



LAPORAN PELAKSANAAN AKTIVITI PELAJAR INTERN

PUSAT TEKNOLOGI DAN PENGURUSAN KRIPTOLOGI MALAYSIA (PTPKM)

Bagi Bulan April 2025

NAMA:	Nur Hanie Elvira binti Hamran
NO. KAD PENGENALAN:	011002-14-0976
UNIVERSITI:	Universiti Putra Malaysia (UPM)
PROGRAM IJAZAH:	Bachelor Sains Matematik dengan Kepujian
BAHAGIAN PENEMPATAN:	Bahagian Polisi, Perundangan dan Kesedaran

1. TUGASAN

1. Pembentangan tentang PQC dan garis panduan migrasi kepada PQC oleh negara lain.
2. Pembentangan tentang MySeal, NCII, dan *risk management*.
3. Penyediaan templat dokumen polisi/prosedur.
4. Penyediaan dokumen polisi *disaster recovery and business continuity plan*.
5. Penyediaan dokumen polisi *code review/secure coding policy*.
6. Penambahbaikan dokumen *disaster recovery and business continuity plan*.
7. Penambahbaikan dokumen polisi *code review/secure coding policy*.
8. Penyediaan laporan isu tadbir urus bahagian polisi, perundangan, dan kesedaran.

2. OBJEKTIF

1. Menambah pengetahuan tentang kriptografi dan PQC.
2. Menambah pengetahuan tentang garis panduan migrasi PQC.
3. Menghasilkan templat dokumen prosedur kawalan untuk PTPKM.
4. Menghasilkan draf dokumen *disaster recovery and business continuity plan*.
5. Menghasilkan draf dokumen polisi *code review/secure coding policy*.
6. Melaporkan sebarang isu tadbir urus dan progres kerja.

3. HASIL TUGASAN & STATUS PELAKSANAAN TUGASAN:

1. Slaid pembentangan PQC dan Garis Panduan Migrasi PQC. [Selesai - Rujuk Lampiran 1 dan 2]
2. Slaid pembentangan *risk management*. [Selesai - Rujuk Lampiran 3-6]
3. Dokumen polisi *disaster recovery and business continuity plan*.
[sedang disemak]
4. Dokumen *code review/secure coding policy*. [sedang disemak]
5. Laporan isu tadbir urus bahagian polisi, perundangan, dan kesedaran.
[sedang disemak]

*Sila sertakan lampiran berkaitan jika ada

Disediakan oleh:

Hanie

.....
Nama: Nur Hanie Elvira
 binti Hamran
Tarikh: 28 April 2025

Disemak oleh:



.....
Nama: Dr. Noorul
 Halimin Mansol
Jawatan: Ketua Bahagian
 Polisi, Perundangan dan
 Kesedaran
Tarikh: 30 April 2025

Disahkan oleh:

.....
Nama:
Jawatan: <Ketua Pengarah>
Tarikh:

Type: Cryptographic algorithms that resist quantum attacks

How it works: Based on mathematical problems that quantum computers can't easily solve

Why it matters: Governments & industries are transitioning to quantum-safe encryption

PQC

Primary PQC algorithms:

- **Kyber (Encryption)** – Lattice-based encryption, replacing RSA/ECC
- **Dilithium (Signatures)** – Lattice-based digital signatures
- **SPHINCS+ (Signatures)** – Hash-based signatures
- **Falcon (Signatures)** – Alternative digital signature scheme

Main Goal:

Find encryption methods that remain secure even when large quantum computers exist.

Lampiran 1: Post-Quantum Cryptography

United Kingdom (UK)

WHO?

Government Communications Headquarters (GCHQ)

WHAT?

- Assessing Quantum Threats
- Providing PQC Roadmaps & Guidelines
- Selecting & Recommending PQC Algorithms
- Encouraging Industry & Government Adoption
- Ensuring Smooth Transition

HOW?

National Cyber Security Centre (NCSC)

WHEN?

- By 2028: Identify services that require upgrades.
- By 2031: Prioritize and implement critical overhauls.
- By 2035: Complete the migration to new encryption systems.

Lampiran 2: Garis Panduan Migrasi UK

RISK MANAGEMENT

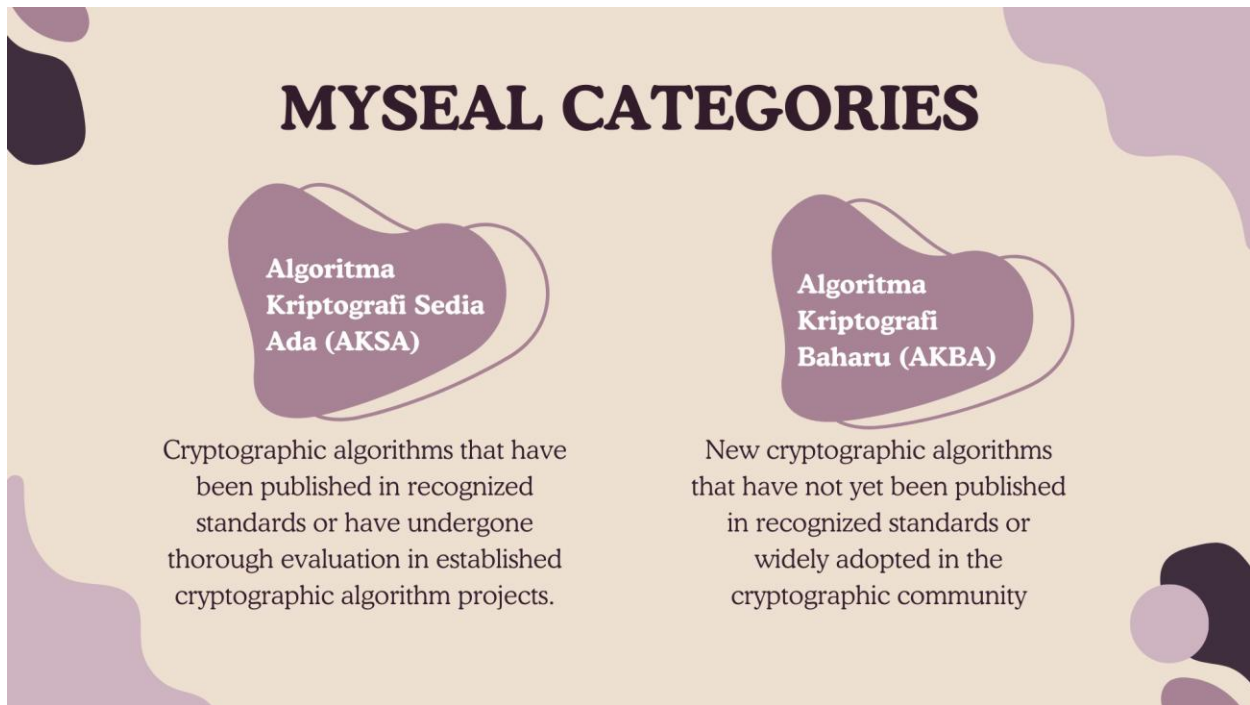
- Process of identifying, assessing, and controlling risks that may affect an organization's ability to achieve its objectives.
- Determine the impact and possibility of risks, creating plans to reduce harm, and keeping an eye on how well measures are working.
- To minimize the potential negative impacts of risks while maximizing the opportunities.
- Critical for organizations across industries to protect assets, reputation, and growth potential.

Lampiran 3: Pengurusan Risiko

POTENTIAL RISKS IF PQC FAILS

Operational Risk	Business Risk	Technical Risk	Financial Risk
Sensitive data breach	Loss of user trust	Algorithm weaknesses	Recovery & data remediation costs
Service disruption	Legal & compliance implication	Dependence on legacy system	Investment losses
Integration errors	Reputation damage	Maintenance & replacement costs	Lawsuits & insurance claims

Lampiran 4: Potensi Risiko Jika PQC Gagal



Lampiran 5: Kategori MYSEAL



Lampiran 6: Sektor NCII di Malaysia