LAPORAN ISU TADBIR URUS KRIPTOGRAFI NEGARA

PUSAT TEKNOLOGI DAN PENGURUSAN KRIPTOLOGI MALAYSIA

Objektif:

1. Mengenal pasti isu-isu utama termasuk kelemahan atau jurang dalam Tadbir Urus Kriptografi di peringkat PTPKM atau negara.
2. Mengumpul maklumat dan mengenal pasti mekanisme pelaporan dan komunikasi Isu tadbir urus yang melibatkan semua bahagian di bawah PTPKM.
3. Mengenalpasti isu-isu tadbir urus yang berkaitan dengan pembangunan akta dan garis panduan yang berkaitan dengan pembangunan dan penggunaan teknologi kriptografi negara.
4. Mengemukakan cadangan dan langkah-langkah penambahbaikan bagi menangani isu-isu berkaitan tadbir urus kriptografi negara.

Mengenal pasti isu-isu utama termasuk kelemahan atau jurang dalam Tadbir Urus Kriptografi di peringkat PTPKM atau negara.

Peringkat PTPKM

1. Kakitangan sukar untuk mengakses laporan/kajian yang dilakukan oleh bahagian lain.
2. Kekurangan pengetahuan dan kemahiran berkenaan kriptografi dikalangan pelajar latihan industri.
3. Kekurangan sumber dan kemudahan yang diperlukan seperti *Microsoft*, *LaTex*, dan bahan rujukan berbayar.

Peringkat Negara

1. Dasar dan prosedur sedia ada tidak sepenuhnya selaras dengan piawaian antarabangsa seperti ISO/IEC 27001 dan NIST.
2. Sistem dan peralatan pengurusan kriptografi belum mencapai tahap keupayaan yang menyokong teknologi terkini seperti algoritma pasca-kuantum.
3. Undang-undang berkaitan penggunaan dan kawalan teknologi kriptografi tidak lengkap, tidak terkini, atau tidak dikuatkuasakan dengan berkesan.
4. Tiada mekanisme tetap untuk koordinasi berkala atau saluran perkongsian maklumat antara agensi berkaitan kriptografi.

<u>Mengumpul maklumat dan mengenal pasti mekanisme pelaporan dan komunikasi isu tadbir urus yang melibatkan semua bahagian di bawah PTPKM.</u>

Kaedah Pelaksanaan:

1. Temu bual bersama wakil setiap bahagian.
2. Analisis dokumen dalaman seperti SOP, carta organisasi dan laporan audit.
3. Soal selidik ringkas untuk menilai kefahaman dan amalan pelaporan.
4. Pemerhatian terhadap proses pelaporan semasa.

Struktur Pelaporan:

1. **Pegawai Pelapor:** Semua pegawai dibenarkan melaporkan isu tadbir urus tanpa halangan.
2. **Peringkat Pertama:** Ketua Unit/Bahagian menyemak dan mengambil tindakan awal.
3. **Peringkat Kedua:** Isu dilaporkan kepada Jawatankuasa Tadbir Urus/JK Risiko Organisasi.
4. **Peringkat Ketiga:** Jika isu bersifat besar/kritikal, lapor terus ke Pengurusan Tertinggi atau Lembaga Pengarah.

Bahagian Terlibat:

1. Bahagian Simetrik
2. Bahagian Asimetrik
3. Bahagian Integrasi Teknologi
4. Bahagian Migrasi PQC
5. Bahagian Polisi, Perundangan, dan Kesedaran

Mengenalpasti isu-isu tadbir urus yang berkaitan dengan pembangunan akta dan garis panduan yang berkaitan dengan pembangunan dan penggunaan teknologi kriptografi negara.

1. Tiada undang-undang khusus yang mentakrifkan skop, tanggungjawab, dan kuasa berkaitan pembangunan serta penggunaan teknologi kriptografi di peringkat nasional.
2. Tiada dokumen rasmi yang memperincikan penggunaan algoritma, pengurusan kunci, kelulusan sistem kriptografi atau pengiktirafan produk.
3. Sektor awam dan swasta masih bebas menggunakan teknologi kriptografi tanpa berpandukan kepada piawaian yang diwajibkan di peringkat negara.
4. Teknologi kriptografi tempatan sukar mendapat pengiktirafan luar kerana tiada dasar standardisasi kebangsaan yang diiktiraf antarabangsa.
5. Kelewatan negara dalam membuat persediaan terhadap ancaman komputer kuantum yang boleh memecahkan kriptografi konvensional.
6. Kurangnya latihan, pendedahan, dan kefahaman di kalangan pemegang taruh mengenai pentingnya tadbir urus kriptografi.

<u>Mengemukakan cadangan dan langkah-langkah penambahbaikan bagi menangani isu-isu berkaitan tadbir urus kriptografi negara.</u>

1. **Pemantapan Kerangka Undang-undang dan Peraturan Kriptografi**
    a. Cadangan:
        i. Mengkaji semula dan mengemaskini undang-undang dan peraturan berkaitan kriptografi supaya selaras dengan perkembangan teknologi terkini, termasuk *post-quantum cryptography* (PQC).

    b. Langkah:
        i. Menubuhkan panel perundangan yang terdiri daripada pakar undang-undang, pengamal kriptografi, dan penggubal dasar untuk melakukan semakan menyeluruh terhadap perundangan sedia ada.
        ii. Menyediakan garis panduan yang jelas bagi penggunaan dan pengawalan teknologi kriptografi di sektor awam dan swasta.
        iii. Memastikan setiap teknologi kriptografi yang digunakan mematuhi standard keselamatan antarabangsa dan kebangsaan.

2. **Seragamkan Dasar dan Garis Panduan Kriptografi**
    a. Cadangan:
        i. Mengharmonikan semua dasar, garis panduan dan piawaian kriptografi merentasi agensi awam dan sektor swasta.

    b. Langkah:
        i. Audit dasar dan panduan sedia ada yang digunakan oleh agensi berkaitan keselamatan siber.
        ii. Membuat satu dokumen garis panduan kebangsaan.
        iii. Mengedarkan garis panduan melalui platform rasmi dan latihan.

3. **Pembangunan Infrastruktur dan Teknologi Kriptografi Nasional**
    a. Cadangan:

i. Memastikan negara mempunyai infrastruktur teknologi yang cukup kuat untuk menyokong penggunaan kriptografi dalam sektor kritikal.

b. Langkah:
   i. Meningkatkan penggunaan kriptografi dalam perlindungan data dan komunikasi kerajaan, termasuk penggunaan kriptografi dalam sistem pengundian, e-perkhidmatan, dan aplikasi kerajaan.
   ii. Melabur dalam pembangunan teknologi kriptografi negara dan penyelidikan tempatan untuk memastikan negara tidak bergantung sepenuhnya kepada teknologi luar.
   iii. Mewujudkan pusat data yang mempunyai perlindungan kriptografi yang tinggi, termasuk dalam sektor kewangan dan perubatan.

4. Perkasakan Mekanisme Pemantauan dan Penguatkuasaan

a. Cadangan:
   i. Mewujudkan sistem audit dan pematuhan berpusat untuk semua aplikasi kriptografi dalam sektor kerajaan.

b. Langkah:
   i. Menubuhkan mekanisme untuk mengaudit dan memantau penggunaan teknologi kriptografi secara berkala.
   ii. Membuat laporan tahunan mengenai status penggunaan dan keberkesanan teknologi kriptografi di negara ini.
   iii. Menggalakkan syarikat swasta dan badan kerajaan untuk mematuhi amalan terbaik dan melaksanakan piawaian yang ditetapkan.

5. Peningkatan Kolaborasi Antarabangsa

a. Cadangan:

i. Meningkatkan kerjasama dengan negara-negara lain dalam bidang kriptografi dan keselamatan siber untuk memastikan amalan terbaik diterapkan.

b. Langkah:
   i. Menjalin perkongsian maklumat dengan negara-negara maju dalam kriptografi untuk mendapatkan pandangan tentang peraturan dan teknik terbaik yang boleh diterapkan.
   ii. Mengikuti dan menyertai perbincangan antarabangsa berkaitan dengan kriptografi dan teknologi baru seperti PQC.
   iii. Meningkatkan penyertaan dalam forum dan badan antarabangsa yang mengawal dan menetapkan piawaian kriptografi global, seperti ISO/IEC dan NIST.

6. Pengurusan Risiko Kriptografi

a. Cadangan:
   i. Menubuhkan sistem pengurusan risiko yang berkesan untuk menangani potensi ancaman atau kerentanan dalam penggunaan teknologi kriptografi.

b. Langkah:
   i. Membentuk pasukan yang khusus untuk mengenal pasti dan menilai risiko berkaitan penggunaan kriptografi, termasuk ancaman dari teknologi baru seperti *quantum computing*.
   ii. Menyediakan garis panduan untuk respons terhadap insiden keselamatan yang melibatkan kelemahan dalam sistem kriptografi.
   iii. Melakukan ujian dan penilaian sistem secara berkala untuk memastikan ketahanan dan keberkesanan algoritma kriptografi yang digunakan.

7. Peningkatan Kesedaran dan Latihan Kriptografi

a. Cadangan:

i. Menyediakan program kesedaran dan latihan berkaitan kriptografi kepada agensi kerajaan, syarikat swasta, dan masyarakat umum.

b. Langkah:
    i. Mengadakan bengkel, seminar, dan kursus berkaitan kriptografi dan keselamatan siber secara berkala untuk golongan yang terlibat.
    ii. Menyediakan platform e-pembelajaran bagi memperkenalkan dasar dan teknik terkini dalam bidang kriptografi.
    iii. Meningkatkan penglibatan institusi pengajian tinggi dalam penyelidikan dan pembangunan kriptografi untuk memastikan negara mempunyai kapasiti intelektual yang mencukupi.

Isu Tadbir Urus: PTPKM masih belum diisytiharkan secara rasmi.

Kesan:

1. Tiada nombor rujukan rasmi atau status penubuhan.
2. Sukar untuk menjalankan aktiviti rasmi antara agensi.

Cadangan: Segerakan draf rasmi dokumen penubuhan pusat.

Isu Tadbir Urus: Pelantikan rasmi pakar di PTPKM

Kesan:

1. Kekangan komitmen penuh kerana mereka masih terikat dengan tugas di agensi asal.
2. Sukar untuk membuat penugasan rasmi atau menetapkan tanggungjawab jelas.
3. Kelewatan dalam penyampaian arahan disebabkan oleh ketiadaan pegawai bertanggungjawab yang sedang bertugas di lokasi berbeza.

Cadangan: Pelantikan sementara atau penugasan rasmi dilakukan melalui surat lantikan kontrak atau Memorandum Persefahaman (MoA).

Isu Tadbir Urus: Pengurusan Tempat Kerja dan Peralatan

Kesan:

1. Tiada kemudahan rasmi seperti komputer berprestasi tinggi atau sistem dokumentasi dalaman.
2. Persekitaran kerja yang tidak kondusif menjejaskan kelancaran pelaksanaan tugasan harian.
3. Kekurangan sokongan logistik dan infrastruktur.

Cadangan:

1. Bekalkan komputer dan peralatan rasmi yang sesuai untuk aktiviti teknikal.
2.
3. Wujudkan sistem pengurusan dokumen rasmi.

Isu Tadbir Urus: Ketiadaan Standard Dalaman bagi Laporan Teknikal

Kesan:

1. Ketidakkonsistenan dari segi format, struktur kandungan, serta tahap kedalaman analisis antara laporan-laporan yang dihasilkan.
2. Menjejaskan keberkesanan penyampaian maklumat, keseragaman penilaian teknikal, dan kejelasan dapatan kepada pihak pengurusan serta pihak berkepentingan luar.

Cadangan:

1. Membangunkan dan melaksanakan satu dokumen Panduan Penyediaan Laporan Teknikal Kriptografi yang meliputi struktur standard.

2. Keperluan semakan dalaman *(peer review)* sebelum pembentangan atau pengedaran

BAHAGIAN MIGRASI PQC

Aktiviti: Pusat Teknologi dan Pengurusan Kriptologi Malaysia (PTPKM) sedang melaksanakan aktiviti penyelidikan berstruktur yang menumpukan kepada pendekatan migrasi kriptografi pasca-kuantum di negara-negara maju dan strategik seperti Jepun, United Kingdom, Amerika Syarikat, Israel, Australia, Kanada, India, Korea Selatan, dan Singapura.

Penekanan utama diberikan terhadap pengumpulan data dan analisis berkenaan strategi pelaksanaan, garis masa peralihan, pemilihan algoritma PQC yang digunakan, serta sektor keutamaan yang diberi perhatian di negara-negara tersebut. Penyelidikan ini dijalankan melalui kajian literatur terbuka, laporan rasmi yang boleh diakses awam, dan pemerhatian terhadap pendekatan dasar serta teknikal yang digunakan oleh negara-negara terbabit.

Tujuan:

1. Memahami pendekatan strategik dan teknikal yang diambil oleh negara-negara utama dalam merancang dan melaksanakan migrasi kepada algoritma PQC.
2. Mengenal pasti garis masa dan fasa peralihan yang diguna pakai bagi memastikan keselamatan kriptografi kekal relevan dalam menghadapi ancaman komputer kuantum.
3. Mengenal pasti algoritma PQC yang sedang dinilai atau diadaptasi oleh negara-negara terlibat.
4. Mengenal pasti sektor-sektor yang menjadi keutamaan dalam pelaksanaan migrasi PQC.

Isu Tadbir Urus:

1. **Kekurangan maklumat terbuka:**
   Tidak semua negara berkongsi pelan migrasi PQC secara terbuka atau menyenaraikan garis masa serta algoritma pilihan mereka. Ini menyukarkan proses perbandingan dan penyesuaian dasar tempatan.

2. **Tiada pelantikan rasmi bagi hubungan antarabangsa:**
   Ketiadaan wakil rasmi yang boleh menjalin komunikasi terus dengan agensi luar menjadikan pengumpulan maklumat teknikal sukar dan tidak formal.
3. **Ketiadaan saluran komunikasi rasmi:**
   Tiada saluran rasmi seperti alamat e-mel institusi atau pusat komunikasi menyebabkan kesukaran untuk memulakan atau mengekalkan hubungan dua hala yang sah dan konsisten.

Cadangan:

1. **Menjalin hubungan dua hala rasmi:**
   PTPKM disarankan untuk menjalinkan hubungan rasmi dengan agensi luar negara yang terlibat dalam penyelidikan dan pelaksanaan PQC melalui saluran diplomatik atau kerjasama teknikal.
2. **Permohonan maklumat melalui saluran kementerian:**
   Mengemukakan permohonan rasmi kepada kementerian yang berkaitan bagi mendapatkan akses kepada maklumat teknikal dari negara luar secara sah.

Rancangan Masa Hadapan:

1. **Sesi kesedaran dan bengkel PQC:**
   Menganjurkan sesi kesedaran dan bengkel latihan teknikal berkaitan migrasi PQC yang akan bermula seawal **Jun 2025**, dengan penglibatan sektor awam dan strategik.
2. **Penubuhan pasukan khas PQC:**
   Proses pengumpulan nama dan pelantikan anggota **pasukan khas PQC** akan dijalankan, bagi menyelaras strategi migrasi, dasar, dan pelaksanaan teknikal PQC secara berperingkat.
3. **Pembangunan dokumen rasmi pelan migrasi PQC PTPKM:**
   Dokumen pelan migrasi PQC rasmi PTPKM akan dibangunkan untuk menjadi rujukan strategik dan panduan pelaksanaan nasional, termasuk cadangan kepada agensi kerajaan berkaitan.

Aktiviti:

1. **Pembentangan Dalaman:**

   Sesi pembentangan telah diadakan secara dalaman bagi membincangkan keperluan mewujudkan satu pasukan khas *(task force)* yang berperanan khusus dalam merancang, menyelaras dan melaksanakan inisiatif migrasi PQC di peringkat organisasi. Sesi ini turut memperincikan cabaran keselamatan siber dalam era pasca-kuantum dan keperluan tindakan proaktif oleh pihak PTPKM.

2. **Pengumpulan Nama Calon Anggota:**

   Proses pengumpulan nama calon anggota pasukan khas PQC daripada setiap bahagian teknikal dan sokongan telah dijalankan. Tujuan pengumpulan ini adalah untuk memastikan kepelbagaian kepakaran dalam kalangan anggota pasukan, termasuk bidang kriptografi, keselamatan rangkaian, dasar teknologi, dan pematuhan perundangan.

Tujuan:

1. **Menubuhkan satu pasukan kerja rasmi** yang bertanggungjawab ke atas pembangunan pelan migrasi PQC PTPKM.

2. **Mewujudkan struktur penyelaras** antara bahagian-bahagian bagi memastikan pelaksanaan migrasi PQC dilaksanakan secara teratur, berfasa, dan berasaskan bukti teknikal.

Isu Tadbir Urus:

1. **Kurangnya kesedaran dalaman:**

   Terdapat jurang pemahaman dalam kalangan pegawai mengenai risiko kriptografi tradisional apabila komputer kuantum menjadi praktikal. Ini menyebabkan komitmen terhadap keperluan penubuhan pasukan khas agak rendah.

2. **Ketiadaan surat pelantikan rasmi:**

   Tanpa surat pelantikan rasmi atau pengiktirafan formal oleh pengurusan atasan, calon anggota menunjukkan kurangnya penglibatan aktif dan tiada rasa tanggungjawab yang jelas terhadap peranan dalam pasukan khas tersebut.

Cadangan:

1. **Peningkatan kesedaran strategik:**
   Menganjurkan taklimat khusus atau siri bengkel kepada semua pegawai PTPKM bagi menjelaskan kepentingan dan impak migrasi PQC serta peranan pasukan khas.
2. **Pelantikan rasmi melalui surat arahan dalaman:**
   Mengeluarkan surat pelantikan rasmi bagi setiap anggota pasukan khas yang telah dikenal pasti, dengan menyatakan mandat, tempoh pelantikan, dan tanggungjawab mereka.

BAHAGIAN INTEGRASI TEKNOLOGI

Aktiviti:

Imbasan teknologi atau infrastruktur yang digunakan oleh agensi kerajaan adalah aktiviti yang berfokus pada pemetaan dan penilaian infrastruktur teknologi yang sedang digunakan oleh agensi-agensi kerajaan di negara ini. Tujuan utama adalah untuk memahami bagaimana teknologi sedia ada berfungsi dan untuk menentukan kesesuaian dan kesiapsiagaan infrastruktur tersebut untuk mengintegrasikan penyelesaian-penyelesaian kriptografi baharu, termasuk yang berkaitan dengan kriptografi pasca-kuantum.

Tujuan:

1. Menilai tahap kesiapsiagaan teknologi semasa: Aktiviti ini akan membantu mengenal pasti sejauh mana infrastruktur dan sistem teknologi yang digunakan oleh agensi kerajaan sekarang ini dapat menampung keperluan teknologi terkini dan penyelesaian kriptografi, terutama berkaitan dengan PQC yang memerlukan keupayaan pengendalian yang tinggi.
2. Mengintegrasikan penyelesaian kriptografi baharu: Dengan kemajuan dalam bidang teknologi, khususnya dalam bidang kriptografi pasca-kuantum, adalah penting untuk memastikan bahawa agensi kerajaan dapat menyesuaikan diri dengan penyelesaian yang lebih teguh terhadap ancaman pengkomputeran kuantum.

Isu Tadbir Urus:

1. **Kekangan Akses Kepada Sistem ICT:**

   Banyak agensi kerajaan mempunyai peraturan ketat mengenai akses kepada sistem ICT mereka untuk melindungi maklumat sensitif dan menjaga keselamatan siber. Oleh itu, untuk menjalankan imbasan infrastruktur atau penilaian kerentanan mungkin sukar jika akses tidak diberikan atau terhad.

2. **Polisi dan Peraturan Dalaman Agensi Kerajaan:**

   Setiap agensi kerajaan biasanya mempunyai polisi dalaman yang mengawal segala bentuk aktiviti keselamatan, termasuk pengimbasan infrastruktur dan penilaian kerentanan. Polisi ini sering diwujudkan untuk tujuan keselamatan tetapi boleh menjadi halangan jika dilihat dari sudut kajian teknologi. Sebagai contoh, pengimbasan yang berkaitan dengan penilaian kerentanan mungkin dianggap sebagai ancaman kepada sistem sedia ada, menyebabkan pelaksanaan kegiatan ini dibatalkan atau tertunda.

Cadangan:

1. **Merancang dan Mengemukakan Permintaan Rasmi (Kebenaran Bertulis):** Sebelum menjalankan imbasan atau penilaian kerentanan, adalah perlu untuk mengemukakan permintaan rasmi kepada pihak berkuasa dalam agensi kerajaan. Permintaan ini perlu disertakan dengan penjelasan yang jelas mengenai tujuan aktiviti tersebut, manfaat jangka panjang yang boleh diperoleh, serta langkah-langkah keselamatan yang akan diambil untuk mengelakkan risiko keselamatan.
2. **Mengadakan Kerjasama Rentas Agensi:**
   Untuk memastikan kelancaran aktiviti ini, adalah disyorkan untuk menjalinkan kerjasama dengan agensi kerajaan lain atau pihak yang relevan. Dengan adanya kerjasama ini, proses permohonan kebenaran dan pelaksanaan pengimbasan dapat dimudahkan. Selain itu, ia juga membuka peluang untuk perkongsian pengetahuan dan pengalaman dalam melaksanakan aktiviti keselamatan dan teknologi.

Rancangan Masa Hadapan:

1. **Lawatan Kerja ke Secure-IC, Perancis (Julai):**
   Satu lawatan kerja ke Secure-IC di Perancis dirancang untuk sesi *knowledge transfer* yang berkaitan dengan pembangunan *secure element (platform environment)*. Lawatan ini akan memberi peluang kepada PTPKM untuk mendapatkan pengetahuan terkini mengenai keselamatan teknologi dan

cara-cara untuk memajukan elemen-elemen keselamatan dalam persekitaran teknologi kerajaan.

2. **Lawatan Kerja ke Brunei untuk Ujian Pilot ASEAN PQC (Oktober):** PTPKM merancang untuk menjalankan ujian *pilot* ASEAN PQC di Brunei. Ujian ini bertujuan untuk menguji aplikasi algoritma PQC dalam konteks ASEAN dan menilai kesesuaian teknologi tersebut untuk digunakan secara seragam di negara-negara ASEAN.

Isu Yang Mungkin Berlaku:

1. **Kesulitan Mendapatkan Kelulusan Rasmi untuk Ujian Pilot dan Lawatan Kerja Antarabangsa:**
   Menguruskan kelulusan rasmi untuk aktiviti seperti ujian pilot dan lawatan kerja antarabangsa mungkin melibatkan birokrasi yang kompleks. Hal ini boleh menyebabkan penundaan atau kesukaran dalam memastikan kelancaran perjalanan.
2. **Keterbatasan Sumber dan Logistik:**
   Aktiviti luar negara seperti lawatan kerja dan ujian pilot memerlukan peruntukan sumber yang mencukupi. Terdapat risiko masalah logistik yang boleh mengganggu kelancaran aktiviti ini, seperti isu pengangkutan, masalah kewangan, atau sumber manusia yang terhad. Oleh itu, perancangan yang teliti dari segi logistik dan sumber kewangan amat penting untuk memastikan semua aktiviti berjalan lancar.

Cadangan Penyelesaian:

1. **Sokongan dan Kerjasama Antarabangsa:** Menggalakkan kerjasama dengan agensi kerajaan di negara yang terlibat untuk memudahkan kelulusan bagi aktiviti ujian pilot dan lawatan kerja.
2. **Perancangan Logistik yang Teliti:** Menyediakan pelan logistik yang lebih terperinci, termasuk merancang peruntukan kewangan lebih awal, dan memastikan sumber yang mencukupi untuk pelaksanaan aktiviti luar negara.

BAHAGIAN ASIMETRIK

Aktiviti:

Bahagian Asimetrik telah melaksanakan aktiviti pengumpulan sijil digital X.509 daripada laman web yang dipercayai mempunyai kepentingan strategik, khususnya laman yang menggunakan domain peringkat atasan negara Malaysia (.my, .gov.my, dan sebagainya). Sehingga kini, lebih daripada 130,000 sijil X.509 telah berjaya dikumpulkan melalui kaedah automasi dan pemerhatian aktif terhadap pelayan-pelayan web awam.

Tujuan:

Tujuan utama aktiviti ini adalah untuk mengekstrak parameter awam algoritma RSA, khususnya nilai Modulus N = pq, daripada sijil-sijil X.509 yang dikumpulkan. Data ini digunakan bagi melaksanakan siri ujian keselamatan dan ketahanan kriptografi ke atas parameter RSA yang digunakan oleh laman-laman web yang dianalisis. Ujian ini penting bagi mengenal pasti sebarang kelemahan yang mungkin timbul akibat penggunaan parameter RSA yang lemah atau tidak selamat.

Isu Tadbir Urus:

1. **Kekangan masa dan tenaga kerja**, memandangkan aktiviti ini bersifat teknikal dan memerlukan pemantauan serta analisis berterusan.
2. **Kepakaran teknikal terhad**, kerana kaedah menjalankan ujian keselamatan terhadap parameter RSA memerlukan kemahiran dalam pengaturcaraan, khususnya dalam Python dan pemahaman mendalam tentang struktur sijil X.509 serta algoritma RSA.
3. **Hanya seorang pelajar industri** yang sedang menjalani latihan di Bahagian Asimetrik mempunyai kemahiran teknikal yang diperlukan untuk menjalankan ujian-ujian tersebut secara efektif.

Cadangan Penambahbaikan:

Bagi mengatasi isu kekangan tenaga pakar dan memperkukuh kapasiti dalaman bahagian, adalah dicadangkan untuk melaksanakan satu bengkel dalaman *(internal workshop)* secara ringkas. Bengkel ini akan berfungsi sebagai sesi perkongsian pengetahuan *(knowledge sharing)*, di mana kemahiran yang dimiliki oleh pelajar industri tersebut dapat dipindahkan kepada pegawai-pegawai lain di bahagian. Ini dapat meningkatkan kebolehan bahagian dalam melaksanakan analisis lanjutan secara kendiri.

Rancangan Masa Hadapan:

1. **Melanjutkan ujian keselamatan** terhadap semua parameter RSA yang telah dikumpulkan daripada sijil X.509, serta **meluaskan skop** analisis kepada algoritma kriptografi lain yang digunakan dalam sijil tersebut, seperti ECC *(Elliptic Curve Cryptography)* dan algoritma PQC *(Post-Quantum Cryptography)* pada masa hadapan.
2. **Membangunkan model keselamatan digital** khusus untuk laman web kerajaan dan organisasi strategik berasaskan kepada data yang telah dikumpulkan. Model ini boleh digunakan untuk menilai tahap kekuatan dan kesediaan kriptografi sesebuah entiti terhadap ancaman semasa dan masa hadapan.

Aktiviti: Laporan Teknikal *Homomorphic Encryption* dan Standard PQC *Algorithm*

Homomorphic Encryption dan *Post-Quantum Cryptography* (PQC) adalah topik penting dalam dunia kriptografi moden, khususnya apabila berhadapan dengan cabaran dari teknologi pengkomputeran kuantum. Laporan teknikal ini akan menjadi rujukan utama semasa lawatan rasmi delegasi PTPKM ke Perancis, di mana mungkin terdapat perbincangan lanjut mengenai aplikasi dan perkembangan teknologi tersebut di peringkat antarabangsa.

Dalam konteks Migrasi PQC yang dijadualkan bermula pada bulan Jun, laporan ini penting untuk memberi panduan mengenai teknologi yang akan digunakan serta untuk mempersiapkan pihak-pihak terlibat dengan pengetahuan teknikal yang diperlukan.

Tujuan:

1. **Lawatan Rasmi Delegasi PTPKM ke Perancis:** Membolehkan delegasi PTPKM mendapat pemahaman yang lebih mendalam mengenai penggunaan dan perkembangan *Homomorphic Encryption* serta algoritma PQC yang sedang diteroka di negara-negara maju, terutamanya di Perancis.
2. **Migrasi PQC pada bulan 6:** Memberikan asas yang kukuh dalam pemilihan dan implementasi algoritma PQC yang sesuai bagi memastikan sistem kriptografi negara dapat mengekalkan keselamatan data walaupun dengan ancaman pengkomputeran kuantum.

Isu Tadbir Urus: Jurang Pengetahuan Antara Pelajar Latihan Industri dan Pakar

Jurang pengetahuan ini timbul kerana pelajar latihan industri biasanya masih dalam proses pembelajaran dan belum mempunyai pengalaman mendalam mengenai teknologi terkini. Manakala pakar yang berpengalaman mempunyai pemahaman yang lebih tinggi terhadap isu-isu teknikal yang kompleks, seperti Homomorphic Encryption dan PQC.

Cadangan:

1. **Sesi Perkongsian Ilmu Merentas Jabatan:** Untuk menutup jurang pengetahuan ini, perlu ada lebih banyak sesi latihan dan perkongsian ilmu antara jabatan. Ini bukan hanya melibatkan jabatan teknikal, tetapi juga jabatan lain seperti jabatan sumber manusia, pentadbiran, dan komunikasi. Sesi-sesi ini boleh berbentuk seminar, bengkel, atau sesi soal jawab bersama pakar.

2. **Penglibatan Aktif Pelajar Latihan Industri:** Melibatkan pelajar dalam projek-projek sebenar serta memberi mereka peluang untuk berinteraksi dengan pakar dalam bidang ini, agar mereka dapat memahami dengan lebih baik teori dan amalan sebenar dalam teknologi ini.

Rancangan Masa Hadapan:

Belum ada rancangan masa hadapan yang konkrit yang boleh diperkatakan buat masa ini. Namun, berdasarkan aktiviti yang sedang dilaksanakan, mungkin perlu untuk merancang lebih banyak inisiatif pengembangan, seperti:

1. **Pembangunan Standard Dalaman PTPKM:** Sebagai contoh, untuk memastikan keseragaman laporan teknikal mengenai algoritma kriptografi, PTPKM mungkin perlu memperkenalkan garis panduan atau template laporan teknikal.
2. **Sesi Latihan Berterusan:** Rancangan jangka panjang untuk menyediakan sesi latihan berkala mengenai Homomorphic Encryption dan PQC untuk memastikan semua pihak sentiasa dikemas kini dengan perkembangan terkini.

Isu Yang Mungkin Berlaku:

Maklumat Tidak Lengkap atau Tidak Terkini: Jika hanya bergantung kepada carian umum dalam internet atau sumber yang tidak sah, terdapat risiko bahawa maklumat yang digunakan mungkin tidak lengkap atau sudah ketinggalan zaman. Oleh itu, perlu ada sumber yang lebih terjamin dan dipercayai bagi mendapatkan maklumat terkini dalam bidang kriptografi dan PQC.

Cadangan:

Latihan yang lebih mendalam mengenai topik-topik seperti *Homomorphic Encryption* dan PQC kepada semua staf, bukan hanya pakar. Ini dapat meningkatkan pemahaman keseluruhan dalam organisasi.