • Train and prepare staff

DNV CYBER

Identify systems to be migrated based on assessed urgency

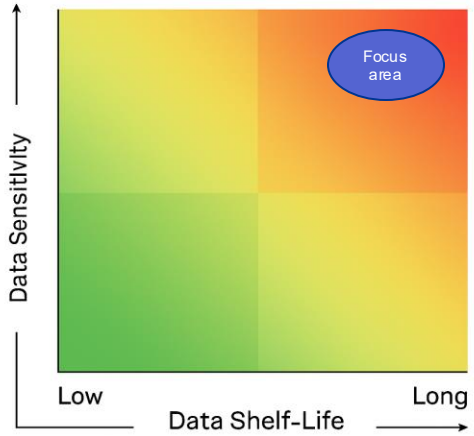
- Consider:
  - In-house developed systems
  - COTS products
  - Cloud services / SaaS
  - Legacy infrastructure
  - Partner APIs and integrations

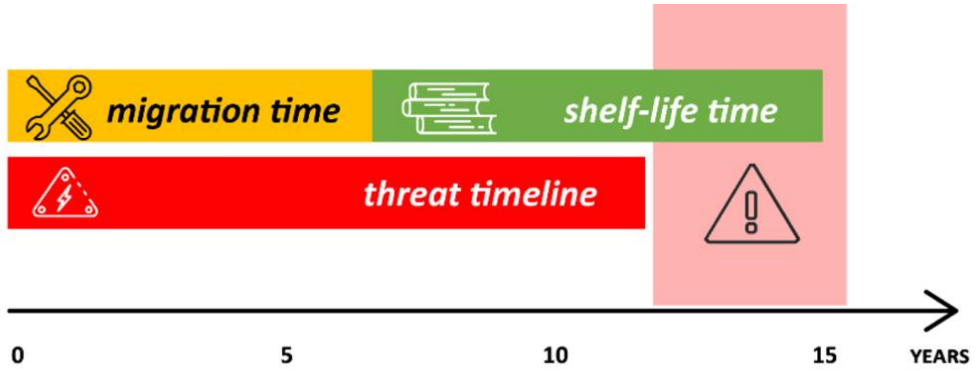
- Challenges to beware of:
  - Shadow IT
  - Complex interdependencies
  - Proprietary and undocumented cryptography

- Build an inventory of systems to be migrated, documenting
  - Which system
  - Purpose
  - Who has provided that system
  - What data they protect
  - Shelf-life of protected data
  - Cryptographic algorithms and key lengths
  - Interdependencies
  - Planned decommissioning or replacement

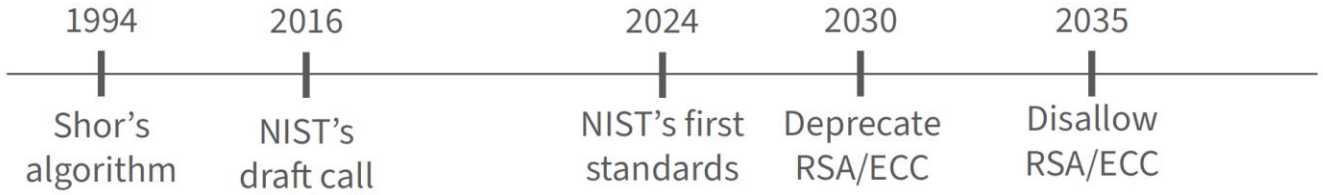
Prioritize systems for migration

- Focus on systems processing long-lived, high-value, externally exposed data





- Consider NIST/NCSC timelines or other regulatory requirements



DNV CYBER

Determine migration strategy and identify solutions

Conclude on migration strategy

- Decommission
- Replace
- Upgrade
- Isolate or protect

Based on NIST and industry guidance, choose approved or high-confidence PQC algorithms

- More in next session

Determine which solutions can be **sourced** from vendors or **developed** in-house

Determine need for **hybrid** and/or **agile cryptographic** implementation to support transition to PQC

Determine need for **hardware** replacement and upgrades

Determine need for intermediate **short-term measures** to reduce current risk level

DNV CYBER

Hybrid cryptography

- Refers to running both classical and post-quantum algorithms simultaneously
  - For **key exchange**: both classical and PQC keys are exchanged and combined to derive the final session key
  - For **signatures**: both classical and PQC signatures may be attached and verified
- Enables smooth transition and backwards compatibility
- Introduces significant computational overhead and key management complexities

Cryptographic agility

- Refers to the ability of systems to quickly and easily switch between cryptographic algorithms – without major redesign or disruption
- Crucial for managing the transition period by enabling
  - Swapping of algorithms
  - Adding support for new standards
  - Using hybrid schemes
- Supports adaptation to future cryptographic shifts (e.g. unforeseen vulnerabilities or new algorithms)

DNV CYBER

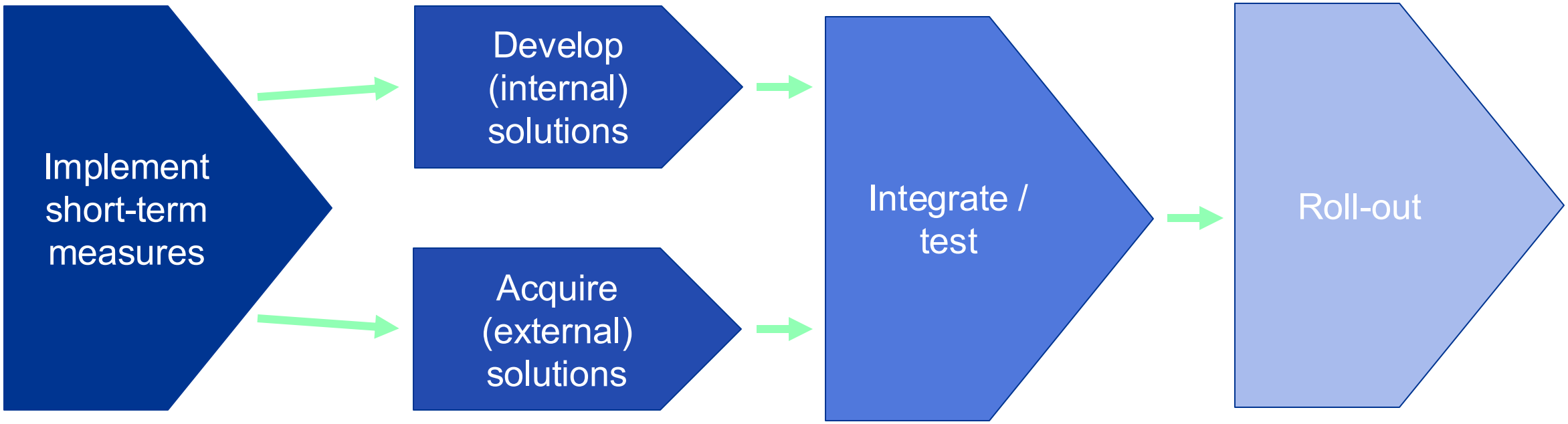
Establish a realistic project timeline and budget covering both development and deployment

- Internal preparations
- In-house development
- Working with vendors and system integrators
- Deployment strategies (test labs, staged roll-out, fallback options, etc.)
- Software and hardware updates
- Integration and testing
- Documentation and training

- Identify required internal and external stakeholders and resources for the entire transition

DNV CYBER

Ensure that post-quantum solutions are acquired or developed and implemented effectively



DNV CYBER

Implement intermediate short-term measures to mitigate “harvest now, decrypt later” threats

Improve cryptographic protection:

- Encrypt long-time data with hybrid (classical + PQC) algorithms
- Improve security of current implementation:
  - Increase key rotation frequency (shorten certificate/key lifetimes)
  - Increase key sizes
  - Select most secure algorithm available
  - Enable modern protocols (e.g. TLS 1.3) and remove old protocols (e.g. TLS 1.2)
- Enhance data protection (e.g. apply disk encryption, or VPN around sensitive traffic)

Improve cyber protection of sensitive systems:

- Implement mitigating actions identified through risk assessments
- Segment and isolate sensitive data flows
- Implement enhanced monitoring
- Strengthen access control and physical protection of key material and backups

Review data retention policy:

- Delete data that is no longer required by business, legal, or regulatory obligations

DNV CYBER

Develop quantum-safe crypto for in-house developed solutions

- Select PQC algorithms and develop necessary applications, libraries, etc.

- Best practices for PQC development:
  - Involve development, security, and IT operations (DevSecOps)
  - Use carefully vetted 3rd party libraries (e.g. OpenSSL) to incorporate PQC
  - Enforce crypto-agility in new designs
  - Include code reviews by cryptography experts if possible
  - In parallel with software development, develop the operational procedures

- **Note**: PQC standards development is still early, so be prepared for multiple iterations as standards evolve

Proactively engage vendors for acquisition of quantum-safe solutions

- Hold vendors accountable for providing quantum-safe options
- Mandate PQC compliance for future technology acquisitions

- Actively engage vendors for updated versions or replacement systems:
  - Agree algorithms, features, and delivery dates
  - Collaborate with vendors to understand interdependencies
  - Audit and track vendor progress
  - Agree support for integration and roll-out

- Replace systems when upgrade is not possible

Use PQC migration as an opportunity to improve cyber resilience

Modernize the entire cryptographic estate

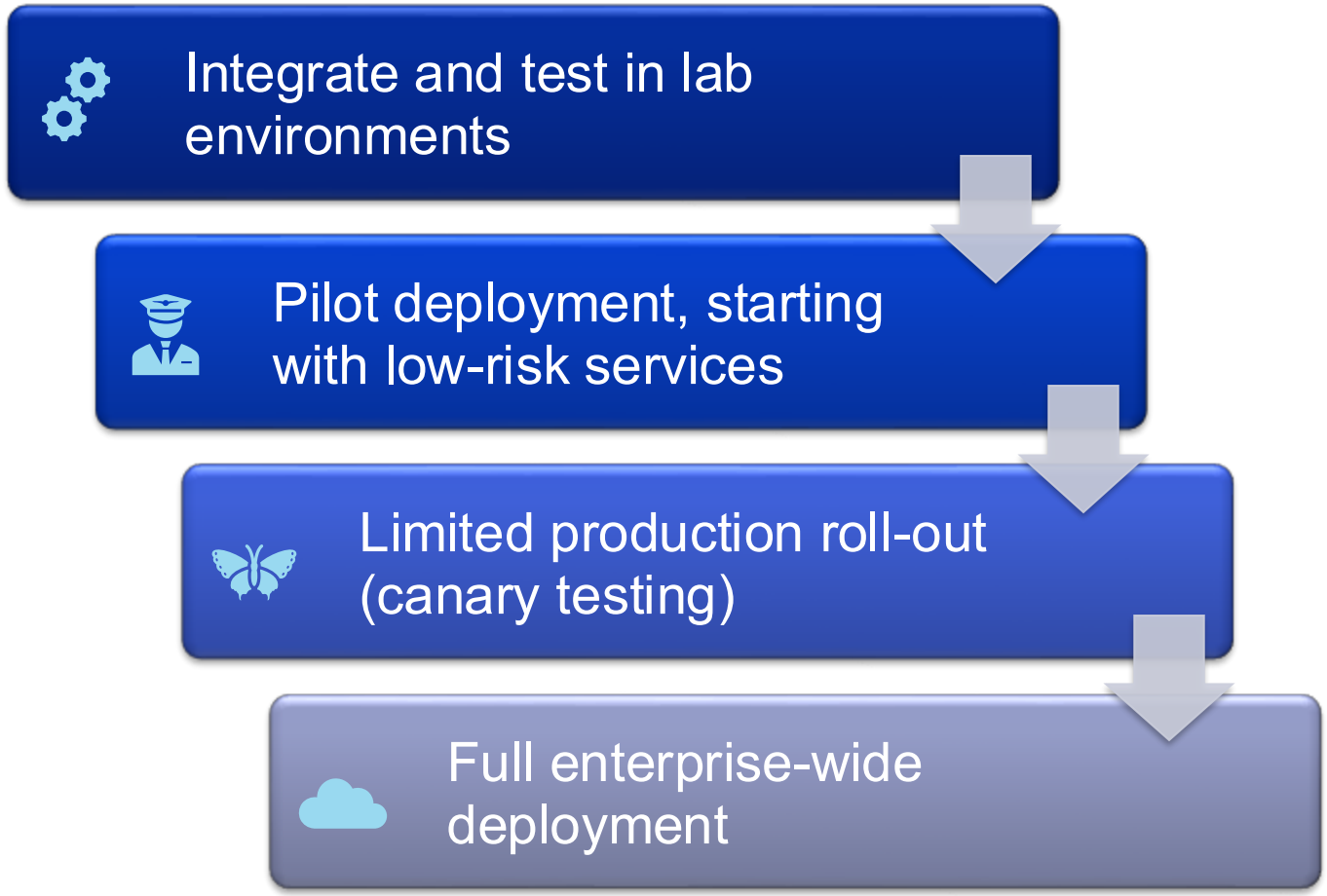
Improve key management practices

Enhance crypto-agility

Address underlying cyber weaknesses

DNV CYBER

Perform incremental-roll out to minimize risk of operational disruptions



- Each deployment step should include monitoring for performance impact
- Determine if existing hardware need firmware for module upgrades
- Verify interoperability with existing systems and interdependent systems
- Ensure robust change control and rollback plans

DNV CYBER

Monitoring and Evaluation

DNV
CYBER

Practical PQC migration

Obtaining a clear overview of the organization's PQC migration objectives	Gathering a comprehensive understanding of the organization's cryptographic landscape	Collaborating with external system vendors and internal system owners to ensure that post-quantum solutions are acquired or developed and implemented effectively	Tracking progress against defined goals and establishing a process for ongoing reassessment of cryptographic security as quantum capabilities evolve
• Identify PQC relevancy • Assign leadership and scope • Identify and engage stakeholders	• Establish or refine data inventory • Develop an inventory of cryptographic assets • Conduct risk assessment and determine urgency	• Select PQC algorithms and solutions • Prepare migration plan • Develop (internal) or acquire (external) solutions • Perform incremental roll-out	• Validate proper implementation • Track migration progress • Review and adapt • Train and prepare staff

DNV CYBER

Perform continuously monitoring of progress and evaluation of need for adjustments

Validate proper implementation

- Functional testing
- Performance testing
- Alignment with industry standards
- Backwards and forwards compatibility

Track migration progress

- Establish KPIs to measure migration success
- Use dashboard and continuous scans to verify rollouts

Review and adapt

- Establish a framework for continuous evaluation of cryptographic security as quantum capabilities evolve
- Monitor for changes in algorithms, attacks, standards, etc.
- Assess and handle migration risks

Train and prepare staff

- Assess workforce needs
- Update documentation and procedures
- Perform training as required

DNV CYBER

PQC Migration Challenges

PQC migration challenges and mitigation strategies

Challenge	Explanation	Mitigation Strategy
"Harvest Now, Decrypt Later" Threat	Adversaries collecting encrypted data today for future decryption.	Prioritize migration of key establishment algorithms (ML-KEM) for long-lived, sensitive data. Implement short-term measures like enhanced monitoring and data retention policy review.
Increased Key/Signature Sizes & Computational Overhead	PQC algorithms require more processing power, memory, and bandwidth.	Conduct performance testing and capacity planning. Evaluate hardware upgrades. Optimize implementations.
Complex Key Management	Managing both classical and PQC keys, especially in hybrid modes.	Establish robust, agile key management infrastructure. Leverage modern PKI solutions capable of supporting PQC certificates.
Supply Chain Dependencies	Reliance on vendors for PQC-compliant software/hardware updates.	Proactive vendor engagement. Mandate PQC compliance in procurement. Develop retrofit strategies for legacy systems.
Legacy Systems & Technical Debt	Deeply embedded, difficult-to-update cryptographic implementations.	Prioritize high-risk legacy systems. Plan for phased upgrades or replacements. Utilize crypto-agility principles where possible.
Organizational Alignment & Resource Allocation	PQC migration requires significant cross-functional buy-in and budget.	Appoint a dedicated migration lead. Develop strategic messaging with clear ROI. Engage all key stakeholders early and continuously.

Group exercise

DNV
CYBER

Group discussion – applying the framework to a financial institution

- **Scenario**: the hypothetical financial institution has decided to start PQC migration for the online banking platform (“nettbank”), and you are now working on the detailed migration strategy
- **Questions for discussion**:
  - What specific short-term measures can be implemented within the next 6-12 months to mitigate "harvest now, decrypt later" risks, prior to full PQC deployment?
  - What steps should be taken to migrate an in-house developed login authentication system to use PQC?
  - How would you engage a key vendor (e.g., a mobile app provider) in the PQC migration?
  - What risks do you foresee if hybrid cryptography is deployed? How can they be mitigated?
  - How would you structure a phased roll-out of the online banking platform to minimize disruption?
  - What key metrics/KPIs should be tracked to assess progress and effectiveness of the migration?

DNV CYBER

Thank you

Tor.Helge.Kristiansen@dnv.com

www.dnv.com/cyber

DNV CYBER