KOLOKIUM PENYELIDIKAN 2020

Komunikasi Selamat Berasaskan Model Keselamatan Mengikut Pengkelasan Maklumat Untuk Kerajaan Digital

MUHAMAD AZLAN YUSOFF

PENYATAAN MASALAH

1

- Dasar Keselamatan ICT dan Arahan Keselamatan menyediakan kaedah perlindungan untuk keselamatan fizikal.

2

- RAKKSSA diperkenalkan untuk mengendalikan maklumat digital.
- Item kawalan capaian dan kriptografi hanya menyediakan panduan umum.

3

- Terdapat keperluan untuk mewujudkan suatu model keselamatan bagi pembangunan aplikasi Kerajaan Digital untuk mengawal komunikasi pelbagai peringkat dalam menjamin keselamatan maklumat-maklumat kerajaan

OBJEKTIF

Mengenal pasti faktor-faktor yang perlu diambil kira bagi komunikasi selamat maklumat kerajaan.

Mencadangkan sebuah model keselamatan yang menyokong penggunaan kawalan capaian dan kriptografi bagi menguruskan maklumat terperingkat dalam bentuk digital.

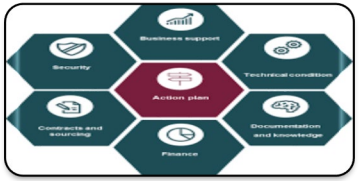
Menyediakan suatu bentuk platfom yang menyokong model yang dicadangkan bagi membangunkan aplikasi Kerajaan Digital.

Mengesahkan keberkesanan model keselamatan yang dicadangkan.

PERSOALAN KAJIAN

OBJEKTIF 1

- Apakah bentuk maklumat kerajaan yang perlu dilindungi bagi aplikasi Kerajaan Digital?
- Apakah faktor yang menyumbang kepada risiko keselamatan bagi aplikasi Kerajaan Digital?



OBJEKTIF 2

- Apakah kaedah yang sesuai digunakan untuk menjamin keselamatan dalam mengendalikan maklumat-maklumat tersebut dalam aplikasi Kerajaan Digital?

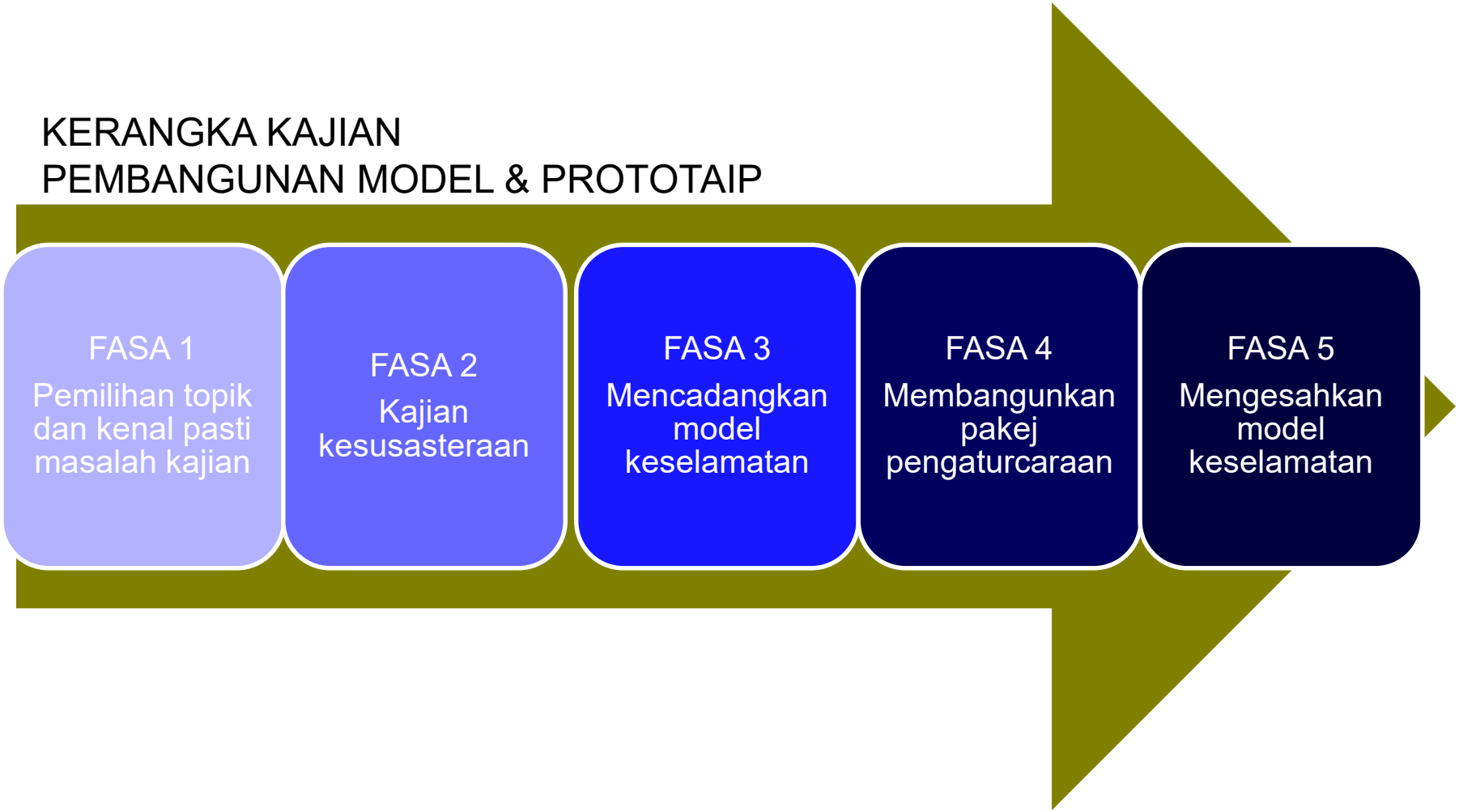
OBJEKTIF 3

- Bagaimanakah kaedah yang dicadangkan dapat membantu dalam aktiviti pembangunan aplikasi Kerajaan Digital?

OBJEKTIF 4

- Adakah kaedah yang dicadangkan dapat mempertingkatkan keselamatan bagi aplikasi Kerajaan Digital?

METODOLOGI KAJIAN



Fasa 1 : Pemilihan topik dan kenal pasti masalah kajian

- Persekitaran semasa iaitu kaedah keselamatan bagi pembangunan aplikasi web Kerajaan Digital
- Kaedah pengkelasan maklumat dipilih sebagai kaedah pembangunan model keselamatan telah menjadi sebahagian dari Dasar Keselamatan ICT Kerajaan yang merujuk kepada Arahan Keselamatan dan Akta Rahsia Rasmi 1972
- Menyokong dokumen RAKKSSA dalam item kawalan capaian dan kriptografi

Fasa 2 : Kajian kesusasteraan

Mengenal pasti peranan pengguna dan mengkategorikan komunikasi mengikut peringkat

Mencadangkan penggunaan kriptografi dengan saiz kekunci tertentu

10 risiko keselamatan untuk aplikasi web

Aplikasi atau sistem juga hendaklah mengikut klasifikasi maklumat yang sama

Kawalan capaian dan kriptografi

Simetrik
Asimestik

RBAC
MAC
DAC
Ejen
Pensijilan

Fasa 3 : Mencadangkan Model Keselamatan CISM

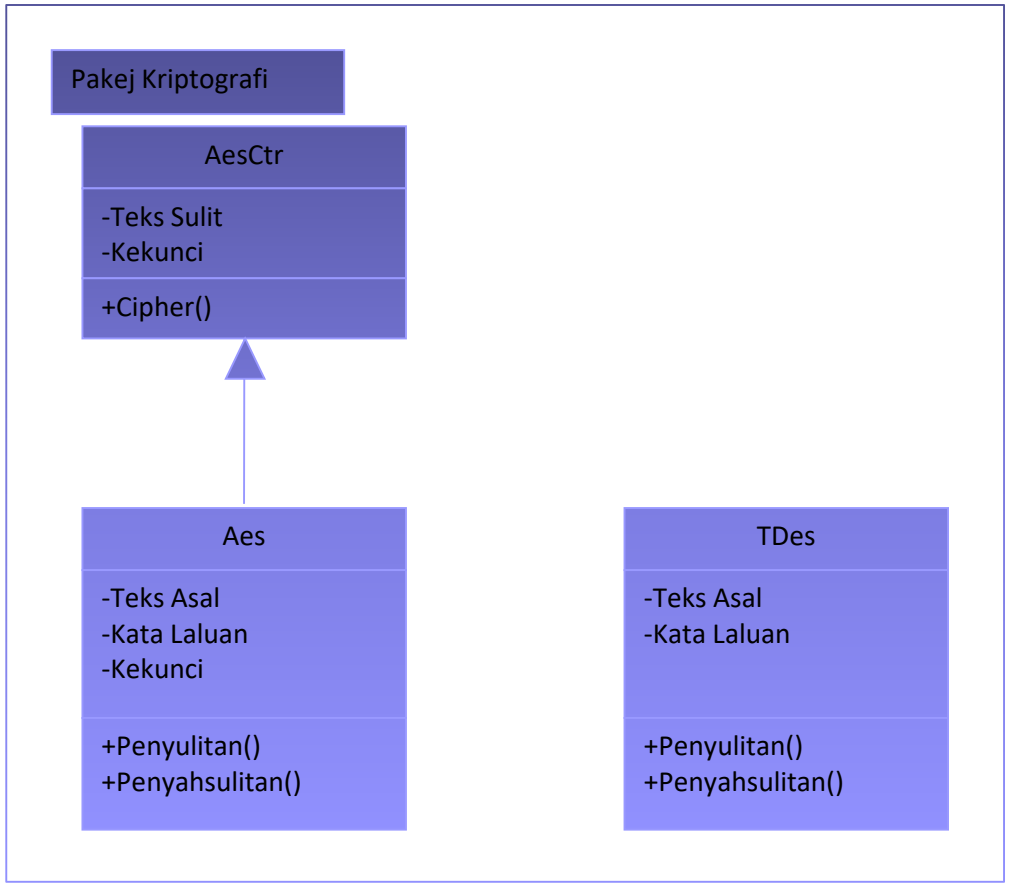
Peringkat Maklumat	Klasifikasi Maklumat	Saiz Kekunci	Contoh Kaedah Penyulitan
Peringkat 1	Rahsia Besar	256 bit	AES
Peringkat 2	Rahsia	192 bit	AES
Peringkat 3	Sulit	128 bit	AES
Peringkat 4	Terhad	112 bit	TDES
Peringkat 5	Terbuka	Tiada	Tiada

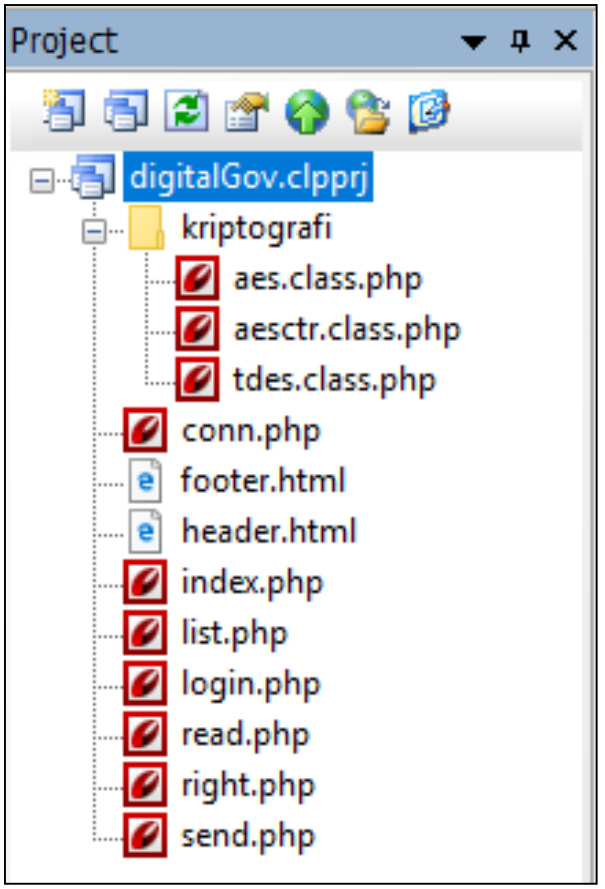
Komponen Model Keselamatan CISM

Cadangan Kawalan Capaian

Peringkat Maklumat	Klasifikasi Maklumat	Kawalan Capaian
Peringkat 1	Rahsia Besar	Pengurusan Tertinggi
Peringkat 2	Rahsia	Pengurusan Tertinggi dan Pengurusan Profesional terpilih
Peringkat 3	Sulit	Semua
Peringkat 4	Terhad	Semua
Peringkat 5	Terbuka	Semua

Fasa 4 : Membangunkan pakej pengaturcaraan dan prototaip





Fasa 5 : Mengesahkan model keselamatan

- Penyediaan bahan temu ramah
- Penyediaan soalan temu ramah
- Menemu ramah pihak yang dikenal pasti

SKOP DAN BATASAN KAJIAN

SKOP 1 Mewujudkan sebuah model keselamatan dengan menggunakan kaedah pengkelasan maklumat

SKOP 2 Anggapan saluran, rangkaian dan pangkalan data sedia ada telah memenuhi prosedur keselamatan yang telah ditetapkan

SKOP 3 Mengatasi dua risiko keselamatan iaitu pendedahan data sensitif dan kawalan capaian tidak selamat

SKOP 4 Platform yang dibangunkan menggunakan kaedah pembangunan web untuk kegunaan bahasa pengaturcaraan PHP

KEPENTINGAN KAJIAN

- Menyumbang dalam bidang keselamatan Kerajaan Digital.

Akademik

- Memperkemaskan kaedah pembangunan aplikasi web kerajaan dengan penyediaan model keselamatan khusus

Perkhidmatan Awam

- Menyokong dan memudahkan kaedah pembangunan aplikasi Kerajaan Digital

Perkhidmatan Awam

SUMBANGAN

Objektif 1

- Soalan 1 dan 2
- Mengenal pasti lima klasifikasi maklumat kerajaan iaitu Rahsia Besar, Rahsia, Terhad, Sulit dan Terbuka
- Meningkatkan keselamatan aplikasi Kerajaan Digital dengan mengatasi dua risiko iaitu pendedahan data sensitif dan kawalan capaian tidak selamat

Objektif 2

- Soalan 3
- Mencadangkan sebuah model keselamatan mengikut pengkelasan maklumat kerajaan yang dapat meningkatkan perlindungan keselamatan maklumat kerajaan mengikut peringkat sensitiviti

SUMBANGAN

Objektif 3

- Soalan 4
- Membangunkan sebuah prototaip pakej pengaturcaraan berasaskan model keselamatan CISM

Objektif 4

- Soalan 5
- Mengesahkan penggunaan model keselamatan CISM dapat meningkatkan keselamatan aplikasi Kerajaan Digital

MASA DEPAN KAJIAN

Pada masa kini terdapat penggunaan banyak peranti untuk membuat capaian terhadap aplikasi kerajaan bagi setiap individu

Terdapat risiko kepada capaian kepada pengguna yang tidak sah

Mewujudkan kaedah kawalan capaian yang dapat mengawal capaian bagi pengguna dan penggunaan peranti yang sah

Sekian Terima Kasih