MODEL PENGUKURAN KEMATANGAN PENGURUSAN KESELAMATAN MAKLUMAT ORGANISASI

MAZLINA BINTI ZAMMANI

UNIVERSITI KEBANGSAAN MALAYSIA

MODEL PENGUKURAN KEMATANGAN PENGURUSAN KESELAMATAN MAKLUMAT ORGANISASI

MAZLINA BINTI ZAMMANI

TESIS YANG DIKEMUKAKAN UNTUK MEMPEROLEHI
IJAZAH DOKTOR FALSAFAH

FAKULTI TEKNOLOGI DAN SAINS MAKLUMAT
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI

2020

PENGAKUAN

Saya akui karya ini adalah hasil kerja saya sendiri kecuali nukilan dan ringkasan yang tiap-tiap satunya telah saya jelaskan sumbernya.

02 Januari 2020

MAZLINA BINTI ZAMMANI
P82834

PENGHARGAAN

Dengan nama Allah Yang Maha Pemurah lagi Maha Mengasihani. Segala pujian bagi Allah Tuhan sekalian alam. Selawat dan salam untuk semulia-mulia utusan dan pengakhiran segala Nabi dan seluruh keluarga dan sahabat baginda.

Syukur ke hadrat Ilahi kerana dengan izinNya, saya dapat menyempurnakan kajian ini. Jutaan terima kasih yang tidak terhingga saya ucapkan kepada penyelia utama iaitu Prof. Madya Dr. Rozilawati Razali di atas segala ilmu dan bimbingan yang diberikan. Tidak lupa juga kepada Prof. Madya Dr. Dalbir Singh selaku penyelia kedua yang turut memberi bimbingan dan tunjuk ajar.

Untuk ibu bapa tersayang, Norzilah Mohamad dan Zammani Mod Amin, suami tercinta Ahmad Yazid Md Lani, serta anak-anak yang dikasihi Ahmad Alif Danial, Ahmad Afiq Danish, Ahmad Ariq Daiyan dan Ahmad Aish Dhafir, jutaan terima kasih atas segala doa, pengorbanan dan sokongan kalian buat saya selama ini.

Tidak lupa juga kepada rakan seperjuangan yang turut sama memberi pandangan, nasihat dan galakan sepanjang menyelesaikan kajian ini.

Akhir sekali, jutaan terima kasih diucapkan kepada semua yang terlibat secara langsung dan tidak langsung dalam kajian ini. Jasa kalian akan sentiasa dikenang dan semoga segala urusan kalian dipermudahkan oleh Allah SWT.

ABSTRAK

Pengurusan Keselamatan Maklumat (PKM) merupakan pendekatan pemeliharaan yang sistematik untuk melindungi kerahsiaan, integriti dan ketersediaan maklumat organisasi daripada capaian yang tidak dibenarkan. Organisasi melaksana inisiatif PKM dengan cara menggubal, mengkaji serta memantap struktur organisasi. Walaupun pelbagai usaha telah dibuat untuk memastikan maklumat dilindungi, namun insiden keselamatan masih lagi berlaku. Fenomena ini menunjukkan pelaksanaan semasa PKM masih kurang berkesan. Pelaksanaan PKM yang kurang berkesan ini membuktikan bahawa kematangan PKM di organisasi adalah ditahap yang rendah. Bagi mencapai tahap kematangan yang lebih tinggi, organisasi perlu sentiasa menilai amalan PKM mereka. Terdapat beberapa model kematangan telah dibangun oleh badan antarabangsa, syarikat perunding dan penyelidik terdahulu bagi membantu organisasi untuk menilai amalan PKM mereka. Namun demikian, model yang dibangunkan tidak mengukur secara holistik amalan PKM organisasi. Ini kerana dimensi pengukuran yang terdapat pada kebanyakan model lebih tertumpu kepada pengukuran terhadap faktor tertentu sahaja. Perkara ini mengakibatkan pengukuran kematangan dibuat secara tidak menyeluruh. Justeru kajian ini bertujuan untuk menangani kelemahan tersebut dengan menghasilkan model pengukuran kematangan PKM yang mengambil kira faktor kejayaan bagi menilai keberkesanan pelaksanaan. Kajian ini mengguna pendekatan kaedah mod campuran yang menggabungkan kajian kualitatif dan kuantitatif untuk mengukuhkan dapatan kajian. Kajian kualitatif melibatkan kajian soroton susastera dan temubual bersama sembilan pengamal industri serta enam pakar bidang manakala kajian kuantitatif melibatkan kajian soal selidik. Data kualitatif dianalisis dengan menggunakan kaedah analisis kandungan manakala data kuantitatif dianalisis menggunakan kaedah analisis statistik. Hasil kajian telah mengenal pasti empat belas faktor kejayaan dan lima puluh tujuh pengukuran kematangan yang mempunyai lima tahap kematangan bagi setiap satunya. Tahap kematangan bagi setiap pengukur dijadikan mekanisme untuk menentukan tahap kematangan PKM secara keseluruhan. Model ini disahkan ketepatan dan kebolehlaksanaannya melalui penilaian tiga pakar bidang dan dua kajian kes. Hasil penilaian menunjukkan model tersebut berupaya mengenal pasti tahap kematangan PKM organisasi. Model ini akhirnya dapat membantu organisasi untuk memperbaiki kelemahan dalam pelaksanaan PKM seterusnya dapat mengurangi insiden keselamatan.

ORGANISATIONAL INFORMATION SECURITY MANAGEMENT MATURITY MODEL

ABSTRACT

Information Security Management (ISM) is a systematic preservation approach to protect the confidentiality, integrity and availability of information from unauthorised access. Organisations implement ISM initiatives by formulating, reviewing and strengthening organisational structures, policy, procedures and security processes. Although various efforts have been done to ensure the information is protected, security incidents continue to occur in organisations. This phenomenon shows that the current implementation of ISM is still ineffective. The ineffective ISM implementation illustrates the low maturity level. To achieve a higher level of maturity, organisations should always evaluate their ISM practices. Several maturity models have been developed by international organisations, consultants and researchers to assist organisations in assessing their ISM practices. However, the current models do not evaluate ISM practices holistically. The measurement dimensions in current models are more focused on assessing certain factors only. This caused the maturity assessment is not executed comprehensively. Therefore, this study aims to address this shortcoming by proposing a comprehensive maturity measurement model that takes into account ISM success factors to evaluate the effectiveness of the implementation. This study adopted a mixed-method approach, which comprises qualitative and quantitative studies to strengthen the research finding. The qualitative study consists of analysing the existing literature and conducting interviews with nine industry practitioners and six experts while quantitative study involves a questionnaire survey. The data obtained from the qualitative study were analysed using content analysis while the quantitative data employed statistics analysis. The study identified fourteen success factors and fifty-seven maturity measures, which each contains five maturity levels. The maturity level for each measurement was then used as the mechanism to determine the overall maturity level. The proposed model evaluated through experts' review and case studies to ensure its accuracy and feasibility. The evaluation shows that the model is able to identify the ISM maturity level systematically and comprehensively. This model will ultimately help the organisations to improve the weaknesses in the implementations thus diminishing security incidents.

KANDUNGAN

SENARAI JADUAL

SENARAI RAJAH

SENARAI SINGKATAN

JPM	Jabatan Perdana Menteri
MIMOS	Malaysia Institute of Microelectronic Systems
MAMPU	Malaysian Administrative Modernisation and Management Planning

BAB I

PENDAHULUAN

1.1 PENGENALAN

Dewasa ini, kebergantungan organisasi terhadap teknologi maklumat dan komunikasi (*Information and Communication Technology*, ICT) telah meningkat secara mendadak ekoran daripada perkembangan teknologi yang semakin pesat (Hamsir & Arief 2015; Karokola, Kowalski & Yngstrom 2011a; Woodhouse 2008). ICT memainkan peranan penting dalam pengendalian operasi harian organisasi untuk menjamin kelancaran dan keberkesanan perkhidmatan (Humairah 2014; Sheikhpour & Modiri 2012). Seiring dengan peningkatan penggunaan ICT dalam operasi harian, organisasi kini turut berhadapan dengan kadar peningkatan ancaman dan risiko terhadap aset ICT yang mengandungi maklumat penting organisasi (Alshaikh 2018; Sheikhpour & Modiri 2012; Woodhouse 2008). Peningkatan ancaman dan risiko keselamatan ini memberi cabaran besar kepada organisasi untuk mempertingkatkan tahap keselamatan maklumat mereka.

Keselamatan maklumat merupakan pemeliharaan terhadap kerahsiaan, integriti dan ketersediaan maklumat (Kazemi, Khajouei & Nasrabadi 2012; Singh, Gupta & Ojha 2014; Mohd & Rozilawati 2011; ISACA 2012; Abu-Musa 2010). Ia bertujuan melindungi maklumat individu mahupun organisasi daripada diceroboh dan disalah guna oleh pihak yang tidak bertanggungjawab (Singh, Gupta & Ojha 2014). Penyalahgunaan maklumat oleh pihak yang tidak bertanggungjawab membawa kesan negatif dan menjejaskan perkhidmatan organisasi. Lantaran itu, bagi mengelak perkhidmatan organisasi terjejas, maklumat perlu diurus dan dikawal dengan sempurna (Sheikhpour & Modiri 2012).

1.2 LATAR BELAKANG

Keselamatan maklumat merupakan pemeliharaan terhadap kerahsiaan, integriti dan ketersediaan maklumat (Kazemi, Khajouei & Nasrabadi 2012; Singh, Gupta & Ojha 2014; Mohd & Rozilawati 2011; ISACA 2012; Abu-Musa 2010). Ia bertujuan melindungi maklumat individu mahupun organisasi daripada diceroboh dan disalah guna oleh pihak yang tidak bertanggungjawab (Singh, Gupta & Ojha 2014). Penyalahgunaan maklumat oleh pihak yang tidak bertanggungjawab membawa kesan negatif dan menjejaskan perkhidmatan organisasi. Lantaran itu, bagi mengelak perkhidmatan organisasi terjejas, maklumat perlu diurus dan dikawal dengan sempurna (Sheikhpour & Modiri 2012).

PKM adalah satu inisiatif dalam mengurus maklumat secara menyeluruh. PKM meliputi sumber manusia, teknologi, proses, kawalan, polisi dan prosedur boleh ditakrif sebagai satu sistem pengurusan yang dilaksana oleh organisasi untuk mewujud serta mengekal persekitaran maklumat yang selamat (Shamala et al. 2018; Singh, Gupta & Ojha 2014). PKM turut ditakrif sebagai pendekatan dan hala tuju strategik untuk menangani risiko, pelanggaran serta insiden keselamatan yang boleh mengancam kerahsiaan, integriti dan ketersediaan maklumat (Kong et al. 2016; Singh, Gupta & Ojha 2014; ISO/IEC 2013a). Pelaksanaan PKM bertujuan memastikan segala sumber, aktiviti, risiko dan insiden keselamatan maklumat diurus dengan berkesan (Singh, Gupta & Ojha 2014; Shojaie, Federrath & Saberi 2014; Lima et al. 2013). Pengurusan yang berkesan dapat mengurangkan pelanggaran dan insiden keselamatan serta memberi keyakinan kepada pelanggan bahawa maklumat telah dilindungi dengan secukupnya (Kazemi, Khajouei & Nasrabadi 2012).

Dalam usaha menjamin keberkesanaan pelaksanaan PKM, organisasi harus sentiasa menilai amalan PKM mereka (Rimawati & Sutikno 2016; Nancylia et al. 2014; Hai & Wang 2014). Amalan PKM boleh dinilai melalui penilaian kematangan (Suhazimah & Zolait 2012). Penilaian kematangan adalah proses mengukur dan memantau amalan PKM terkini di samping mengenal pasti kelemahan dan kekuatan yang ada. Penilaian ini perlu bagi tujuan penambahbaikan dan peningkatan tahap

kematangan amalan semasa. Untuk mencapai tahap kematangan yang dikehendaki, organisasi perlu mempamer kemajuan yang berterusan (Matrane et al. 2015).

1.3 PENYATAAN MASALAH

Keselamatan maklumat dalam konteks organisasi adalah konsep yang berkaitan dengan perlindungan terhadap maklumat organisasi. Bagi memastikan maklumat sentiasa selamat, organisasi telah melaksana inisiatif PKM dengan cara menggubal, mengkaji dan memantap struktur organisasi, polisi, proses, prosedur dan aktiviti keselamatan (Noralinawati & Nor'ashikin 2018).

Walaupun pelbagai usaha telah dibuat oleh organisasi untuk memastikan maklumat sentiasa dilindungi, namun insiden dan pelanggaran keselamatan masih lagi berlaku (AlHogail 2015; Chander, Jain & Shankar 2013; Mohd & Rozilawati 2011; Ge, Yuan & Lu 2011; Alfawaz 2011). Bilangan insiden dan pelanggaran keselamatan terus meningkat setiap tahun (Alshaikh 2018; Jacob & Antony 2016; Bobbert & Mulder 2015; Nazareth & Choi 2015). Berdasarkan tinjauan yang dikeluarkan oleh Ketua Pegawai Maklumat PricewaterhouseCooper, sebanyak 42.8 juta insiden keselamatan dikesan pada tahun 2016, dengan peningkatan sebanyak 48% berbanding tahun sebelumnya (Mamonov & Benbunan-fich 2018). Organisasi di negara membangun mahupun negara maju tidak terlepas daripada mengalami masalah ini. Sebagai contoh, sepanjang tahun 2010 hingga 2016, sebanyak 60,000 insiden keselamatan telah dilapor berlaku di organisasi besar Amerika Syarikat (Kuypers, Maillart & Paté-cornell 2016). Di Malaysia sendiri, dalam laporan insiden keselamatan yang dikeluarkan oleh *Malaysia Computer Emergency Response Team* (MyCert), sebanyak 10699 insiden keselamatan telah dikesan berlaku sepanjang tahun 2018 (CyberSecurity Malaysia 2018).

Fenomena tersebut menggambarkan pelaksanaan semasa PKM masih kurang berkesan (Edwards 2018; Noralinawati & Nor'ashikin 2018; Ge, Yuan & Lu 2011). Organisasi lazimnya menganggap PKM sebagai isu teknikal (Sung & Kang 2017) dan kurang memberi tumpuan kepada isu bukan teknikal (Shojaie & Federrath 2015). Pelaksanaan PKM yang kurang berkesan ini menunjukkan bahawa kematangan PKM organisasi adalah pada tahap yang rendah. Bagi mencapai tahap kematangan yang lebih

tinggi, organisasi seharusnya menilai amalan PKM mereka secara berkala agar penambahbaikan boleh dilaksana (Rimawati & Sutikno 2016).

Dalam bidang penilaian kematangan ini, terdapat beberapa model dan kaedah telah dibangun oleh badan antarabangsa, syarikat perunding mahupun penyelidik. Antara model yang dibangunkan adalah *Control Objectives for Information and Related Technology* (COBIT 4.1) (ITGI 2007), *Information Security Management Maturity Model* (ISM3) (Aceituno 2004), *Open Information Security Management Maturity Model* (O-ISM3) (TOG 2011), *A Cyclical Evaluation Model of Information Security Maturity* (Rigon et al. 2014) dan *Risk Management Maturity Model in Information Security* (MMGRseg) (Mayer & Fagundes 2009). Setiap model mempunyai fokus tertentu dan mencadang skala kematangan yang mengandungi beberapa tahap kematangan. Bagaimanapun, model yang dibangun ini tidak mengukur secara keseluruhan amalan PKM (De Bruin & Von Solms 2015; Kajava & Savola 2005). Kebanyakan model yang dibangun mengukur kematangan berdasar kepada penambahbaikan dan kemajuan proses (Edwards 2018; Suhazimah & Zolait 2012) serta teknologi yang diguna (Karokola, Kowalski & Yngstrom 2011a, 2011b). Dimensi pengukuran yang terdapat pada kebanyakan model lebih tertumpu kepada penilaian terhadap aspek teknikal seperti proses dan teknologi (Barclay 2014, Suhazimah & Zolait 2012) dan kurang mengambil kira aspek bukan teknikal (Karokola, Kowalski & Yngstrom 2011a, 2011b) seperti manusia dan dokumen. Aspek manusia seharusnya tidak diketepikan kerana penglibatan manusia adalah sangat penting bagi menjayakan segala aktiviti PKM (Stewart, & Jürjens 2017; Shojaie & Federrath 2015). Manakala aspek dokumen seperti prosedur dan garis panduan keselamatan juga tidak boleh dipandang ringan kerana dokumen tersebut diperlukan semasa melaksanakan aktiviti PKM.

PKM merangkumi pelbagai faktor dan setiap faktor perlu diberi tumpuan (Edwards 2018; Suhazimah & Zolait 2012). Faktor kejayaan yang meliputi aspek teknikal dan bukan teknikal harus diambil kira dalam pengukuran kematangan. Faktor kejayaan tersebut perlu diberi perhatian sewajarnya bagi memastikan PKM dilaksana dengan berkesan (Edwards 2018; Tu & Yuan 2014; Kazemi, Khajouei & Nasrabadi 2012; CyberSecurity Malaysia 2013; Torres et al. 2006). Meskipun begitu, kajian yang

berkaitan dengan pembangunan model kematangan yang mengambil kira faktor kejayaan kurang diberi penekanan. Kebanyakan model hanya mengukur dan memberi penekanan terhadap faktor daripada aspek tertentu sahaja (De Bruin & Von Solms 2015). Perkara ini mengakibatkan pengukuran kematangan dibuat secara tidak menyeluruh kerana tidak mengambil kira keseluruhan faktor yang menyumbang kepada kejayaan pelaksanaan PKM. Hal ini mengakibatkan organisasi kurang peka terhadap faktor kejayaan PKM dan seterusnya mengakibatkan pelaksanaan PKM di organisasi menjadi kurang berkesan.

Dalam pada itu, model kematangan yang telah dibangun juga kurang praktikal berikutan sukar untuk diguna pakai oleh organisasi (De Bruin & Von Solms 2015; Goksen et al. 2015). Hal ini berlaku berikutan kebanyakan model mempunyai skop tersendiri dan sulit untuk disesuaikan mengikut keperluan organisasi secara keseluruhan (Goksen et al. 2015).

Penyataan di atas menunjukkan keperluan untuk membangunkan model pengukuran kematangan yang mengambil kira masalah yang dinyatakan. Justeru, kajian ini bertujuan untuk mengenal pasti faktor kejayaan PKM, pengukuran dan tahap kematangan setiap faktor yang lebih menyeluruh daripada konteks pengurusan serta menggabungkannya dalam bentuk model pengukuran kematangan PKM organisasi. Model kematangan yang dicadang bukan sahaja mengandungi faktor kejayaan, pengukuran dan tahap kematangan tetapi turut boleh diguna secara praktikal oleh pelbagai jenis organisasi tanpa mengira skop, saiz atau jenis organisasi. Model yang dicadang akhirnya dapat menyenaraikan tahap kematangan keseluruhan bagi membantu organisasi mengenal pasti status pelaksanaan PKM mereka secara berterusan. Hal ini perlu kerana kegagalan dalam melaksana PKM dengan berkesan akan meningkatkan insiden dan pelanggaran keselamatan di samping turut menjejaskan pendapatan, reputasi dan kelebihan daya saing organisasi.

1.4 PERSOALAN KAJIAN

Berdasarkan pernyataan masalah yang dinyatakan, persoalan kajian adalah seperti berikut:

1. Apakah faktor yang menyumbang kepada kejayaan PKM?
2. Apakah pengukuran dan tahap kematangan bagi setiap faktor kejayaan yang dikenal pasti?
3. Bagaimanakah faktor kejayaan, pengukuran dan tahap kematangan setiap faktor yang dikenal pasti dapat membentuk model pengukuran kematangan PKM organisasi yang menyeluruh dan praktikal?
4. Bagaimanakah model pengukuran kematangan PKM organisasi yang dibangun dapat mengukur tahap kematangan keseluruhan?

1.5 OBJEKTIF KAJIAN

Untuk menjawab persoalan yang dinyatakan di atas, kajian ini menetapkan lima objektif kajian seperti berikut:

1. Mengenal pasti faktor kejayaan PKM.
2. Menentukan pengukuran dan tahap kematangan bagi setiap faktor kejayaan.
3. Membangunkan model pengukuran kematangan PKM yang menyeluruh dan praktikal yang mengandungi faktor kejayaan, pengukuran kematangan dan tahap kematangan setiap faktor.
4. Menentukan tahap kematangan PKM organisasi keseluruhan melalui model yang dibangun.
5. Menguji dan mengesah ketepatan dan kebolehlaksanaan model yang dibangun.

1.6 SKOP KAJIAN

Secara amnya, PKM diamalkan di pelbagai peringkat iaitu antarabangsa, negara dan organisasi. Fokus kajian ini melibatkan pengamalan PKM pada peringkat organisasi.

Organisasi yang terlibat pula adalah organisasi sektor awam, swasta dan badan berkanun yang telah melaksana PKM.

Proses PKM secara lazimnya melibatkan beberapa fasa iaitu perancangan, pelaksanaan, penyemakan dan penambahbaikan. Kajian ini memberi tumpuan kepada semua fasa PKM tetapi dalam konteks pengurusan sahaja. Kajian ini tidak meliputi konteks teknikal seperti perincian mendalam berkenaan perkakasan, perisian dan kawalan keselamatan.

1.7 KEPENTINGAN KAJIAN

Kepentingan kajian adalah seperti berikut:

1. Menggabungkan faktor kejayaan, pengukuran dan tahap kematangan sebagai model kematangan PKM yang holistik.
2. Membolehkan organisasi menilai tahap kematangan pelaksanaan PKM secara sistematik dan komprehensif.
3. Model yang dibangun bukan hanya menggariskan kelemahan dalam pelaksanaan semasa tetapi juga menonjolkan kekuatan dan peluang yang dapat dimanfaatkan lagi untuk pelaksanaan PKM yang lebih berkesan.
4. Menjadi rujukan kepada penyelidik yang ingin menjalankan kajian berkaitan pengukuran kematangan PKM di masa hadapan.

1.8 KAEDAH KAJIAN

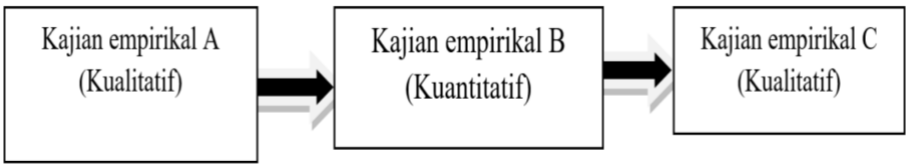
Kajian yang dijalankan adalah berbentuk mod campuran iaitu kualitatif dan kuantitatif. Reka bentuk kaedah mod campuran adalah gabungan reka bantuk berurutan penerokaan (exploratory sequential) dan reka bentuk berurutan penerangan (explanatory sequential). Kajian ini melibatkan empat fasa seperti berikut:

a) Fasa 1 : Kajian Teoritikal

Kajian teoritikal adalah kajian kesusasteraan yang dilakukan untuk mendalami bidang kajian. Kajian ini menentukan penyataan masalah, persoalan kajian, objektif dan skop kajian. Kajian ini juga melibatkan pengenalpastian faktor kejayaan PKM serta model kematangan sedia ada. Data dikumpul daripada dokumen berkaitan yang diperoleh melalui carian di pelbagai pangkalan data. Data kemudiannya dianalisis melalui kaedah analisis kandungan. Hasil kajian teoritikal ini adalah model konsep kematangan PKM yang mengandungi faktor kejayaan dan tahap kematangan. Model konsep ini menjadi asas kepada kajian empirikal.

b) Fasa 2 : Kajian Empirikal

Kajian empirikal terbahagi kepada tiga iaitu kajian empirikal A, kajian empirikal B dan kajian empirikal C seperti yang digambarkan dalam Rajah 1.1.



Rajah 1.1 Reka bentuk kajian empirikal

Kajian empirikal A bertujuan mengesah faktor yang diperoleh daripada kajian teoritikal dan mengenal pasti faktor baharu yang mungkin wujud. Kajian empirikal A dilakukan melalui temu bual individu dan temu bual secara kumpulan fokus bersama pengamal industri yang terlibat di dalam PKM. Hasil dapatan daripada kajian empirikal A kemudiannya disahkan melalui kaedah kuantitatif secara soal selidik dalam kajian empirikal B.

Soal selidik dijawab oleh sampel yang lebih besar berbanding kajian kualitatif. Melalui kaedah kuantitatif ini, soal selidik diedar secara rawak kepada organisasi yang melaksana PKM. Sampel yang dipilih adalah daripada kalangan pengurusan atasan,

pasukan pelaksana, pasukan audit, pasukan penyelaras dan kakitangan organisasi sektor awam, badan berkanun dan sektor swasta yang terlibat dalam PKM.

Hasil dapatan kajian empirikal B dijadikan asas untuk melaksana kajian empirikal C. Kajian empirikal C ini melibatkan temu bual bersama pakar bidang keselamatan maklumat. Sesi ini bertujuan memperoleh pengukuran dan tahap kematangan bagi faktor yang telah disah dalam kajian empirikal B.

c) Fasa 3 : Pembangunan Model

Faktor kejayaan, pengukuran dan tahap kematangan merupakan hasil dapatan daripada kajian teoritikal dan empirikal yang dianalisis mengguna kaedah analisis kandungan dan analisis statistik. Dapatan digabung untuk membentuk cadangan model kematangan PKM.

d) Fasa 4 : Penilaian Model

Bagi menilai ketepatan dan kebolehlaksanaan model yang dicadang, penilaian dilaksana melalui dua kaedah. Kaedah yang pertama adalah penilaian melalui pakar bidang dan kaedah yang kedua adalah penilaian melalui kajian kes.

a. Penilaian pakar bidang

Penilaian pakar dijalankan untuk menilai ketepatan kandungan model yang dibina. Penilaian pakar membabitkan aktiviti temu bual bersama individu yang mempunyai kepakaran dan pengalaman meluas dalam bidang keselamatan maklumat. Penambahbaikkan terhadap model kemudiannya dilaksana berdasarkan pandangan yang diberi oleh pakar dan seterusnya hasil akhir model dibawa kepada penilaian secara kajian kes.

b. Penilaian kajian kes

Penilaian secara kajian kes diguna untuk mengesah kebolehlaksanaan model yang dibangun. Kajian kes melibatkan dua kajian kes (Kes 1 dan Kes 2) di dua organisasi yang berbeza. Kes 1 merupakan organisasi yang tidak menghadapi

insiden keselamatan terhadap skop PKM mereka, manakala Kes 2 merupakan organisasi yang menghadapi beberapa insiden keselamatan terhadap skop PKM yang dilaksana. Analisis dilakukan bagi memperoleh tahap kematangan kedua-dua kes serta menambah baik model.

1.9 ORGANISASI TESIS

Kajian ini mengandungi tujuh bab dengan pembahagian seperti berikut:

Bab I Pendahuluan terdiri daripada pengenalan, latar belakang, penyataan masalah, persoalan kajian, objektif kajian, skop kajian, kaedah kajian dan kepentingan kajian.

Bab II Sorotan Susastera membincangkan kajian kesusasteraan berkaitan keselamatan maklumat secara amnya dan PKM secara khususnya. Bagi keselamatan maklumat, bab ini memperi tumpuan terhadap insiden keselamatan maklumat yang sering terjadi di organisasi. Manakala bagi PKM pula, bab ini melaporkan piawaian dan rangka kerja PKM, faktor kejayaan PKM dan model kematangan sedia ada. Hasil akhir bab ini adalah model konsep kematangan PKM.

Bab III Metodologi Kajian menghurai metodologi yang diguna dalam mencapai objektif kajian. Bab ini membincangkan empat fasa utama yang dilaksana bagi membangunkan model kematangan PKM untuk kajian ini. Bab ini menghurai setiap fasa secara terperinci meliputi pensampelan, instrumen, protokol dan analisis data.

Bab IV Analisis Kajian membincangkan secara mendalam hasil analisis data yang diperoleh daripada kajian empirikal A, kajian empirikal B dan kajian empirikal C.

Bab V Pembangunan Model menerangkan pembangunan model kematangan PKM yang merangkumi faktor kejayaan, pengukuran dan tahap kematangan bagi setiap faktor kejayaan. Seterusnya, bab ini turut menerangkan kaedah bagi memperoleh tahap kematangan keseluruhan.

Bab VI Penilaian Model membincangkan hasil penilaian pakar terhadap ketepatan model yang dicadangkan. Seterusnya, bab ini turut memperincikan hasil penilaian kajian kes terhadap kebolehlaksanaan model.

Bab VII Rumusan mengandungi kesimpulan hasil kajian. Bab ini juga memberi cadangan untuk tujuan kesinambungan kajian masa depan.

1.10 KESIMPULAN

Bab ini memberi penerangan tentang gambaran keseluruhan kajian yang dijalankan. Kajian ini bertujuan untuk membangun model kematangan PKM organisasi dengan mengambil kira faktor kejayaan sebagai asas untuk mengukur kematangan. Bab ini dimulakan dengan pengenalan serta latar belakang kajian, diikuti dengan pernyataan masalah, persoalan kajian, objektif kajian dan skop kajian. Ia kemudiannya disusuli dengan kaedah kajian, kepentingan kajian dan organisasi tesis.

BAB II

SOROTAN SUSASTERA

2.1 PENGENALAN

Bab ini akan menghurai soroton susastera mengenai PKM dan model kematangan PKM. Huraian termasuk definisi, insiden keselamatan maklumat semasa, piawaian dan rangka kerja PKM, faktor penyumbang kepada kejayaan PKM dan model kematangan sedia ada. Rumusan berupa model konsep disertakan di penghujung bab yang mengandungi faktor kejayaan PKM sekaligus menjadi faktor untuk menilai tahap kematangan PKM.

2.2 KESELAMATAN MAKLUMAT

2.2.1 Definisi

Maklumat adalah data yang telah diproses, disusun dan mempunyai makna kepada penerima (Rainer, Turban, Potter 2007). Dalam konteks organisasi, maklumat merupakan aset berharga yang diguna untuk komunikasi dalaman, operasi teknikal, laporan dalaman, laporan luaran dan pelbagai tujuan lain (Putra et al. 2017; Rosmiati, Riadi & Prayudi 2016; Nancylia et al. 2014; Hajdarevic & Allen 2013). Maklumat disimpan dan disampai dalam pelbagai bentuk seperti dokumen, audio, video, cakera keras, pelayan, pangkalan data dan pemacu pena (Jacob & Antony 2016; Hajdarevic & Allen 2013; Suhazimah, Ainin & Zolait 2009). Maklumat terdedah kepada risiko dan ancaman apabila disimpan atau dipindah melalui saluran komunikasi (Hajdarevic & Allen 2013). Risiko dan ancaman ini datang dalam pelbagai bentuk seperti penipuan, pemalsuan dan penyebaran virus. Sehubungan dengan itu, maklumat seharusnya diberi

perlindungan yang sewajarnya melalui pelaksanaan keselamatan maklumat (Tatiara et al. 2018; Kossyva et al. 2014; Nancylia et al. 2014).

Keselamatan maklumat merupakan pemeliharaan terhadap kerahsiaan, integriti dan ketersediaan maklumat (Sung & Kang 2017; Asosheh, Hajinazari & Khodkari 2013; ISO/IEC 2013a; ISACA 2012). Pemeliharaan ini bermaksud maklumat tidak boleh didedahkan atau dicapai tanpa kebenaran; maklumat hendaklah tepat, lengkap, terkini dan hanya boleh diubah dengan cara yang dibenarkan; dan maklumat seharusnya boleh dicapai pada bila-bila masa diperlukan (Tatiara et al 2018; Singh, Gupta & Ojha 2014). Selain daripada kerahsiaan, intergriti dan ketersedian, keselamatan maklumat turut merangkumi ciri-ciri seperti keaslian, kebertanggungjawaban, tanpa sangkalan dan kebolehpercayaan maklumat (Asmidartul 2016).

Keselamatan maklumat juga boleh ditakrif sebagai perlindungan ke atas maklumat sama ada dalam bentuk simpanan, pemprosesan dan permindahan daripada diceroboh dan disalah guna oleh pihak yang tidak bertanggungjawab (Adnan Rizal, Suhaimi & Norhayati 2017; Kazemi, Khajouei & Nasrabadi 2012). Melalui pelaksanaan kawalan keselamatan yang bersesuaian, maklumat organisasi dapat dilindungi daripada risiko dan ancaman, selamat untuk dicapai apabila diperlukan, serta tepat dan lengkap semasa ianya diproses (Tu & Yuan 2014; Mohd & Rozilawati 2011). Ini secara tidak langsung dapat menjamin kesinambungan perkhidmatan, mengelak kerugian kepada organisasi dan meminimum bilangan insiden keselamatan maklumat (Asosheh, Hajinazari & Khodkari 2013; Chang & Ho 2006).

2.2.2 Insiden Keselamatan Maklumat

Insiden keselamatan maklumat bermaksud musibah yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut yang berpotensi untuk mengakibatkan kobocoran atau kerosakan kepada maklumat (JPM 2006). Aset ICT merangkumi data, maklumat, perkakasan, perisian, aplikasi, dokumentasi dan sumber manusia. Insiden keselamatan kebiasaannya berlaku apabila terdapat kelemahan pada pengurusan dan pengendalian aset ICT. Insiden keselamatan yang berlaku akan menyebabkan kerugian dan menjejas imej organisasi (Hsu, Wang & Lu 2016; Hajdarevic & Allen 2013). Jadual

2.1 menyenarai antara insiden keselamatan maklumat yang kerap berlaku di sesebuah organisasi.

Jadual 2.1 Insiden keselamatan maklumat

Insiden	Penerangan
Pelanggaran Dasar (*Violation of Policy*)	Penggunaan aset ICT bagi tujuan kebocoran atau capaian maklumat yang melanggar Dasar Keselamatan Maklumat.
Penghalangan Penyampaian Perkhidmatan (*Denial of Service*)	Perkhidmatan pemprosesan maklumat sengaja dinafikan terhadap pengguna sistem. Ia melibatkan sebarang tindakan yang menghalang sistem daripada berfungsi secara normal.
Pencerobohan (*Intrusion*)	Mengubah suai ciri perkakasan, perisian atau komponen sesebuah sistem; atau menggunakannya tanpa pengetahuan, arahan atau persetujuan dari pihak yang empunya maklumat. Ini termasuk pencerobohan laman sesawang, capaian tanpa kebenaran, melakukan kerosakan kepada sistem atau data; dan meminda konfigurasi sistem.
Pemalsuan (*Forgery*)	Pemalsuan, penyamaran dan penyalahgunaan identiti milik individu lain.
Penipuan (*Fraud*)	Penipuan yang dilakukan untuk tujuan keuntungan peribadi.
Spam	Penghantaran e-mel ke akaun individu lain secara berulang kali dalam satu tempoh tertentu yang menyebabkan kesesakan rangkaian dan tindak balas menjadi perlahan.
Malicious Code	Kod yang merbahaya yang dimasuk ke dalam sesebuah perisian atau sistem tanpa kebenaran yang menyebabkan kekacauan kepada sistem dan perisian tersebut. Di antara Malicious code yang terkenal adalah virus, trojan horse, backdoor dan worm.
Attempts/Hack Threats/Information Gathering	Percubaaan untuk mencapai sistem atau maklumat tanpa kebenaran. Ini termasuk spoofing, phishing, probing, war driving dan scanning.
Kehilangan Fizikal (*Physical Loss*)	Kehilangan capaian dan kegunaan maklumat yang disebabkan oleh kecurian, kerosakan dan kebakaran ke atas aset ICT.

Sumber : (Al-Mhiqani et al. 2018; Kuypers, Maillart & Paté-cornell 2016; JPM 2006)

Dalam laporan insiden yang dikeluarkan oleh MyCERT, insiden keselamatan di Malaysia meningkat daripada 7962 kes pada tahun 2017 kepada 10699 kes pada tahun 2018 (CyberSecurity Malaysia 2018). Insiden penipuan (fraud) merupakan insiden yang

paling kerap berlaku pada tahun 2018 dengan jumlah sebanyak 5123 kes diikuti dengan insiden percubaan pencerobohan yang melibatkan 1805 kes. Di negara maju seperti Amerika Syarikat, sebanyak 60,000 insiden telah dilaporkan berlaku sepanjang tempoh tahun 2010 hingga 2016 (Kuypers, Maillart & Pate-cornell 2016). Manakala di Belanda pula, sebanyak 18% organisasi kecil dan sederhana dilanda serangan insiden setiap tahun (Mijnhardt, Baars & Spruit 2016). Kesan dari insiden tersebut telah menyebabkan kerugian kepada organisasi yang terlibat (Mijnhardt, Baars & Spruit 2016; Bobbert & Mulder 2015). Kerugian ini termasuklah daripada segi kemerosotan kewangan, kemusnahan terhadap infrastruktur kritikal, kehilangan keyakinan pelanggan dan keruntuhan imej organisasi (Al-Mhiqani et al. 2018; ISACA 2012). Hal ini jelas menunjukkan bahawa insiden keselamatan maklumat bukan sesuatu yang boleh dipandang ringan tetapi harus diambil tindakan dan pendekatan bersesuaian untuk meminimum bilangan dan kesannya demi mencapai objektif keselamatan maklumat.

Objektif keselamatan maklumat adalah bertujuan untuk menjamin kesinambungan perkhidmatan (Horne et al. 2016). Objektif keselamatan yang turut meliputi kerahsiaan, integriti, ketersediaan dan tanpa sangkalan maklumat, merupakan cabaran besar bagi setiap organisasi (Horne et al. 2016; CyberSecurity Malaysia 2013). Ia tidak boleh dicapai melalui teknologi semata-mata tetapi turut bergantung kepada keberkesanan proses, organisasi serta individu yang mengurus dan melaksana keselamatan maklumat (Suhazimah & Zolait 2012). Oleh yang demikian, terdapat keperluan untuk memandang keselamatan maklumat daripada perspektif menyeluruh dan organisasi perlu mempunyai kaedah pengurusan keselamatan maklumat yang sistematik bagi memastikan aset ICT yang mengandungi maklumat organisasi sentiasa berada dalam keadaan selamat (Nancylia et al. 2014; Suhazimah, Ainin & Zolait 2009).

2.3 PENGURUSAN KESELAMATAN MAKLUMAT (PKM)

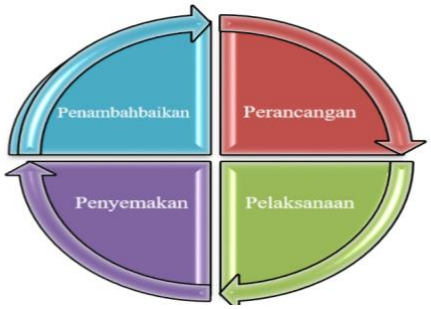
2.3.1 Definisi

Pengurusan keselamatan maklumat (PKM) merupakan pendekataan atau kaedah menyeluruh dan bersistematik melibatkan pelaksanaan kawalan yang perlu dilaksana oleh sesebuah organisasi untuk menangani risiko dan insiden keselamatan yang boleh mengancam kerahsiaan, integriti dan ketersediaan maklumat (Kong et al. 2016; Singh,

Gupta & Ojha 2014; Asosheh, Hajinazari & Khodkari 2013; ISO/IEC 2013a; ISACA 2012; Kazemi, Khajouei & Nasrabadi 2012; Bowen, Hash & Wilson 2006). PKM merupakan sebahagian daripada sistem pengurusan keseluruhan organisasi (ISO/IEC 2013a; Nurbojatmiko, Susanto & Shobariah 2016) yang merangkumi dasar, prosedur, garis panduan, aktiviti dan sumber berkaitan keselamatan maklumat (Singh, Gupta & Ojha 2014; CyberSecurity Malaysia 2013). PKM meliputi lima komponen utama keselamatan maklumat iaitu organisasi keselamatan dan infrastruktur; dasar, piawaian dan prosedur keselamatan; garis panduan keselamatan dan penilaian risiko; kesedaran keselamatan dan program latihan; dan pematuhan (ISO/IEC 2013a; Tudor 2001; Hong et al. 2003).

PKM menyediakan hala tuju strategik untuk pelaksanaan proses dan aktiviti keselamatan bagi memastikan objektif keselamatan tercapai, pengurusan risiko yang konsisten dan penggunaan sumber maklumat yang berkesan (Lima et al. Melalui PKM, misi dan visi organisasi serta aktiviti keselamatan dapat diselaras dalam satu strategi bersepadu (Singh, Gupta & Ojha 2014). PKM juga adalah disiplin pelbagai dimensi yang perlu diberi perhatian sewajarnya untuk memastikan persekitaran yang sesuai dan selamat dalam melindungi maklumat organisasi (Suhazimah & Zolait 2012).

PKM melibatkan amalan seperti penubuhan, pelaksanaan, penyelenggaraan dan penambahbaikan aktiviti keselamatan maklumat (Nurbojatmiko, Susanto & Shobariah 2016; Singh, Gupta & Ojha 2014; Nancylia et al. 2014). Amalan ini perlu dilaksana secara kerana ancaman dan kelemahan yang sentiasa berubah. Pada masa kini, kebanyakan organisasi mengamalkan model kitaran hayat "Plan-Do-Check-Act" (PDCA) dalam melaksana PKM (Shamala et al. 2018). Penggunaan model kitaran hayat PDCA dalam PKM ini bertujuan untuk memastikan kawalan keselamatan maklumat sesebuah organisasi dilaksana, diperkuat dan diperbaiki dari semasa ke semasa (Suhaimi et al. 2014). Kitaran hayat ini terbahagi kepada empat fasa iaitu perancangan, pelaksanaan, penyemakan dan penambahbaikan (Johnson 2014; Nancylia et al. 2014; Asosheh, Hajinazari & Khodkari 2013; MAMPU 2010) seperti yang ditunjukkan pada Rajah 2.1.



Rajah 2.1 Fasa PKM

(Sumber: Johnson 2014; Nancylia et al. 2014; Asosheh, Hajinazari & Khodkari 2013)

Fasa perancangan merangkumi aktiviti perancangan dan pengurusan strategik. Perancangan strategik merupakan antara pendekatan pengurusan untuk mencapai matlamat keselamatan maklumat organisasi. Ia dilaksana melalui proses penetapan objektif, penggubalan polisi, pengenalpastian isu strategik, pemantapan tadbir urus, peruntukan sumber kewangan, peruntukan tenaga manusia dan penilaian risiko (Nurazean et al. 2015, Asosheh, Hajinazari & Khodkari 2013; Nancylia et al. 2014; Saint-Germain 2005). Pengurusan strategik pula melibatkan aktiviti seperti pengurusan sumber dan penganjuran program kesedaran serta latihan kepada kakitangan organisasi (Aceituno 2004). Aktiviti pada fasa perancangan ini adalah sangat penting untuk menjamin aktiviti pada fasa pelaksanaan berjalan dengan lancar (Nurazean et al. 2015).

Fasa pelaksanaan melibatkan pengendalian operasi keselamatan. Pengendalian operasi keselamatan ini diterajui oleh pasukan pelaksana keselamatan (Nurazean et al. 2015). Antara aktiviti yang terlibat pada fasa pelaksanaan adalah seperti aktiviti pemulihan risiko, penyediaan prosedur operasi, pelaksanaan operasi dan kawalan keselamatan, dan pengendalian insiden dan bencana (Asosheh, Hajinazari & Khodkari 2013; Nancylia et al. 2014; Saint-Germain 2005). Kesemua aktiviti tersebut memerlukan komitmen yang tinggi daripada seluruh ahli pasukan pelaksana. Kesemua aktiviti tersebut seterusnya akan dinilai keberkesanannya pada fasa penyemakan.

Fasa penyemakan membabitkan proses memantau semua aktiviti, mengukur prestasi dan mengkaji keberkesanan PKM (Kossyva et al 2014; MAMPU 2010). Pematuhan terhadap polisi, prosedur dan kawalan keselamatan turut dinilai pada fasa penyemakan. Hasil penilaian akan dilapor kepada pengurusan atasan untuk

pertimbangan (MAMPU 2010). Hasil penilaian juga akan dilapor kepada pihak yang bertanggungjawab supaya ketidakpatuhan atau ketidakakuran terhadap segala aspek keselamatan maklumat boleh diambil tindakan.

Tindakan pembetulan dan pencegahan dilaksana pada fasa penambahbaikan. Tindakan ini dibuat berdasar kepada teguran audit dan laporan ketidakpatuhan yang dikeluarkan oleh pasukan audit (Nancylia et al. 2014; Asosheh, Hajinazari & Khodkari 2013). Di samping itu, pengemaskinian polisi, prosedur, pelan dan proses juga turut dilaksana pada fasa penambahbaikan (MAMPU 2010). Keperluan untuk melaksana semua aktiviti ini adalah untuk memastikan PKM organisasi mencapai peningkatan yang berterusan (Kossyva et al 2014).

Peningkatan PKM yang berterusan memberi pelbagai manfaat kepada organisasi. Antara kelebihan PKM adalah seperti berikut:

a. Memandu organisasi dalam menyelaras dan mengurus aktiviti keselamatan maklumat secara lebih berkesan (Kazemi, Khajouei & Nasrabadi 2012).

b. Menyediakan pendekatan yang sistematik dalam mengurus risiko (ISO/IEC 2013a; Nurazean et al. 2015).

c. Mewujudkan amalan kerja lebih baik bagi menyokong matlamat organisasi dengan mewujudkan polisi, prosedur dan garis panduan yang mantap (ISO/IEC 2013a; ISACA 2012; Kazemi, Khajouei & Nasrabadi 2012).

d. Membantu kakitangan memahami dan mematuhi keperluan keselamatan (Nurazean et al. 2015).

e. Memberi keyakinan kepada pelanggan organisasi (Kazemi, Khajouei & Nasrabadi 2012) dan menjadikan organisasi lebih berdaya saing (ISO/ICE 2013a, Chang & Ho 2006; Park C., Jang & Park Y. 2010).

2.3.2 Piawaian dan Rangka Kerja PKM

Pelbagai piawaian dan rangka kerja telah dibangun oleh badan antarabangsa, kerajaan, industri dan penyelidik bagi memandu organisasi dalam melaksana PKM (Asosheh, Hajinazari & Khodkari 2013; Azah & Norizan 2013; Nurazean et al. 2015). Antara piawaian yang sering menjadi rujukan ialah *Information technology – Security Techniques – Information Security Management System – Requirement* (ISO/IEC 27001), *Information technology – Security Techniques – Code of Practice for Information Security Management System* (ISO/IEC 27002), *COBIT 5 for Information Security, Information Security Handbook: A Guide for Managers* (NIST 800-100) dan *Information Technology Infrastructure Library* (ITIL).

a) Information technology – Security Techniques – Information Security Management System – Requirement (ISO/IEC 27001)

Asal usul ISO / IEC 27001 bermula daripada pembangunan kod amalan baik yang dicadangkan oleh *Department of Trade Industry*, UK pada tahun 1989 yang kemudiannya berkembang menjadi BS7799 (Sheikhpour & Modiri 2012). BS7799 adalah piawaian yang diterbitkan oleh British Institution Standard (BSI Group) pada tahun 1995. Tujuan piawaian BS7799 dibangunkan adalah untuk meningkatkan kesedaran tentang isu-isu keselamatan dan mencadangkan kawalan bagi melindungi maklumat. Piawaian BS7799 secara perlahan-lahan telah melalui beberapa versi pindaan dan yang terkini adalah ISO / IEC 27001 yang telah digubal oleh *International Organization for Standardization* (ISO) dan *International Electrotechnical Commission* (IEC). Piawaian ISO/IEC 27001 ini turut melalui beberapa versi dan pindaan. Versi yang terkini adalah ISO/IEC 27001:2013 yang digubal pada tahun 2013. Piawaian ini menetap keperluan untuk mewujud, melaksana, mengekal dan menambah baik sistem pengurusan keselamatan maklumat di dalam organisasi (ISO/IEC 2013a). Piawaian ini menyentuh berkenaan keperluan untuk menilai dan memulih risiko keselamatan maklumat. Piawaian ini menggabungkan keperluan teknologi, proses dan sumber manusia untuk membantu organisasi melindungi aset maklumat mereka secara tersusun (Shojaie & Federrath 2015). Piawaian terkini ini menggaris tujuh klausa yang mesti diikuti oleh organisasi iaitu konteks organisasi (context of the organization),

kepimpinan (leadership), perancangan (planning), sokongan (support), operasi (operation), penilaian prestasi (performance evaluation) dan penambahbaikan (improvement). Organisasi yang tidak mematuhi keperluan di dalam tujuh klausa yang digaris dianggap tidak mematuhi piawaian yang ditetapkan (ISO/IEC 2013a).

b) Information technology – Security Techniques – Code of Practice for Information Security Management System (ISO/IEC 27002)

Selain daripada ISO/IEC 27001, *International Organization for Standardization* (ISO) dan *International Electrotechnical Commission* (IEC) turut membangunkan piawaian ISO/IEC 27002. Piawaian ISO/IEC 27002 merupakan piawaian yang digubal bagi membantu organisasi untuk memilih kawalan keselamatan semasa melaksana proses pengurusan keselamatan maklumat. Piawaian ISO/IEC 27002 mengandungi panduan pelaksanaan untuk keperluan yang dinyatakan dalam ISO/IEC 27001 (Suomu 2015). Edisi terkini piawaian ini adalah ISO/IEC 27002:2013 yang mengganti edisi sebelumnya iaitu ISO/IEC 27002:2007. Piawaian ini mempunyai 14 klausa kawalan keselamatan meliputi 35 kategori utama dan 114 kawalan (ISO/IEC 2013b).

c) COBIT 5 for Information Security

Control Objectives for Information and Related Technologies 5 (COBIT 5) menyediakan rangka kerja menyeluruh bagi membantu organisasi untuk mencapai objektif teknologi maklumat yang meliputi tadbir urus dan pengurusan organisasi. COBIT 5 *for Information Security* dibina di atas rangka kerja COBIT 5 yang memberi fokus kepada aspek keselamatan maklumat. COBIT 5 *for Information Security* merupakan rangka kerja yang mengintegrasi perniagaan atau perkhidmatan dengan tanggungjawab pihak yang terlibat. Rangka kerja ini memberi gambaran jelas berkenaan amalan pengurusan keselamatan maklumat, menggaris peranan dan tanggungjawab pihak yang terlibat dan menyenarai langkah untuk melaksana proses keselamatan (ISACA 2012).

d) Information Security Handbook: A Guide for Managers (NIST 800-100)

National Institute of Standards and Technology (NIST) telah membangun garis panduan keselamatan NIST 800-100 pada tahun 2006 yang bertujuan untuk membantu pihak pengurusan dalam memahami dan melaksana program keselamatan maklumat. Garis panduan ini menggaris elemen yang perlu ada di dalam keselamatan maklumat. Topik dalam garis panduan ini dirangka berdasar kepada undang-undang dan peraturan yang berkaitan dengan keselamatan maklumat. Garis panduan ini boleh dijadikan rujukan untuk memperoleh maklumat mengenai topik tertentu atau boleh diguna dalam proses membuat keputusan untuk membangun program keselamatan maklumat. Organisasi yang mengguna pakai garis panduan ini perlu menyesuaikan panduan ini mengikut keperluan keselamatan perkhidmatan mereka (Bowen, Hash & Wilson 2006).

e) Information Technology Infrastructure Library (ITIL)

Information Technology Infrastructure Library (ITIL) merupakan rangka kerja yang menggariskan set amalan terbaik dalam pengurusan perkhidmatan teknologi maklumat (ITSM) yang memberi tumpuan kepada penyelarasan perkhidmatan teknologi maklumat (IT) dengan keperluan perniagaan. ITIL menerangkan proses dan prosedur yang boleh diguna oleh organisasi untuk mengurus operasi IT. Rangka kerja ITIL telah dibangunkan oleh *Central Computing and Telecommunications Agency* (Agensi Pengkomputeran dan Telekomunikasi Pusat) yang kini dikenali sebagai *Office of Government Commerce* (Pejabat Perdagangan Kerajaan). ITIL telah melalui beberapa versi pindaan dan terkini terdiri daripada lima buku meliputi proses dan peringkat kitar hayat perkhidmatan IT yang berbeza iaitu strategi perkhidmatan, reka bentuk perkhidmatan, peralihan perkhidmatan, operasi perkhidmatan dan peningkatan perkhidmatan berterusan (Rosmiati, Riadi & Prayudi 2016; Haufe et al. 2016; Cartlidge et al. 2012).

f) Rangka Kerja Keselamatan Siber Sektor Awam Malaysia

Rangka Kerja Keselamatan Siber Sektor Awam Malaysia (RAKKSSA) versi 1.0 telah dibangunkan pada tahun 2016 oleh Unit Pemodenan Tadbiran Dan Perancangan Pengurusan Malaysia (MAMPU) dengan usaha sama CyberSecurity Malaysia (CSM),

Pejabat Ketua Pegawai Keselamatan Kerajaan (CGSO) dan MIMOS Berhad. Objektif pembangunan RAKKSSA adalah untuk memastikan keselamatan penyampaian perkhidmatan sektor awam. RAKKSSA menerangkan lapan komponen utama keselamatan yang perlu diambil kira oleh agensi sektor awam Malaysia untuk melindungi maklumat yang terdapat dalam ruang siber mereka. Lapan komponen tersebut adalah kenal pasti, lindung, kesan, tindak balas, pulih, peroleh, audit keselamatan dan kuat kuasa seperti yang digambarkan dalam Rajah 2.2.

Rajah 2.2 Komponen Rangka Kerja Keselamatan Siber Sektor Awam Malaysia (RAKKSSA)
Sumber: MAMPU et al. 2016

Secara ringkasnya, terdapat pelbagai piawaian dan rangka kerja diwujudkan bagi membantu organisasi memilih program dan kawalan yang sesuai dalam PKM. ISO/IEC 27001 dan ISO/IEC 27002 merupakan piawaian yang paling banyak diguna pakai oleh organisasi (Asosheh, Hajinazari & Khodkari 2013). Piawaian tersebut membentangkan keperluan untuk menetap, melaksana, menggerak, memantau, mengkaji semula, memelihara, mengemas kini, dan meningkat sistem pengurusan keselamatan maklumat (ISO/IEC 2013a, 2013b). COBIT 5 for Information Security pula merupakan rangka kerja yang diwujudkan bagi membantu para profesional dan keselamatan IT memahami dan melaksana aktiviti keselamatan maklumat di samping meningkatkan kesedaran berkenaan teknologi terkini dan ancaman yang wujud melalui teknologi tersebut (ISACA 2012). NIST 800-100 pula memberikan gambaran keseluruhan mengenai elemen program keselamatan maklumat untuk membantu

pengurus dalam memahami bagaimana untuk mewujud dan melaksana program keselamatan maklumat (Bowen, Hash & Wilson 2006). Sementara itu, ITIL bertindak sebagai rangka kerja yang menggabungkan amalan terbaik untuk pengurusan infrastruktur teknologi maklumat, perkhidmatan dan keselamatan yang berkesan (Haufe 2017). Manakala RAKKSSA memberi panduan asas kepada agensi sektor awam Malaysia mengenai komponen keselamatan yang perlu diberi perhatian bagi melindungi maklumat dalam ruangan siber (RAKKSSA 2016).

2.3.3 Faktor Kejayaan PKM

Kejayaan PKM sesebuah organisasi berkait rapat dengan komitmen dan kepimpinan pengurusan atasan (Noralinawati & Nor'ashikin 2018; Sari et al. 2016; Alnatheer 2015; Nurazean et al. 2015; Singh, Gupta & Ojha 2014; Chander, Jain & Shankar 2013; ISO/IEC 2013a; CyberSecurity Malaysia 2013; Kazemi, Khajouei & Nasrabadi 2012; Suhazimah & Zolait 2012; Hu et al. 2012; ISACA 2012; Woodhouse 2008; Bowen, Hash & Wilson 2006). Pada peringkat awal pelaksanaan PKM, pengurusan atasan hendaklah mewujudkan objektif dan polisi keselamatan maklumat yang selari dengan matlamat organisasi (ISO/IEC 2013a). Pengurusan atasan bertanggungjawab dalam penggubalan polisi keselamatan maklumat dengan memastikan polisi tersebut perlu jelas, menyeluruh, sentiasa dikaji dan dihebah kepada seluruh kakitangan organisasi, pihak ketiga dan pihak berkepentingan (Noralinawati & Nor'ashikin 2018; Sari et al. 2016; MAMPU et al. 2016; Alnatheer 2015; Singh, Gupta & Ojha 2014; Chander, Jain & Shankar 2013; Kazemi, Khajouei & Nasrabadi 2012; ISO/IEC 2013a; ISACA 2012; Suhazimah & Zolait 2012; Hu et al. 2012; Cartlidge et al. 2012; Azhari 2008; Woodhouse 2008; Bowen, Hash & Wilson 2006). Pengurusan atasan perlu mempunyai sifat kepimpinan yang tinggi dengan memastikan polisi, prosedur, kawalan dan proses keselamatan maklumat dilaksana dan dipatuhi oleh kakitangan serta pihak ketiga (Noralinawati & Nor'ashikin 2018; ISO/IEC 2013a,2013b; Cartlidge et al. 2012). Komitmen pihak atasan turut diperlukan dalam memberi maklumbalas berkenaan sebarang isu keselamatan dan memperuntukan sumber kewangan dan sumber manusia yang mencukupi untuk melaksana aktiviti dan proses PKM (Noralinawati & Nor'ashikin 2018; Sari et al. 2016; Alnatheer 2015; Bowen, Hash & Wilson 2006; Chander, Jain & Shankar 2013; ISO/IEC 2013a; ISACA 2012; Cartlidge et al. 2012).

Antara proses utama PKM adalah pengurusan risiko (MAMPU et al. 2016; Alnatheer 2015; Singh, Gupta & Ojha 2014; ISO/IEC 2013a; Chander, Jain & Shankar 2013; ISACA 2012; Mohd & Rozilawati 2011; Suhazimah & Zolait 2012; Hu et al. 2012; Cartlidge et al. 2012; Saleh & Alfantookh 2011; Yang 2011; Woodhouse 2008; Bowen, Hash & Wilson 2006). Pengurusan risiko bertujuan untuk mengenal pasti, menganalisis, menilai dan mengambil tindakan untuk mengawal risiko. Organisasi harus melaksana pengurusan risiko secara konsisten dan sistematik (MAMPU et al. 2016; Mayer & Fagundes 2009). Pengurusan risiko melibatkan dua aktiviti utama iaitu penilaian dan pemulihan risiko. Penilaian risiko adalah aktiviti mengenal pasti, menganalisis dan menilai risiko aset maklumat manakala pemulihan risiko pula melibatkan pelaksanaan strategi pemulihan terhadap aset yang berisiko berdasar daripada laporan penilaian risiko yang dikeluarkan (ISO/IEC 2013a; Tsohou et al. 2010).

Selain daripada pengurusan risiko, pengurusan kesinambungan perkhidmatan turut merupakan proses penting yang terdapat dalam PKM (MAMPU et al. 2016; Aisyah et al. 2015; Singh, Gupta & Ojha 2014; Chander, Jain & Shankar 2013; ISO/IEC 2013b; Cartlidge et al. 2012). Objektif pengurusan kesinambungan perkhidmatan adalah untuk menjamin perkhidmatan organisasi dapat diteruskan semasa atau selepas berlakunya insiden keselamatan atau bencana (Mansol et al. 2014; Randeree, Mahal & Narwani 2012). Bagi tujuan tersebut, pengurusan kesinambungan perkhidmatan memerlukan pelan pengurusan kesinambungan perkhidmatan yang efektif (Singh, Gupta & Ojha 2014) yang inputnya diperoleh daripada penilaian risiko dan analisis impak perkhidmatan (Cartlidge et al. 2012; Mayer & Fagundes 2009; Bowen, Hash & Wilson 2006). Pelan pengurusan kesinambungan perkhidmatan merangkumi maklumat sumber, proses, prosedur, peranan dan tanggungjawab pihak yang terlibat. Untuk memastikan keberkesanan dan kebolehlaksanaan pelan pengurusan kesinambungan perkhidmatan yang dibangun, organisasi hendaklah melakukan simulasi secara berkala (MAMPU et al. 2016; Singh, Gupta & Ojha 2014; Chow & Ha 2009; Bowen, Hash & Wilson 2006).

Simulasi terhadap pelan pengurusan kesinambungan perkhidmatan dan aktiviti pengurusan risiko dikendali oleh pasukan pelaksana. Pasukan pelaksana

bertanggungjawab melaksana operasi dan kawalan keselamatan (Nurazean et al. 2015). Lantaran itu, pasukan pelaksana perlu mempunyai pengetahuan, kemahiran dan memberi komitmen penuh terhadap operasi dan kawalan keselamatan yang sedang dijalankan (MAMPU et al. 2016; Nurazean et al. 2015). Sepanjang melaksana operasi keselamatan, pasukan pelaksana harus mengikuti tatacara yang dinyatakan dalam prosedur keselamatan. Bagi menjamin pasukan pelaksana dapat mengikuti tatacara prosedur dengan betul, prosedur keselamatan haruslah jelas dan lengkap dalam menerang langkah kerja yang perlu dipatuhi serta dihebahkan kepada semua ahli pasukan (Singh, Gupta & Ojha 2014; ISO/IEC 2013b; CyberSecurity Malaysia 2013; Bowen, Hash & Wilson 2006).

Bagi mengekal atau meningkatkan prestasi perkhidmatan serta mengurangkan insiden dan pelanggaran keselamatan, kakitangan organisasi dan pihak ketiga perlu mematuhi polisi, undang-undang dan peraturan keselamatan organisasi (Chander, Jain & Shankar 2013; ISO/IEC 2013a; ISACA 2012; Mohd & Rozilawati 2011; Bowen, Hash & Wilson 2006). Pematuhan terhadap polisi, undang-undang dan peraturan keselamatan boleh dipertingkat sekiranya kakitangan dan pihak ketiga mempunyai kesedaran (Bowen, Hash & Wilson 2006; Singh, Gupta & Ojha 2014; Chander, Jain & Shankar 2013; Alnatheer 2015; Woodhouse 2008) dan motivasi yang tinggi (Chander, Jain & Shankar 2013; Kazemi, Khajouei & Nasrabadi 2012) mengenai kepentingan dan keperluan keselamatan maklumat. Untuk meningkatkan kesedaran mengenai kepentingan dan keperluan keselamatan maklumat, program kesedaran perlu diberi kepada seluruh kakitangan, pihak ketiga mahupun pihak berkepentingan (Noralinawati & Nor'ashikin 2018; Sari et al. 2016; MAMPU et al. 2016; Alnatheer 2015; Singh, Gupta & Ojha 2014; Chander, Jain & Shankar 2013; Hu et al. 2012; ISO/IEC 2013a; CyberSecurity Malaysia 2013; Kazemi, Khajouei & Nasrabadi 2012; ISACA 2012; Bowen, Hash & Wilson 2006). Pada masa yang sama, program latihan untuk pasukan pelaksana, individu atau pihak yang berkaitan perlu dianjur bagi memastikan mereka yang terlibat dalam PKM berkemahiran, berpengetahuan dan cekap untuk melaksana tugasan (Noralinawati & Nor'ashikin 2018; MAMPU et al. 2016; Alnatheer 2015; Singh, Gupta & Ojha 2014; Chander, Jain & Shankar 2013; ISO/IEC 2013a; Hu et al. 2012; Kazemi, Khajouei & Nasrabadi 2012; ISACA 2012; Bowen, Hash & Wilson 2006).

Dalam usaha untuk mengesahkan PKM dilaksana dengan betul dan berkesan, organisasi sewajarnya melaksana proses pengauditan (Islam, Farah & Stafford 2018; Razana & Shafiuddin 2016; MAMPU et al. 2016; IEC 2013a). Kelemahan dan ketidakpatuhan terhadap polisi, proses, prosedur dan kawalan boleh dikenal pasti semasa proses pengauditan (Noralinawati & Nor'ashikin 2018; Singh, Gupta & Ojha 2014; Chander, Jain & Shankar 2013; Yang 2011; Bowen, Hash & Wilson 2006). Proses pengauditan ini dilaksana oleh pasukan audit. Semasa proses pengauditan, program audit yang merangkumi perancangan audit, latihan dan pelaksanaan audit perlu diadakan (Bowen, Hash & Wilson 2006; Chander, Jain & Shankar 2013; Singh, Gupta & Ojha 2014; ISO/IEC 2013a; ISACA 2012). Di akhir proses pengauditan, laporan audit yang merangkumi penemuan audit harus dikeluarkan oleh pasukan audit untuk dilapor kepada pengurusan atasan dan pihak yang berkenaan (ISO/IEC 2013a). Sehubungan itu, pengetahuan, kemahiran dan komitmen pasukan audit adalah penting dalam menjaya pross pengauditan (Razana & Shafiuddin 2016; Singh, Gupta & Ojha 2014; Chander, Jain & Shankar 2013; ISO/IEC 2013a; ISACA 2012).

Proses pengauditan boleh dilaksana secara manual atau secara berkomputer mengguna perisian khas bagi memudahkan pasukan audit melaksana pengauditan (van der Nest, Smidt & Lubbe 2017). Penggunaan Infrasrtuktur ICT yang meliputi perisian dan perkakasan tertentu adalah perlu bukan sahaja untuk memudahkan proses pengauditan tetapi turut diguna untuk menyokong operasi keselamatan yang lain (Azah & Norizan 2013). Penggunaan perisian dan perkakasan terkini diperlukan bagi melindungi keselamatan maklumat organisasi (MAMPU et al. 2016; Chander, Jain & Shankar 2013; ISACA 2012).

Berdasarkan penyataan di atas, terdapat beberapa faktor dan elemen yang menyumbang kepada kejayaan PKM. Jadual 2.2 menyenarai faktor dan elemen kejayaan yang diperoleh dari beberapa kajian lepas, rangka kerja dan piawaian antarabangsa. Faktor dan elemen kejayaan tersebut telah disusun mengikut empat aspek iaitu manusia, dokumen organisasi, proses dan teknologi. Aspek manusia terdiri daripada individu atau pihak yang terlibat secara langsung dalam PKM. Faktor dalam aspek manusia ialah pengurusan atasan, pasukan pelaksana, pasukan audit, kakitangan dan pihak ketiga. Aspek dokumen organisasi pula merujuk kepada dokumen strategik

dan operasi yang perlu dibangun dan dipatuhi demi mencapai kejayaan PKM. Dua faktor yang dikenal pasti dalam aspek dokumen organisasi ialah polisi keselamatan dan prosedur keselamatan. Manakala aspek proses terdiri daripada aktiviti utama yang perlu dilaksana oleh pihak yang terlibat. Perancangan sumber, pengurusan risiko, pembangunan kompetensi dan latihan, pengurusan kesinambungan perkhidmatan dan pengauditan merupakan faktor dalam aspek proses. Akhir sekali aspek teknologi terdiri daripada faktor Infrastruktur ICT yang meliputi perkakasan dan perisian

Dapatan menunjukkan kebanyakan piawaian antarabangsa, rangka kerja dan kajian lepas bersetuju bahawa pengurusan atasan dan kakitangan merupakan faktor penting yang menyumbang kepada kejayaan PKM. Keperluan organisasi untuk mempunyai polisi keselamatan turut disokong oleh kebanyakan piawaian antarabangsa, rangka kerja dan kajian lepas. Di samping itu, faktor pembangunan kompetensi dan latihan juga dipersetujui menjadi penyumbang kepada kejayaan PKM. Faktor tersebut mengandungi elemen program latihan dan program kesedaran yang perlu dilaksana bagi memperoleh pengetahuan, mengasah kemahiran dan memupuk kesedaran kakitangan, individu dan pasukan yang terlibat. Selain itu, faktor perancangan sumber dan pengurusan risiko turut mendapat perhatian. Perancangan sumber terdiri daripada sumber manusia dan sumber kewangan yang diperlukan untuk melaksana aktiviti keselamatan. Pengurusan risiko pula terdiri daripada aktiviti penilaian risiko dan pemulihan risiko yang diperlukan untuk mengenal pasti, menganalisis dan mengawal risiko. Dalam pada itu, faktor pasukan pelaksana, pasukan audit, pihak ketiga, penguditan, pengurusan kesinambungan perkhidmatan, prosedur keselamatan dan infrastruktur ICT turut diberi dipersetujui oleh beberapa kajian lepas, rangka kerja dan paiwaian antarabangsa sebagai faktor yang menyumbang kepada kejayaan PKM.

Secara ringkasnya, sebanyak 13 faktor dan 32 elemen yang meliputi aspek teknikal dan bukan teknikal telah dikenal pasti menyumbang kepada kejayaan PKM. Faktor dan elemen kejayaan tersebut disatukan seperti di Rajah 2.3.

Jadual 2.2 Kajian lepas mengenai faktor kejayaan PKM

Aspek	Faktor dan elemen kejayaan	ISO 27001 & 27002	NIST 800-100	COBIT 5	ITIL	RAKKSSA	Sari et al. (2016)	Alnatheer (2015)	Nurazean et al. (2015)	Singh, Gupta & Ojha (2014)	Chander, Jain & Shankar (2013)	Kazemi, Khajouei & Nasrabadi (2012)	Woodhouse (2008)
Manusia	Pengurusan Atasan [Kepimpinan; Komitmen]	√	√	√	√		√	√	√	√	√	√	√
	Pasukan Pelaksana [Pengetahuan; Kemahiran; Komitmen]	√	√	√		√			√				
	Pasukan Audit [Pengetahuan; Kemahiran; Komitmen]	√		√		√				√	√		
	Kakitangan [Kesedaran; Kepatuhan; Motivasi]	√	√	√		√	√	√		√	√	√	√
	Pihak ketiga [Kesedaran; Kepatuhan]	√				√							

bersambung…

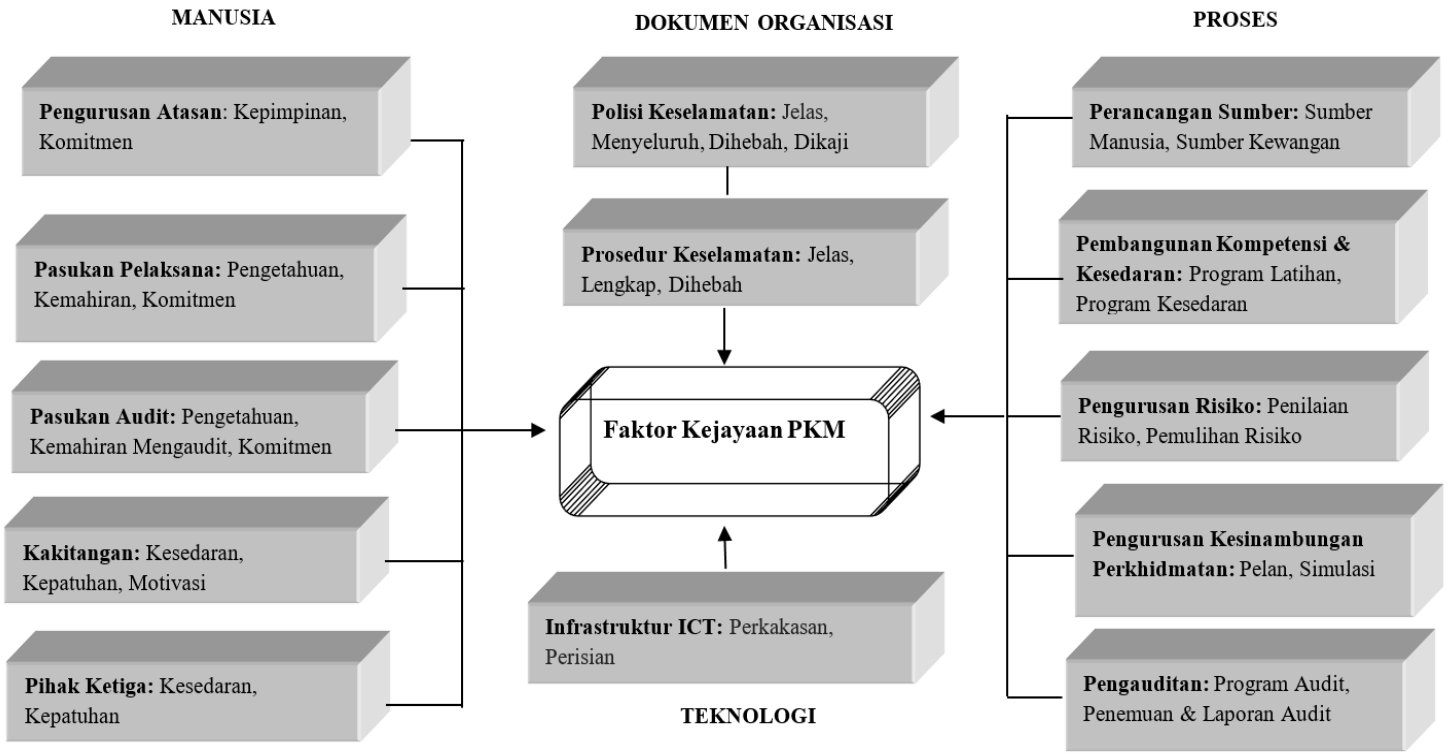
…sambungan

Dokumen Organisasi	Polisi Keselamatan [Menyeluruh; Jelas; Dihebahkan; Dikaji]	√	√	√	√	√	√	√	√	√	√
	Prosedur Keselamatan [Jelas; Lengkap; Dihebahkan]	√	√						√		
Proses	Pembangunan Kompetensi [Program Latihan; Program Kesedaran]	√	√	√		√	√	√	√	√	√
	Perancangan Sumber [Sumber Manusia; Sumber Kewangan]	√	√	√		√	√		√	√	
	Pengurusan Risiko [Penilaian Risiko; Pemulihan Risiko]	√	√	√	√	√		√		√	

bersambung…

…sambungan

	Pengurusan Kesinambungan Perkhidmatan [Pelan; Simulasi]	√ √			√	√				√	√
	Pengauditan [Program Audit; Penemuan & Laporan Audit]	√	√	√		√				√	√
Teknologi	Infrastruktur ICT [Perisian; Perkakasan]	√	√	√	√	√					√



Rajah 2.3 Faktor dan elemen kejayaan PKM

2.4 KEMATANGAN PKM

Bahagian ini menjelaskan definisi kematangan dalam perspektif PKM, teori pengukuran dan kematangan, serta model kematangan sedia ada yang dibangun oleh pengkaji terdahulu.

2.4.1 Definisi

Kematangan menggambarkan keadaan yang lengkap dan sempurna (Matrane et al. 2015). Kematangan dalam konteks PKM merujuk kepada keadaan di mana keselamatan maklumat organisasi telah menunjuk sifat matang daripada segi pengurusannya. (Matrane et al. 2015; Leem et al. 2008). Ia merupakan ukuran kepada keupayaan organisasi untuk melindungi dan mengekal keselamatan maklumatnya (Suhazimah, Ainin & Zolait 2009). Keperluan untuk mengukur kematangan PKM adalah untuk menjamin penggunaan sumber, amalan dan teknologi yang diguna adalah bersesuaian, berkesan dan mencapai objektif keselamatan maklumat (Anderson et al. 2014).

2.4.2 Teori Pengukuran

Teori pengukuran merupakan salah satu daripada cabang matematik yang diguna mengukur dan menganalisis data (Sarle 1995). Teori pengukuran dipopularkan dalam bidang psikologi oleh Stevens (1946) yang memperkenalkan idea skala pengukuran. Teori asas pengukuran menerangkan bahawa sifat alat pengukur mestilah tidak sama dengan objek yang hendak diukur (Sarle 1995). Pengukuran adalah pembandingan antara objek yang diukur dengan alat untuk mengukurnya.

Pengukuran dalam erti yang lebih luas juga boleh ditakrifkan sebagai proses pewakilan angka atau label kepada objek (pemboleh ubah) mengikut set peraturan tertentu (Stevens 1946; Kerlinger 1986). Set peraturan tertentu untuk memberi angka atau label bagi mengukur pemboleh ubah dinamakan skala pengukuran.

Terdapat empat jenis skala pengukuran asas iaitu skala nominal, skala ordinal, skala selang dan skala nisbah yang diguna untuk mengukur (Stevens 1946; Hand 1996; Chua 2011a).

- Skala nominal

Skala nominal ialah skala yang menggunakan angka untuk mewakili kategori sesuatu pemboleh ubah. Contoh pemboleh ubah skala nominal iaitu jantina, bangsa, agama dan negara. Bagi jantina, ia biasanya dikodkan menggunakan angka "1" dan "2" yang mewakili kategori "lelaki" dan "perempuan". Angka ini hanya mewakili jenis kategori dan tidak mempunyai makna pengiraan matematik. Maka nilainya tidak boleh ditambah, ditolak, didarab dan dibahagi (Chua 2011a).

- Skala ordinal

Skala ordinal ialah skala yang melibatkan data yang disusun secara teratur bermula dari angka atau peringkat yang lebih kecil kepada angka atau peringkat yang lebih besar. Skala ordinal umumnya diguna dalam mengukur pemboleh ubah untuk menunjukkan perbezaan peringkat dengan menggunakan nilai angka. Sebagai contoh, skala likert yang merupakan ordinal menggunakan angka 1,2,3,4 dan 5 untuk mewakili tahap persetujuan subjek mengenai sesuatu pernyataan seperti yang digambarkan pada Rajah 2.4.

Penyataan Item: Kerjasama berpasukan antara ahli pasukan audit perlu dipupuk bagi memudahkan urusan pengauditan.

1. Sangat tidak setuju
2. Tidak setuju
3. Kurang pasti
4. Setuju
5. Sangat setuju

Rajah 2.4 Contoh skala ordinal

- Skala selang

Skala nisbah melibatkan data yang disusun secara teratur bermula dari angka yang kecil mewakili nilai yang kecil kepada angka yang lebih besar yang mewakili nilai yang lebih besar. Skala selang mirip kepada skala nisbah namum skala selang ini tidak mempunyai nilai sifar. Skala ini menunjukkan angka yang sebenar. Angka yang terdapat dalam skala selang boleh digunakan dalam operasi matematik seperti pengurangan, pertambahan, pendaraban dan pembahagian. Contoh skala selang ditunjukkan dalam Rajah 2.5.

Penyataan Item: Berapa harikah anda hadir lewat ke pejabat dalam tempoh setahun?

1. 1 kali
2. 2 kali
3. 3 kali
4. 4 kali
5. 5 kali

Rajah 2.5 Contoh skala selang

- Skala nisbah

Skala nisbah melibatkan data yang disusun secara teratur bermula dari angka yang kecil mewakili nilai yang kecil kepada angka yang lebih besar yang mewakili nilai yang lebih besar. Skala ini mempunyai nilai sifar yang sebenar. Sebagai contoh, dalam satu ujian Sains Tingkatan 4, skor pelajar adalah antara 0 hingga 98. Angka 0 merupakan sifar sebenar kerana ia menunjukkan bahawa pelajar menjawab salah dalam kesemua soalan dalam ujian tersebut. Bagi skala ini, jarak antara satu angka dengan angka yang lain adalah sama dan pengiraan matematik yang menggunakan operasi tambah, tolak, bahagi dan darap boleh dilaksana.

Secara ringkasnya terdapat empat jenis skala pengukuran asas iaitu skala nominal, skala ordinal, skala selang dan skala nisbah yang diguna dalam mengukur sesuatu pemboleh

ubah atau objek. Skala ordinal merupakan skala yang paling banyak diguna pakai bidang penyelidikan. Ini kerana skala ordinal lebih mudah diguna bagi membuat analisis perbandingan dan kesimpulan (Chua 2011a).

2.4.3 Model Kematangan

Model kematangan merupakan rangka kerja berstruktur yang bertujuan untuk mengukur tahap perkembangan dan pembangunan aktiviti, projek atau program dalam sesebuah organisasi (Matrane et al. 2015, Goksen et al. 2015). Model kematangan juga bertujuaan mengenal pasti masalah semasa dan menentukan keutamaan dalam membuat penambahbaikan (Rosmiati, Riadi & Prayudi 2016). Ia membantu dalam menilai kekuatan dan kelemahan organisasi seterusnya membawa organisasi ke tahap kematangan yang lebih tinggi berdasar kepada matlamat yang ingin dicapai (Matrane et al. 2015; Leem et al. 2008).

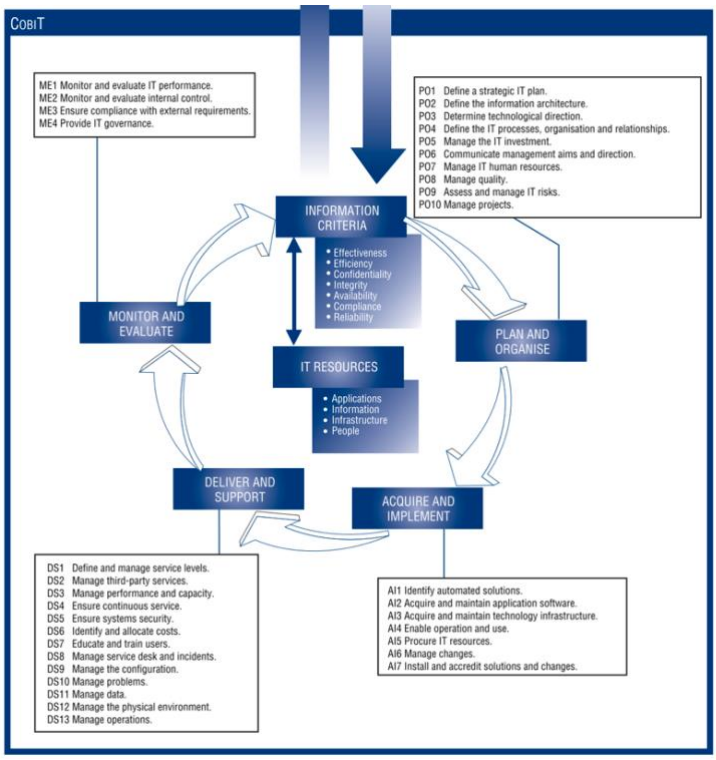
Orgnisasi yang pengurusan keselamatan maklumatnya berada pada tahap kematangan yang rendah menunjukkan bahawa terdapat kesukaran dalam mengguna, mengawal dan mengintegrasikan teknologi yang kompleks dalam amalan operasi (Anderson et al. 2014), manakala organisasi yang pengurusan keselamatan maklumatnya berada pada tahap kematangan yang tinggi menunjukkan bahawa amalan PKM berada dalam keadaan yang lengkap dan sempurna yang mana segala aspek dan sumber keselamatan maklumat dapat diurus, dikawal, diguna dan dipantau dengan berkesan (Mohd & Rozilawati 2011; Leem et al. 2008).

Dewasa ini, terdapat pelbagai model kematangan yang telah dibangun oleh badan antarabangsa, syarikat perunding, ahli akademik dan penyelidik bagi membantu organisasi untuk mengukur tahap kematangan proses pengurusan mereka. Antara model kematangan yang terawal dibangun dan sering dirujuk adalah *Control Objectives for Information and Related Technology* (COBIT 4.1) (ITGI 2007), *Information Security Management Maturity Model* (ISM3 1.0) (Aceituno 2004) dan *Capability Maturity Model Integration* (CMMI) (Kan 2002, CMMI 2010).

Model kematangan COBIT 4.1 telah dibangun oleh IT Governance Institute (ITGI) dan Information Systems Audit and Control Association (ISACA) bagi

membantu pihak pengurusan organisasi untuk menilai tahap kematangan proses pengurusan dan kawalan teknologi maklumat. Kawalan ini membantu mengoptimum pelaburan di dalam teknologi maklumat serta memastikan penyampaian perkhidmatan yang berterusan (Rigon et al. 2014). Berdasar kepada sejarah pembangunan COBIT, versi pertama COBIT telah dibangun pada tahun 1996 yang pada asalnya adalah sebagai satu set objektif kawalan untuk membantu komuniti audit kawangan bekerja dalam persekitaran ICT (Haes & Grembergen 2015; Stroud 2012). Seterusnya versi kedua dan ketiga dibangun pada tahun 1998 dan 2000 dengan skop yang lebih meluas. Bagi mengikut perkembangan teknologi semasa, komponen teknologi maklumat terkini yang meliputi pengurusan dan teknologi komunikasi kemudiannya ditambah dalam versi COBIT 4.1 yang diterbitkan pada tahun 2007.

Melalui model kematangan COBIT 4.1 ini, sebanyak empat domain (*Plan & Organise, Acquire & Implement, Deliver & Support; Monitor & Evaluate*) meliputi 34 proses dinilai dan setiap proses diperuntuk dengan pengukuran yang spesifik (Dirgahayu & Ariyadi 2015). Pecahan terhadap empat domain dan 34 proses ditunjukkan seperti Rajah 2.6.



Rajah 2.6 Domain dan proses COBIT 4.1

Penilaian dibuat berdasar kepada penelitian terhadap kesemua 34 proses melalui enam dimensi iaitu kesedaran dan komunikasi; dasar, rancangan dan prosedur; alatan dan automasi; kemahiran dan kepakaran; peranan dan tanggungjawab; dan penetapan dan pengukuran matlamat. Model kematangan ini dapat membantu pihak pengurusan dalam mengenal pasti prestasi sebenar organisasi, status semasa organisasi dan sasaran organisasi untuk penambahbaikan. Secara tidak langsung, organisasi dapat memperbaiki segala kelemahan yang wujud. Terdapat enam tahap pada skala kematangan model COBIT 4.1 ini yang dinilai dari tahap kematangan 0 hingga tahap 5. Penerangan setiap tahap adalah seperti di Jadual 2.3.

Jadual 2.3 Tahap kematangan model COBIT 4.1

Tahap	Penerangan Tahap
0 - Tidak Wujud	Tiada proses dikenal pasti dan diwujudkan.
1 - Permulaan / Awal	Organisasi mengenal pasti proses yang harus diwujudkan. Namun, pembangunan proses masih tidak teratur. Tindakan diambil berdasarkan situasi semasa.
2 - Berulang	Terdapat proses yang diwujudkan. Bagaimanapun, ia adalah berdasar kepada prosedur yang pernah dibuat oleh pihak lain yang menjalankan aktiviti yang hampir sama.
3 - Proses Ditakrifkan	Prosedur diwujudkan, didokumen dan dihebah kepada kakitangan organisasi. Setiap proses yang tedapat dalam prosedur diikuti. Namun, masih terdapat pelanggaran yang dikesan.
4 - Urus Dan Ukur	Pihak pengurusan memantau dan mengukur pematuhan terhadap prosedur yang dibangun dan mengambil tindakan terhadap proses yang kurang berkesan. Terdapat beberapa kaedah yang diguna untuk memantau proses yang terlibat.
5 - Optimum	Semua proses telah dilaksana dengan baik. Teknologi maklumat diguna secara menyeluruh dalam aliran proses kerja bagi meningkatkan kualiti dan keberkesanan kerja.

Model Kematangan Pengurusan Keselamatan Maklumat versi 1.0 (*Information Security Management Maturity Model*, ISM3 1.0) mendefinisi kematangan melalui proses pengurusan keselamatan maklumat berdasarkan kepada tiga aspek iaitu pengurusan strategik (*strategic management*), pengurusan taktikal (*tactical management*) dan pengurusan operasi (*operational management*) (Aceituno 2004).

Model ini dibina berdasar kepada piawaian, rangka kerja dan amalan terbaik sedia ada seperti CMMI, ITIL, ISO 9000, dan ISO 17799/27001. Penilaian kematangan dilaksana melalui pencarian bukti kewujudan proses dalam ketiga-tiga aspek pengurusan. Pengurusan strategik adalah berkaitan dengan penetapan matlamat dan perancangan sumber, pengurusan taktikal menjurus kepada pengurusan matlamat yang lebih spesifik dan pengurusan sumber, manakala pengurusan operasi adalah mencapai matlamat yang ditetapkan di dalam pengurusan strategik dan pengurusan taktikal. Sekumpulan proses dikelompok mengikut aspek seperti berikut.

- *Strategic management*
    - *SSP-1 Report to Stakeholders*
    - *SSP-2 Coordination*
    - *SSP-3 Strategic vision*
    - *SSP-4 Define TPSRSR rules*
    - *SSP-5 Check compliance with TPSRSR rules*
    - *SSP-6 Allocate resources for information security*
- *Tactical management*
    - *TSP-1 Report to strategic management*
    - *TSP-2 Manage allocated resources*
    - *TSP-3 Define Security Targets*
    - *TSP-4 Define metrics for security processes*
    - *TSP-5 Define Properties Groups*
    - *TSP-6 Define environments and lifecycles*
    - *TSP-7 Background Checks*
    - *TSP-8 Security Personnel Selection*
    - *TSP-9 Security Personnel Training*
    - *TSP-10 Disciplinary Process*
    - *TSP-11 Security Awareness*
    - *TSP-12 Select Specific Processes*
- *Operational management*
    - *OSP-1 Report to tactical management.*

- *OSP-2 Select tools for implementing security measures*
- *OSP-3 Inventory Management*
- *OSP-4 Information Systems Environment Change Control*
- *OSP-5 Environment Patching OSP-6 Environment Clearing*
- *OSP-7 Environment Hardening*
- *OSP-8 Software Development Lifecycle Control*
- *OSP-9 Security Measures Change Control*
- *OSP-10 Backup & Redundancy Management*
- *OSP-11 Access control over services, repositories channels and interfaces*
- *OSP-12 User Registration*
- *OSP-13 Encryption Management*
- *OSP-14 Physical Environment Protection Management*
- *OSP-15 Operations Continuity Management*
- *OSP-16 Segmentation and Filtering Management*
- *OSP-17 Malware Protection Management*
- *OSP-18 Insurance Management*
- *OSP-19 Attacks, Errors and Accidents Emulation (Internal Audit)*
- *OSP-20 Incident Emulation*
- *OSP-21 Information Quality Probing*
- *OSP-22 Alerts Monitoring*
- *OSP-23 Events Detection and Analysis*
- *OSP-24 Handling of incidents and near-incidents*
- *OSP-25 Forensics*

Tujuan utama model ISM3 1.0 ini dibangun adalah untuk mencegah serangan, kesilapan dan kemalangan yang boleh menjejas keselamatan sistem maklumat dan proses organisasi. Di samping itu, model ini turut memberi penerangan yang jelas berkenaan peranan dan tanggungjawab setiap kakitangan yang terlibat dalam setiap proses pengurusan.

Model ini menawarkan pendekatan baharu untuk menentu, melaksana, mengendali dan menilai sistem pengurusan keselamatan maklumat. Melalui penilaian yang dilaksana, model ini dapat menunjukkan perbezaan di antara tahap kematangan sebenar dan tahap kematangan sasaran (Aceituno 2004). Terdapat lima tahap kematangan pada model ISM3 1.0 bermula dari tahap 0 hingga tahap 4. Penerangan setiap tahap adalah seperti di Jadual 2.4.

Jadual 2.4 Tahap kematangan model ISM3 1.0

Tahap	Penerangan Tahap
0 - Tidak disyorkan	Risiko daripada ancaman teknikal tidak dapat dikurangkan.
1 -Sasaran keselamatan rendah dalam persekitaran berisiko rendah	Risiko daripada ancaman teknikal dapat dikurangkan.
2 - Sasaran keselamatan maklumat normal dalam persekitaran risiko biasa.	Risiko daripada ancaman teknikal dapat dikurangkan dengan lebih banyak.
3 - Sasaran keselamatan maklumat tinggi dalam persekitaran yang berisiko tinggi.	Risiko daripada ancaman teknikal dapat dikurangkan dengan lebih banyak berbanding tahap 1 dan 2.
4 - Sasaran keselamatan maklumat tinggi dalam persekitaran berisiko tinggi yang melibatkan keperluan khusus.	Pengurangan risiko daripada ancaman teknikal adalah paling tinggi.

CMMI adalah model kematangan yang menggabung beberapa badan disiplin serta badan pengetahuan seperti kejuruteraan sistem, kejuruteraan perisian dan pembekal luar. CMMI telah dibangunkan oleh Software Engineering Institute, Carnegei Melon University pasukan produk CMMI, serta pasukan pakar dari kerajaan dan industri untuk menambah baik *Software Capability Maturity Model* (SW-CMM) yang telah dikeluarkan pada tahun 1991(Kan 2002). Pasukan pembangun CMMI menyedari bahawa amalan terbaik yang digariskan untuk pembangunan perisian boleh digabungkan menjadi satu rangka kerja kemajuan proses. CMMI merupakan pendekatan peningkatan proses untuk membantu organisasi dalam mengetahui ciri keberkesanan setiap proses serta membantu organisasi dalam membangun pelan penambahbaikan proses. Versi awal CMMI adalah CMMI versi 1.0 yang telah diterbitkan pada tahun 2000.

CMMI versi 1.3 (v.1.3) dibangun pada tahun 2010 mengandungi tiga cabang iaitu CMMI-Pembangunan, CMMI-Perkhidmatan dan CMMI-Perolehan. Aspek keselamatan yang diterap di dalam CMMI v.1.3 terdapat dalam satu proses CMMI-Perkhidmatan iaitu pengurusan keselamatan dan empat proses CMMI-Pembangunan iaitu persediaan organisasi dalam keselamatan pembangunan, pengurusan keselamatan dalam projek, keperluan keselamatan dan penyelesaian teknikal, dan pengesahan keselamatan (Siemens 2013).

Terdapat 16 proses utama di dalam model CMMI v.1.3 ini yang perlu diukur. Setiap proses ini mempunyai matlamat yang ditetapkan untuk dicapai oleh organisasi. Setiap matlamat pula mempunyai amalan atau aktiviti yang perlu dilaksana. Model CMMI mempunyai lima tahap kematangan. Setiap tahap kematangan mempunyai sekumpulan proses yang perlu dilaksana. Tahap kematangan dinilai berdasar kepada pencapaian matlamat yang ditetapkan di dalam setiap proses. Penerangan setiap tahap adalah seperti di Jadual 2.5.

Jadual 2.5 Tahap kematangan model CMMI

Tahap	Penerangan Tahap
1 - Awal	Proses yang ada tidak menentu dan tidak dikawal dengan baik.
2 - Diuruskan	Proses dan keperluan diurus dengan baik. Setiap proses dirancang dan dilaksana.
3 - Ditakrifkan	Proses diperincikan dengan baik dan mudah difahami. Proses diurus dengan lebih proaktif .
4 – Diuruskan secara kuantitatif	Proses diukur sentiasa dan prestasi proses dikawal menggunakan teknik kuantitatif.
5 - Optimum	Proses sentiasa ditambahbaik. Organisasi telah mencapai matlamat yang ditetapkan.

Secara keseluruhan, ketiga-tiga model ini mempunyai persamaan dari segi penilaian iaitu menilai tahap kematangan berdasarkan proses kerja (Suhazimah & Zolait 2012). Namun begitu, proses kerja yang dinilai adalah berbeza antara satu sama lain. Ini kerana ketiga-tiga model dihasilkan berdasarkan domain yang tertentu.

Terdapat beberapa kajian daripada penyelidikan semasa yang mengguna model kematangan di atas sebagai asas untuk membangun model kematangan yang baharu. Sebagai contoh, model kematangan yang dibangun oleh *The Open Group* (TOG) dan diketuai oleh Vicente Aceituno selaku penulis utama telah menambah baik model kematangan ISM3 1.0 (Aceituno 2011). Model terkini yang diberi nama *Open Information Security Management Maturity Model* (O-ISM3) merupakan sebuah rangka kerja keselamatan maklumat yang bertujuan untuk memastikan proses keselamatan dilaksana dan beroperasi pada tahap yang selaras dengan keperluan perkhidmatan organisasi.

Proses keselamatan yang terdapat pada O-ISM3 masih mengikuti kebanyakan proses yang terdapat dalam ISM3 versi 1.0. Gabungan beberapa proses yang diamalkan pada tahap keupayaan tertentu menentukan tahap kematangan. Hubungan antara proses, keupayaan dan tahap kematangan adalah semakin banyak proses, semakin tinggi keupayaan, maka semakin tinggi tahap kematangan (TOG 2011). Rajah 2.7 menyenaraikan senarai proses yang terlibat dalam penilaian kematangan O-ISM3.

Generic Processes	Strategic – Specific Processes
GP-1: Knowledge Management GP-2: ISMS and Business Audit GP-3: ISM Design and Evolution	SSP-1: Report to Stakeholders SSP-2: Coordination SSP-4: Define TPSRSR Rules SSP-6: Allocate Resources for Information Security
Operational-Specific Processes	**Tactical-Specific Processes**
OSP-1: Report to Tactical Management OSP-2: Security Procurement OSP-3: Inventory Management OSP-4: Information Systems Environment Change Control OSP-5: Environment Patching OSP-6: Environment Clearing OSP-7: Environment Hardening OSP-8: Software Development Lifecycle Control OSP-9: Security Measures Change Control OSP-16: Segmentation and Filtering Management OSP-17: Malware Protection Management OSP-11: Access Control OSP-12: User Registration OSP-14: Physical Environment Protection Management OSP-10: Backup Management OSP-26: Enhanced Reliability and Availability Management OSP-15: Operations Continuity Management OSP-27: Archiving Management OSP-19: Internal Technical Audit OSP-20: Incident Emulation OSP-21: Information Quality and Compliance Probing OSP-22: Alerts Monitoring OSP-28: External Events Detection and Analysis OSP-23: Internal Events Detection and Analysis OSP-24: Handling of Incidents and Near-incidents OSP-25: Forensics	TSP-1: Report to Strategic Management TSP-2: Manage Allocated Resources T TSP-3: Define Security Targets TSP-4: Service-Level Management TSP-6: Define Environments and Lifecycles TSP-13: Insurance Management TSP-7: Background Checks TSP-8: Personnel Security TSP-9 Security Personnel Training TSP-10: Disciplinary Process TSP-11: Security Awareness TSP-14: Information Operations

Rajah 2.7 Proses O-ISM3

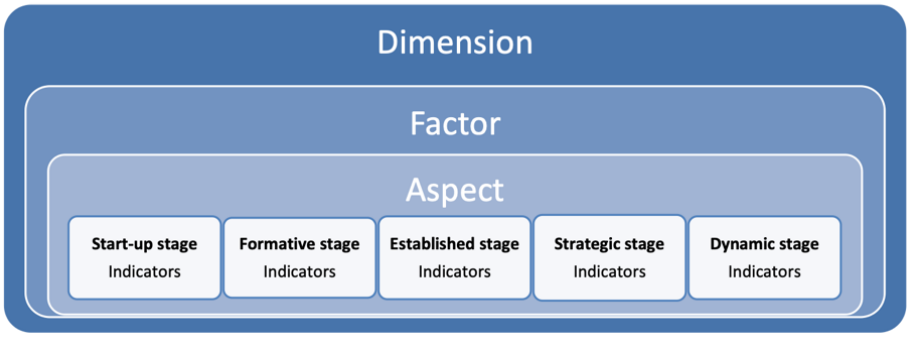
Global Capacity Security Capacity Centre (GCSCC) telah membangun prototaip kematangan yang diberi nama *Cyber Security Capability Maturity Model* (CMM) pada tahun 2014. Model ini kemudiannya disemak semula serta dibuat penambahbaikan pada tahun 2016 dan dikenali dengan nama baru iaitu *CyberSecurity Capability Maturity Model for Nations* (CMM).

Model CMM ini dibangun melalui kerjasama dengan beberapa rakan strategik GCSCC seperti *Organization of American States* (OAS), *World Bank, Commonwealth Telecommunications Organisation* (CTO) and the *International Telecommunication Union* (ITU). Pandangan panel penasihat daripada GCSCC dan beberapa pakar siber dari pelbagai domain diambil kira dalam pembangunan model tersebut.

Beberapa negara seperti Kosovo, Bhutan, Uganda, Senegal, Republik Kyrgyzstan, Cyprus, Lithuania, Madagaskar dan Indonesia merupakan antara negara

rintis yang telah mengguna pakai model CMM ini. Penggunaan model ini membolehkan badan kerajaan setiap negara menilai sendiri keselamatan keselamatan siber mereka.

CMM ini menilai kematangan melalui lima dimensi iaitu dasar dan strategi siber; budaya siber dan masyarakat; pendidikan keselamatan siber, latihan dan kemahiran; rangka kerja perundangan dan peraturan; dan piawaian, organisasi dan teknologi. Dalam setiap dimensi, terdapat beberapa faktor, aspek, tahap kematangan dan indikator (penunjuk) kapasiti keselamatan siber seperti yang digambarkan dalam Rajah 2.8. Dimensi merujuk kepada kluster kapisiti siber; faktor pula merujuk kepada elemen yang menyumbang kepada peningkatan kematangan kapasiti siber; manakala aspek pula adalah elemen yang terdapat dalam setiap faktor. Setiap aspek mengandungi beberapa petunjuk yang dipecahkan kepada beberapa tahap kematangan. Terdapat lima tahap kematangan bermula dari tahap permulaan (*start-up)* kepada tahap dinamik (*dynamic*) (GCSCC 2016) dalam model CMM. Rajah 2.9 menunjukkan contoh gabungan komponen yang terdapat dalam model CMM ini. Penggunaan model ini adalah dengan merujuk kepada setiap komponen yang terdapat dalam model ini. Penilaian dibuat dengan menilai komponen pada semua dimensi. Melalui penilaian yang dilaksana, status keselamatan siber negara yang mengguna pakai model ini dapat diperoleh.



Rajah 2.8 Komponen CMM

Dimension 1: Cybersecurity Policy and Strategy

D 1.1: National Cybersecurity Strategy					
Aspect	*Start-Up*	*Formative*	*Established*	*Strategic*	*Dynamic*
Strategy Development	No national cybersecurity strategy exists, although planning processes for strategy development may have begun. Advice may have been sought from international partners.	An outline/draft national cybersecurity strategy has been articulated. Processes for strategy development have been initiated. Consultation processes have been agreed for key stakeholder groups, including international partners.	A national cybersecurity strategy has been published. Multi-stakeholder consultation processes have been followed and observations fed back to the identified strategy 'owners'. National cybersecurity strategy is promoted and implemented by multiple stakeholders across government and other sectors.	Strategy review and renewal processes are confirmed. Regular scenario and real-time cyber exercises that provide a concurrent picture of national cyber resilience are considered a strategic priority. Relevant metrics, measurement, and monitoring processes, data, and historic trends are evaluated and inform decision-making. Cybersecurity strategic plans, aligned with national strategic priorities, drive capacity building and investments in security.	Continual revision and refinement of cybersecurity strategy is conducted proactively to adapt to changing socio-political, threat and technology environments. The country is a leader within the international community and the debate shaping the development of global cybersecurity strategy.
Organisation	No overarching national cybersecurity programme has been developed.	A coordinated cybersecurity programme is being developed through a multi-stakeholder consultative process. However, budgets reside in disparate public departments without a discrete cybersecurity budget line.	The single agreed cybersecurity programme has a designated coordinating body with a mandate to consult across public and private sectors, and civil society. The programme is defined according to goals and objectives, using metrics to measure progress. Discrete budget for cybersecurity exists, but is	Evidence exists of iterative application of metrics and resulting refinements to operations and strategy across government, including resource allocation considerations. A consolidated cybersecurity budget has been administered in order to allocate resources.	A singular national cybersecurity posture exists with the ability to reassign tasks and budgets dynamically according to changing risk assessments. A designated national body disseminates and receives feedback on the strategy from wider society to continuously enhance the national cybersecurity posture.

Rajah 2.9 Model CMM

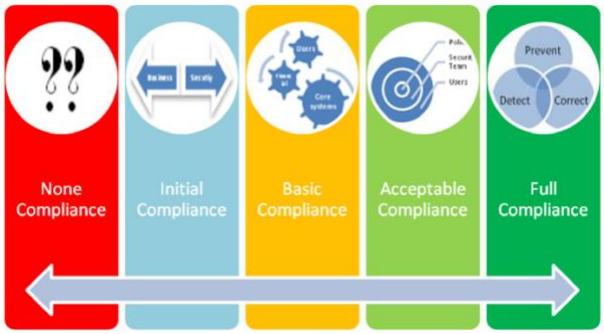
Mohd & Rozilawati (2011) telah mencadang model penilaian tahap pelaksanaan keselamatan maklumat berdasar kepada empat faktor iaitu manusia, teknologi, proses dan prosedur; dan penilaian risiko. Model ini mencadangkan beberapa dimensi pengukuran berdasarkan faktor yang disenarai. Pembangunan model ini dimulakan dengan kaedah *Systematic Literature Review* (SLR) sebagai instrumen untuk menentukan faktor dan dimensi pengukuran yang sesuai.

Untuk mengukur tahap kematangan pelaksanaan, setiap faktor diberikan dimensi yang membolehkannya untuk dikategorikan kepada tiga tahap kematangan iaitu asas (*bacis*), pertengahan (*intermediate*) dan maju (*advance*). Dimensi ditetapkan berdasarkan kepada darjah kepentingan. Rajah 2.10 menunjukkan model kematangan yang dicadangkan oleh Mohd & Rozilawati. Model yang dicadangkan ini boleh digunakan sebagai senarai semak penilaian kendiri (*self-assessment*) organisasi. Penilaian kendiri boleh dilakukan melalui temu bual personel utama, penyemakan dokumen dan pemeriksaan kawasan (*on-site*).

Level	Factor	Dimension
Level 1: Basic	People Process/Procedure Technology Risk Assessment	Low Low/Non-existence Non-existence Low
Level 2: Intermediate	People Process/Procedure Technology Risk Assessment	Moderate Moderate Low/Moderate Moderate
Level 3: Advanced	People Process/Procedure Technology Risk Assessment	High High High High

Rajah 2.10 Model penilaian tahap pelaksanaan keselamatan maklumat (Mohd & Rozilawati 2011)

Model kematangan yang dibangun oleh Saleh (2011) adalah bertujuan untuk menilai keupayaan organisasi dalam memenuhi objektif keselamatan. Model yang dibangun mentakrif proses mengurus, mengukur dan mengawal keselamatan berdasar kepada empat aspek iaitu tadbir urus, pengurusan keselamatan, senibina sistem dan pengurusan perkhidmatan. Setiap aspek mempunyai indikator tersendiri. Model ini mempunyai lima tahap pematuhan. Bermula dari tahap ketidakpatuhan sehingga ke tahap mematuhi sepenuhya aspek keselamatan seperti yang ditunjukkan pada Rajah 2.11.

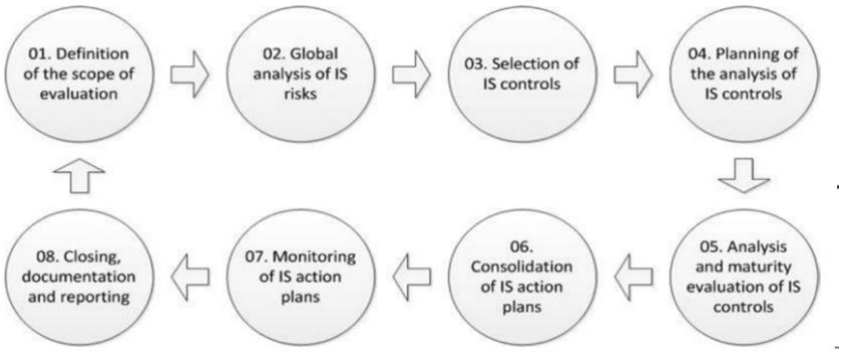


Rajah 2.11. Tahap pematuhan model kematangan Saleh 2011

Model ini mengguna kaedah soal selidik yang perlu dijawab oleh kakitangan organisasi. Soal selidik dipecahkan empat bahagian iaitu Bahagian 1: Tadbir Urus; Bahagian 2: Pengurusan Keselamatan; Bahagian 3: Senibina Sistem; dan Bahagian 4: Pengurusan perkhidmatan. Setiap bahagian perlu dijawab dan markah akan dikira

mengikut bahagiabn. Seterusnya markah setiap bahagian akan dikumpul dan digabung untuk menentukan tahap pematuhan keseluruhan.

Rigon et al. (2014) telah membangunkan sebuah model kitaran penilaian kematangan. Model ini mencadang proses penilaian kematangan secara berterusan dengan membentang lapan langkah yang perlu diikuti sepanjang melaksana penilaian seperti yang ditunjukkan dalam Rajah 2.12.



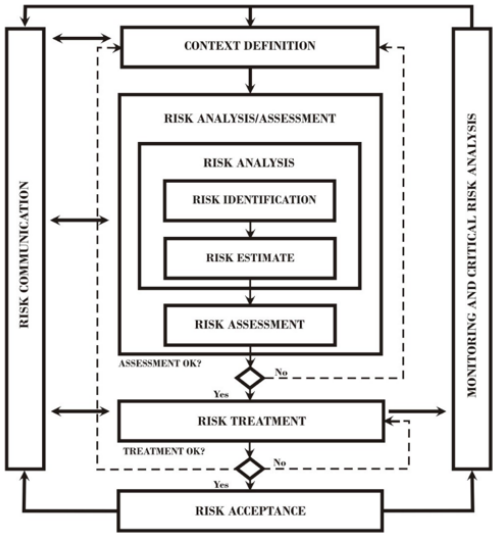
Rajah 2.12 Model kitaran penilaian kematangan

Langkah penilaian dimulakan dengan mendefinisikan skop penilaian dan diakhiri dengan penutupan, dokumentasi dan laporan. Pengukuran kematangan dibuat pada langkah yang kelima iaitu analisis dan penilaian kematangan. Kematangan diukur melalui keberkesanan proses yang terdapat dalam kawalan keselamatan. Kawalan keselamatan yang dinilai adalah berpandu kepada kawalan keselamatan yang dicadang oleh piawaian ISO/IEC 27002 seperti yang disenaraikan dalam Rajah 2.13. Setiap kawalan yang dinilai akan mempunyai tahap kematangan masing-masing. Tahap kematangan pada kajian ini adalah mengikut skala tahap kematangan COBIT 4.1.

Section	Description – ISO/IEC 27002
5	Security policy
6	Organizing information security
7	Asset management
8	Human resources security
9	Physical and environmental security
10	Communications and operations management
11	Access control
12	Information systems acquisition, development and maintenance
13	Information security incident management
14	Business continuity management
15	Compliance

Rajah 2.13. Kawalan keselamatan piawaian ISO/IEC 27002

Model yang dibangun Mayer & Fagundes (2009) pula telah memfokuskan kepada penilaian kematangan proses pengurusan risiko keselamatan maklumat. Model *Risk Management Maturity Model in Information Security* (MMGRseg) yang dibangun ini adalah berasaskan piawaian ISO/IEC 27005. Model ini mengambil kira beberapa elemen yang terdapat pada model kematangan Cobit 4.1 dan CMMI. Model ini menilai kematangan terhadap enam aktiviti pengurusan risiko iaitu definasi konteks (*context definition*), penilaian risiko (*risk analysis/assessment)*, pemulihan risiko (risk treatmenet), penerimaan risiko (*risk acceptance*), komunikasi risiko (*risk communication*) dan pemantauan analisis risiko kritikal (*monitoring & critical risk analysis*) seperti yang digambarkan dalam Rajah 2.14.



Rajah 2.14 Aktiviti pengurusan risiko keselamatan maklumat MMGRseg

Terdapat lima tahap kematangan yang dicadang dalam model ini iaitu Tahap 1 hingga Tahap 5. Bagi menilai tahap kematangan, setiap aktiviti pengurusan risiko ditetapkan objektifnya dan setiap objektif mempunyai indikator tersendiri. Setiap indikator pula disusun dan dikelompok mengikut tahap. Bagi memperoleh tahap yang dikehendaki, organisasi perlu melaksanakan indikator yang ditetapkan pada setiap tahap. Rajah 2.15 menunjukkan perhubungan antara aktiviti, indikator dan tahap kematangan yang tetdapat pada model ini.

Risk Management activities	Maturity Levels				
	Level 1	Level 2	Level 3	Level 4	Level 5
Context definition	No control is implemented	CD1.1, CD1.2 and CD1.3	CD1.4, CD1.5, CD1.6 and CD1.7	CD1.8	CD1.9
Risk Analysis/ Assessment	No control is implemented	AA1.1 and AA1.2	AA1.3, AA1.4 and AA1.5	AA1.6	AA1.7 and AA1.8
Risk Treatment	No control is implemented	RT1.1	RT1.2, RT1.3, RT1.4, RT1.5 and RT1.6	RT1.7	RT1.8
Risk Acceptance	No control is implemented	RA1.1 and RA1.2	RA1.3, RA1.4 and RA1.5	RA1.6	RA1.7
Risk Communication	No control is implemented	RC1.1	RC1.2 e RC1.3	RC1.4 and RC1.5	RC1.6
Monitoring and Critical Risk Analysis	No control is implemented	MA1.1	MA1.2 and MA1.3	MA1.4	MA1.5

Rajah 2.15 Perhubungan antara aktiviti, indikator dan tahap kematangan dalam MMGRseg

Jadual 2.6 membanding model yang dibincangkan. Jadual tersebut menunjukkan setiap model mempunyai fokus yang berbeza iaitu kematangan proses pengurusan dan kawalan teknologi maklumat (COBIT 4.1), kematangan proses dalam domain kejuruteraan (CMMI), kematangan proses pengurusan strategik, taktikal dan operasi (ISM3 1.0 & O-ISM3), kematangan kapisiti keselamatan siber (CMM), kematangan tahap pelaksanaan keselamatan maklumat (Mohd & Rozilawati 2011), kematangan organisasi dalam memenuhi objektif keselamatan (Saleh 2011), kematangan proses kawalan keselamatan maklumat (Rigon et al. 2014) dan kematangan proses pengurusan risiko (MMGRseg) (Mayer & Fagundes 2009). Bagaimanapun, kebanyakan model mempunyai skop pengukuran yang hampir sama iaitu mengukur pelaksanaan proses. Pengukuran yang terdapat pada model komersial sepeti COBIT 4.1, CMMI, dan CMM bersifat umum manakala pengukuran bagi model yang dibangunkan oleh penyelidik atau ahli akademik seperti ISM3, O-ISM3 dan MMGRseg lebih menjurus kepada aspek teknikal keselamatan maklumat. Dalam proses pembangunan pula, kebanyakan model komersial dibangunkan melalui perbincangan bersama antara pihak berkepentingan manakala model yang dibangun oleh ahli akademik pula melihat kepada perbandingan dan penambahbaikan model sedia ada.

Jadual 2.6 menunjukkan setiap model mempunyai tahap kematangan yang berlainan kecuali model yang dibangun oleh Rigon et al. (2014) yang mempunyai persamaan dengan tahap kematangan COBIT 4.1 (2007). Model COBIT 4.1 banyak digunakan dalam industri yang terlibat dalam teknologi maklumat, model CMMI pula dirujuk oleh kebanyakkan organisasi yang terlibat dalam kejuruteraan perisian

manakala model ISM3, O-ISM dan CMM banyak diguna pakai oleh organisasi yang menekankan kepada persekitaran keselamatan maklumat.

Jadual 2.6 turut menunjukkan terdapatnya faktor dan elemen kejayaan PKM seperti tertera pada Rajah 2.3 yang diambil kira sebagai dimensi pengukuran kematangan. Faktor dan elemen kejayaan yang diambil kira adalah berbeza bagi setiap model. Bagi aspek proses, program latihan, program kesedaran dan program audit merupakan elemen yang paling banyak dijadikan dimensi pengukuran dalam model yang dibincangkan. Selain itu, faktor pengurusan risiko yang terdiri daripada elemen penilaian dan pemulihan risiko turut diambil kira dalam kebanyakkan model kematangan. Tidak terkecuali juga faktor perancangan sumber yang meliputi elemen sumber manusia dan sumber kewangan turut dititikberatkan dalam beberapa model kematangan.

Bagi aspek teknologi pula, elemen perkakasan dan perisian turut diberi penekanan dalam kebanyakan model yang dibincang. Kewujudan elemen perkakasan dan perisian sebagai dimensi pengukuran menunjukkan bahawa kedua-dua elemen tersebut adalah penting dalam pelaksanaan PKM. Seterusnya, bagi aspek dokumen organisasi, faktor polisi dan prosedur keselamatan juga diberi perhatian sebagai dimensi pengukuran. Namun begitu, hanya sebilangan model sahaja yang menjadikan faktor tersebut sebagai dimensi pengukuran.

Berbanding aspek proses dan teknologi, faktor di bawah aspek manusia adalah yang paling kurang diberi perhatian dalam kebanyakan model kematangan. Sebilangan model mengambil kira faktor pengurusan atasan, pasukan pelaksana dan kakitangan. Manakala, faktor pasukan audit dan pihak ketiga tidak ditekankan sebagai dimensi pengukuran.

Secara ringkasnya, terdapat beberapa faktor dan elemen kejayaan PKM diambil kira sebagai dimensi pengukuran kematangan pada model yang dibincangkan. Rajah 2.16 memaparkan faktor dan elemen kejayaan PKM yang diambil kira dalam model kematangan yang dibincang. Melalui jadual 2.6 dan rajah 2.16 yang dipaparkan, didapati model sedia ada ini tidak mengguna keseluruhan faktor dan elemen kejayaan PKM. Model sedia ada juga kurang memberi penekanan terhadap faktor dan elemen

yang terdapat pada aspek manusia dan dokumen organisasi. Kebanyakan model memberi tumpuan kepada faktor dan elemen yang terdapat pada aspek proses dan teknologi.

Di samping itu, faktor dan elemen pengukuran yang dicadangkan oleh kebanyakan model sedia ada adalah bersendirian. Sebagai contoh, bagi faktor pengauditan, kebanyakan model hanya mengukur pelaksanaan program audit tanpa melihat kepada elemen penemuan dan laporan audit yang juga menyumbang kepada keberkesanan PKM.

Perkara ini menyebabkan penilaian kematangan yang dicadang oleh model sedia ada dibuat secara tidak menyeluruh kerana tidak meliputi kesemua aspek, faktor dan elemen kejayaan PKM. Model kematangan seharusnya mengambil kira kesemua aspek, faktor dan elemen kejayaan dan bukan melihat kepada beberapa aspek, faktor atau elemen sahaja. Dalam pada itu, kebanyakan model kematangan turut menghadkan pengukuran terhadap terhadap domain atau skop tertentu sahaja. Ini menyukarkan organisasi yang PKM mereka tidak termasuk dalam domain yang dihadkan untuk menyesuaikan model tersebut dengan keperluan organisasi.

Sehubungan itu, model kematangan yang holistik diperlukan dengan menggabung kesemua aspek, faktor dan elemen kejayaan bagi menjamin keberkesanaan PKM. Model kematangan yang tidak menghadkan mana-mana domain juga perlu dibangunkan bagi memastikan pelbagai organisasi boleh mengguna pakai model yang dicadang.

Jadual 2.6. Perbandingan model kematangan sedia ada

Model / Pengkaji	COBIT 4.1	ISM3 1.0	CMMI v.1.3	CMM	Rigon et al.	O-ISM3	Mohd & Rozilawati	Saleh	MMGRseg
Tahun	2007	2004	2010	2016	2014	2011	2011	2011	2009
Tujuan dan skop	Menilai kematangan setiap proses pengurusan dan kawalan teknologi maklumat.	Menilai kematangan setiap proses yang terdapat dalam tiga domain pengurusan iaitu pengurusan strategik, pengurusan taktikal dan pengurusan operasi	Menilai kematangan setiap proses dalam domain kejuruteraan	Menilai kapisiti keselamatan siber negara	Menilai kematangan proses kawalan secara berterusan	Menilai kematangan proses keselamatan maklumat yang merangkumi empat tahap pengurusan iaitu generik, strategik, taktikal dan operasi	Menilai tahap pelaksanaan pengurusan keselamatan maklumat	Menilai keupayaan organisasi dalam memenuhi objektif keselamatan	Menlai kematangan proses pengurusan risiko
Faktor / elemen kejayaan yang terlibat dalam penilaian	34 proses	43 proses	16 proses utama	Lima dimensi	Proses kawalan keselamatan		Empat aspek/faktor utama	Empat aspek/faktor utama	Lima aktiviti pengurusan risiko
Aspek Manusia									
1. Pengurusan Atasan									
- Komitmen	√				√		√	√	
-Kepimpinan	√				√			√	

bersambung…

…sambungan

2. Pasukan pelaksana									
- Pengetahuan	√			√					
- Kemahiran	√				√			√	
- Komitmen	√								
3. Pasukan Audit									
- Pengetahuan									
- Kemahiran									
- Komitmen									
4. Kakitangan									
-Kesedaran	√								
-Motivasi	√								
-Kepatuhan	√						√	√	
5. Pihak ketiga									
-Kesedaran									
-Kepatuhan									
Aspek Dokumen Organisasi									
1.Polisi									
-Menyeluruh	√	√		√					
-Jelas	√	√		√	√		√		
-Dihebah	√			√	√	√			
-Dikaji				√	√	√			
2. Prosedur									
- Jelas	√	√		√	√	√			
- Lengkap	√				√				
- Dihebah	√					√			
Aspek Proses									
1. Pembangunan kompetensi dan kesedaran									
-Program Latihan	√		√	√	√	√	√		
-Program Kesedaran	√	√		√	√	√	√	√	√

bersambung…

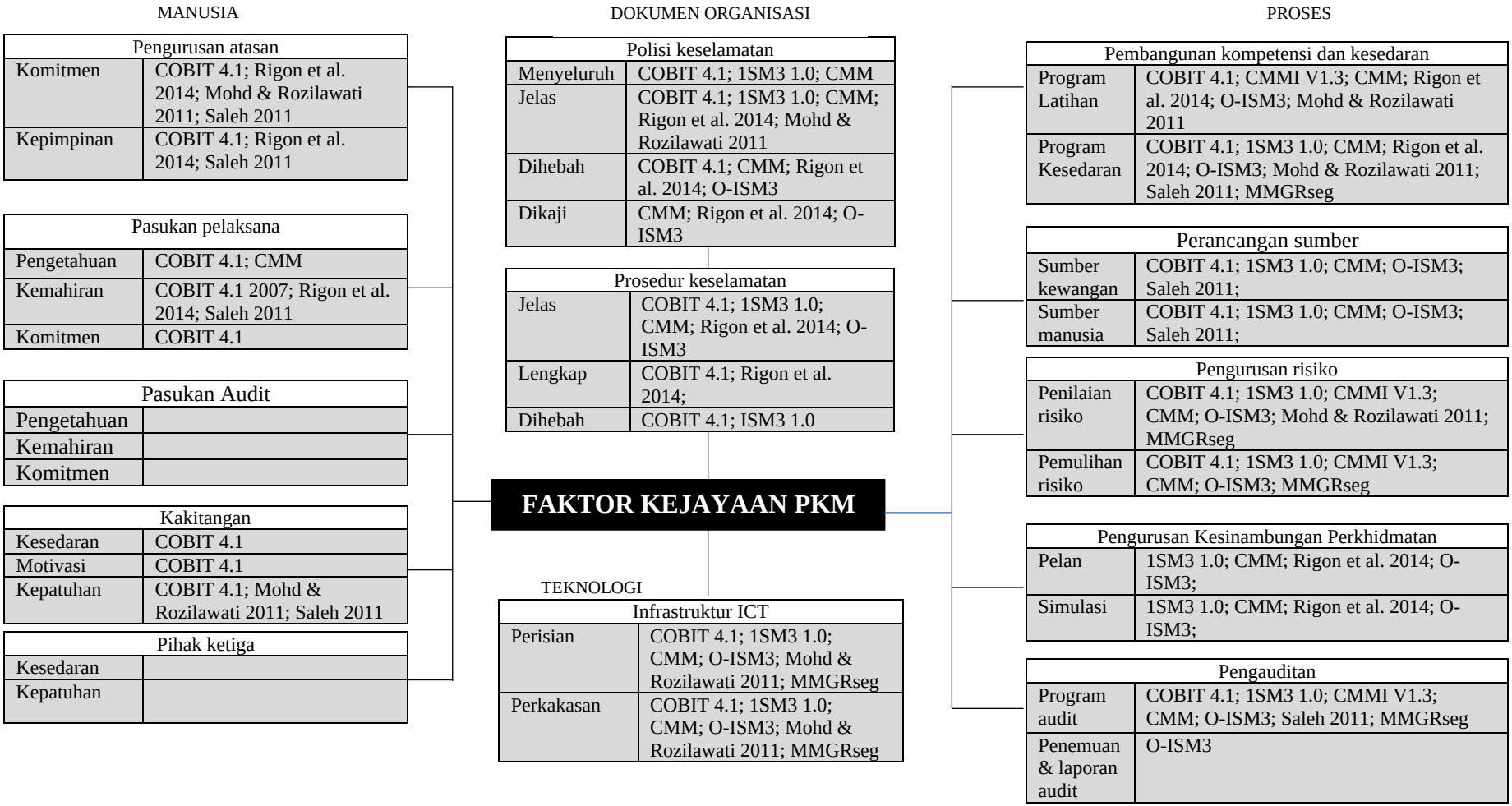
…sambungan

2. Perancangan sumber									
-Sumber kewangan	√	√		√		√		√	
-Sumber manusia	√	√		√		√		√	
3. Pengurusan risiko									
-Penilaian risiko	√	√	√	√		√	√		√
-Pemulihan risiko	√	√	√	√		√			√
4. Pengurusan Kesinambungan Perkhidmatan									
-Pelan		√		√	√	√			
-Simulasi		√		√	√	√			
5. Pengauditan									
-Program audit	√	√	√	√		√		√	√
-Penemuan & laporan audit						√			
Aspek Teknologi									
Infrastruktur ICT									
-Perisian	√	√		√		√	√		√
-Perkakasan	√	√		√		√	√		√
Kaedah penilaian	Berdasarkan ciri yang ditetapkan dalam tahap kematangan	Berdasarkan proses yang ditetapkan dalam tahap kematangan	Berdasarkan pencapaian matlamat	Berdasarkan ciri yang ditetapkan dalam tahap kematangan	Berdasarkan proses dan aktiviti yang menyokong kawalan	Berdasarkan komposisi proses dan keupayaan setiap proses	Metrik asas	Set soalan	Berdsarkan pencapaian sub-aktiviti dalam aktiviti utama

bersambung…

…sambungan

Skala / tahap kematangan	0 - Tidak Wujud 1 - Permulaan / Awal 2 - Berulang 3 - Proses Ditakrifkan 4 - Urus Dan Ukur 5 - Optimum	0 - Tidak disyorkan 1 - Sasaran keselamatan maklumat rendah 2 - Sasaran keselamatan maklumat normal 3 - Sasaran keselamatan maklumat tinggi dalam persekitaran yang berisiko tinggi. 4 - Sasaran keselamatan maklumat tinggi dalam persekitaran berisiko tinggi yang melibatkan keperluan khusus.	1 - Awal 2 - Diuruskan 3 - Ditakrifkan. 4 – Diuruskan secara kuantitatif 5 - Optimum	1 – Permulaan 2 – Formatif 3 – Stabil 4 – Strategik 5 - Dinamik	0 - Tidak Wujud 1 - Permulaan / Awal 2 - Berulang 3 - Proses Ditakrifkan 4 - Urus Dan Ukur 5 - Optimum	1 - Tahap 1 2 - Tahap 2 3 - Tahap 3 4 - Tahap 4 5 - Tahap 5	1- Asas 2 - Pertengahan 3 - Maju	- Kitadakpatuhan - Pematuhan awal - Pematuhan asas - Pematuhan yang boleh diterima - Pematuhan penuh	1- Permulaan 2-Diketahui 3-Seragam 4-Diurus 5-Optimum



Rajah 2.16 Pemetaan antara faktor kejayaan dan elemennya dengan model kematangan

2.4.4 Garis Panduan Pembangunan Model Kematangan

International Organization for Standardization (ISO) dan *International Electrotechnical Commission* (IEC) telah membangunkan satu piawaian ISO / IEC 33004:2015 *Information technology — Process assessment — Requirements for process reference, process assessment and maturity models* sebagai panduan dalam pembangunan model kematangan. Piawaian ini telah menggariskan keperluan yang perlu dipatuhi dalam pembangunan model rujukan proses, model penilaian proses, dan model kematangan.

Pembangunan sesebuah model kematangan perlu mengambil kira kepentingan organisasi dan tindakan yang diambil untuk mencapai persetujuan di dalam organisasi tersebut. Oleh demikian, model kematangan yang dibina harus mempunyai skop yang jelas. Hal ini perlu bagi memastikan semua objek yang dinilai kematangannya adalah termasuk dalam sempadannya.

Model kematangan yang dibangun juga harus bersandarkan sekurang-kurangnnya kepada satu model penilaian proses sedia ada. Proses yang dipilih haruslah berdasarkan skop yang dipersetujui.

Di samping itu, model kematangan juga perlu direka dalam bentuk skala ordinal yang mempunyai beberapa peringkat (angka / titik). Tahap kematangan perlu diperuntukan pada setiap peringkat tersebut. Tahap kematangan perlu menunjukkan peningkatan yang berterusan bermula daripada tahap yang paling rendah. Setiap tahap kematangan perlu mempunyai ciri-ciri tersendiri dan penerangan yang jelas (ISO/IEC 33004).

2.5 RUMUSAN

PKM adalah pendekatan strategik untuk menangani risiko, pelanggaran keselamatan dan mengurangkan insiden keselamatan yang boleh menjejaskan kerahsiaan, integriti dan ketersedian maklumat organisasi. Risiko, insiden dan pelanggaran keselamatan ini boleh diminimum sekiranya pihak organisasi dapat melaksana PKM secara berkesan.

Keberkesanan PKM boleh dicapai sekiranya organisasi menilai kematangan amalan PKM mereka menggunakan model kematangan yang holistik. Model kematangan yang holistik perlu mengambil kira faktor kejayaan PKM berserta elemennya demi memastikan penilaian dibuat secara menyeluruh.

Hasil daripada kajian kesusasteraan menunjukkan terdapat 13 faktor dan 32 elemen yang menyumbang kepada kejayaan PKM. Jadual 2.7 menyenarai faktor dan elemen yang dikenal pasti.

Jadual 2.7 Definisi faktor kejayaan PKM

Aspek	Faktor	Definisi	Rujukan
Manusia	Pengurusan Atasan	Pihak yang mempunyai kuasa penuh terhadap PKM organisasi. Pengurusan atasan perlu menunjukkan **kepimpinan** dan **komitmen** yang tinggi dalam memastikan kejayaaan PKM.	(Noralinawati & Nor'ashikin 2018; Sari et al. 2016; Alnatheer 2015; Bowen, Hash & Wilson 2006; Singh, Gupta & Ojha 2014; Chander, Jain & Shankar 2013; Kazemi, Khajouei & Nasrabadi 2012; Nurazean et al. 2015; Suhazimah & Zolait 2012; Hu et al. 2012; Cartlidge et al. 2012; ISO/IEC 2013a; ISACA 2012; Woodhouse 2008).
	Pasukan Pelaksana	Pihak yang bertanggungjawab dalam melaksanakan operasi keselamatan maklumat. Elemen yang diperlukan pada pasukan pelaksana adalah **pengetahuan** dalam domain keselamatan maklumat, **kemahiran** teknikal dan **komitmen** yang tinggi dalam melaksanakan operasi, proses dan prosedur keselamatan.	(Noralinawati & Nor'ashikin 2018; Nurazean et al. 2015; MAMPU et al. 2016; ISO/IEC 2013a; ISACA 2012; Bowen, Hash & Wilson 2006).
	Pasukan Audit	Pihak yang bertanggungjawab dalam memastikan kawalan, proses, prosedur dan aktiviti keselamatan dilaksana dengan betul. Pasukan audit perlu mempunyai **pengetahuan** terhadap perkara yang perlu di audit, mengaplikasi kemahiran **mengaudit** dan memberi	(Singh, Gupta & Ojha 2014; Chander, Jain & Shankar 2013; ISO/IEC 2013a; ISACA 2012).

bersambung…

…sambungan

		komitmen penuh sepanjang proses pengauditan.	
	Kakitangan	Kakitangan merujuk kepada pekerja tetap atau kontrak di dalam sesebuah organisasi. Elemen yang perlu ada pada setiap kakitangan adalah **kesedaran** dan **kepatuhan** terhadap polisi, arahan dan undang-undang keselamatan, serta sentiasa **bermotivasi** tinggi dalam mematuhi segala keperluan yang ditetapkan.	(MAMPU et al. 2016; Singh, Gupta & Ojha 2014; Chander, Jain & Shankar 2013; Alnatheer 2015; Woodhouse 2008; Kazemi, Khajouei & Nasrabadi 2012; Bowen, Hash & Wilson 2006;).
	Pihak Ketiga	Individu atau syarikat yang terlibat dalam membekal perkhidmatan kepada organisasi pada tempoh masa tertentu. Untuk memastikan maklumat organisasi kekal selamat, pihak ketiga perlu **sedar** dan **mematuhi** polisi keselamatan, undang-undang keselamatan dan kontrak yang ditandatangani.	(Mohd & Rozilawati 2011; Chander, Jain & Shankar 2013; ISO/IEC 2013a; ISACA 2012; Bowen, Hash & Wilson 2006;).
Dokumen Organisasi	Polisi Keselamatan	Hala tuju atau peraturan keselamatan peringkat tertinggi yang harus diikuti oleh seluruh kakitangan organisasi bagi melindungi aset ICT organisasi. Elemen yang perlu ada pada sesebuah polisi keselamatan adalah jelas, **menyeluruh**, sentiasa **dikaji** dan **dihebah** kepada seluruh kakitangan organisasi, pihak ketiga dan pihak berkepentingan.	(Noralinawati & Nor'ashikin 2018; Sari et al. 2016; MAMPU et al. 2016; Alnatheer 2015; Singh, Gupta & Ojha 2014; Chander, Jain & Shankar 2013; Kazemi, Khajouei & Nasrabadi 2012; Suhazimah & Zolait 2012; Hu et al. 2012; ISO/IEC 2013a; ISACA 2012; Cartlidge et al. 2012; Azhari 2008; Woodhouse 2008; Bowen, Hash & Wilson 2006).
	Prosedur Keselamatan	Tatacara dan panduan operasi sesebuah proses dan aktiviti keselamatan itu perlu dilaksana. Elemen yang harus pada prosedur keselamatan adalah **jelas**, **lengkap** dan **dihebah** kepada kakitangan dan pasukan yang terlibat dalam perlaksanaan operasi keselamatan.	(Bowen, Hash & Wilson 2006; Singh, Gupta & Ojha 2014; ISO/IEC 2013b).
Proses	Perancangan Sumber	Program merancang serta mengurus sumber bagi menyokong dan melaksana aktiviti dan operasi keselamatan. Perancangan sumber terbahagi kepada dua iaitu	(Noralinawati & Nor'ashikin 2018; Sari et al. 2016; MAMPU et al. 2016; Alnatheer 2015;

bersambung…

…sambungan

	perancangan **sumber kewangan** dan perancangan **sumber manusia**.	Chander, Jain & Shankar 2013; ISO/IEC 2013a; ISACA 2012; Bowen, Hash & Wilson 2006).
Pembangunan Kompetensi dan Kesedaran	Program untuk membangun kompetensi dan kesedaran kakitangan terhadap kepentingan keselamatan maklumat. Dua elemen penting adalah **program latihan** dan **program kesedaran**.	(Noralinawati & Nor'ashikin 2018; Sari et al. 2016; MAMPU et al. 2016; Kazemi, Khajouei & Nasrabadi 2012; Singh, Gupta & Ojha 2014; Chander, Jain & Shankar 2013; Alnatheer 2015; Hu et al. 2012; ISO/IEC 2013a; ISACA 2012; Bowen, Hash & Wilson 2006)
Pengurusan Risiko	Proses bagi mengenal pasti, menganalisis dan mengukur tahap risiko aset maklumat seterusnya mengambil tindakan untuk mengawal risiko. Dua aktiviti penting dalam pengurusan risiko adalah **penilaian risiko** dan **pemulihan risiko.**	(MAMPU et al. 2016; Alnatheer 2015; Singh, Gupta & Ojha 2014; ISO/IEC 2013a; Chander, Jain & Shankar 2013; ISACA 2012; Mohd & Rozilawati 2011; Suhazimah & Zolait 2012; Hu et al. 2012; Cartlidge et al. 2012; Saleh & Alfantookh 2011; Yang 2011; Woodhouse 2008; Bowen, Hash & Wilson 2006).
Pengurusan Kesinambungan Perkhdmatan (PKP)	Proses yang diperlukan untuk memastikan perkhidmatan organisasi berjalan lancar semasa atau selepas berlakunya insiden keselamatan atau bencana. Elemen penting pada pengurusan kesinambungan perkhidmatan adalah **pelan** dan **simulasi**.	(Aisyah et al. 2015; Singh, Gupta & Ojha 2014; Chander, Jain & Shankar 2013; ISO/IEC 2013b; Cartlidge et al. 2012).
Pengauditan	Proses untuk mengukur, memantau, menilai pelaksanaan PKM. Dua elemen penting dalam pengauditan adalah **program audit**, dan **laporan serta penemuan audit.**	(Islam, Farah & Stafford 2018; Chander, Jain & Shankar 2013; Singh, Gupta & Ojha 2014; ISO/IEC 2013a; ISACA 2012;

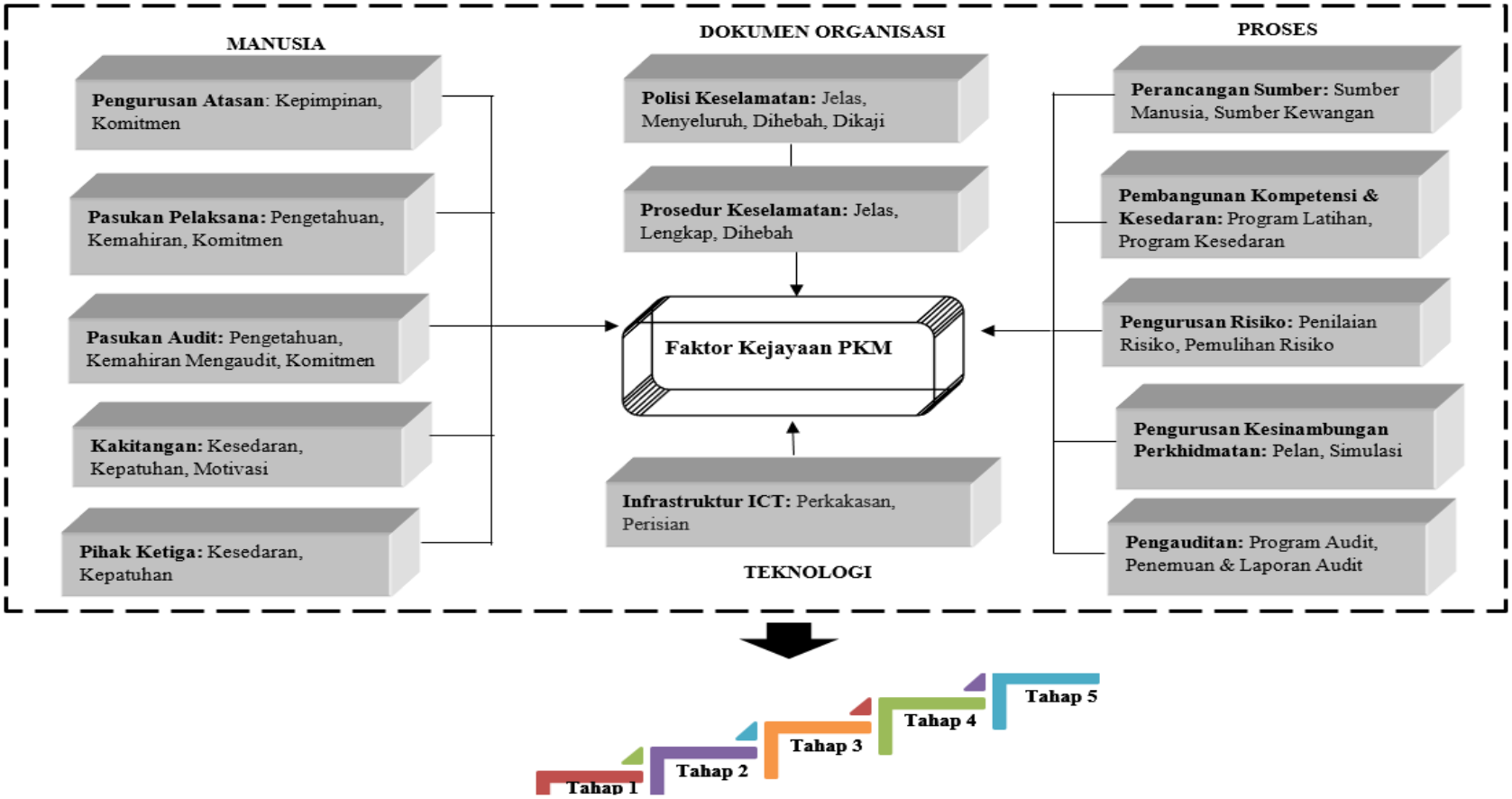
bersambung…

…sambungan

			Bowen, Hash & Wilson 2006)
Teknologi	Infrastruktur ICT	Infrastruktur ICT yang terdiri daripada **perkakakasan** dan **perisian** adalah prasarana asas yang digunakan untuk menyokong pelaksanaan PKM.	(MAMPU et al. 2016; Azah & Norizan 2013; Chander, Jain & Shankar 2013; ISO/IEC 2013a; ISACA 2012; Cartlidge et al. 2012; Woodhouse 2008; Bowen, Hash & Wilson 2006).

Faktor berserta elemennya yang disenarai di Jadual 2.7 dijadikan asas dalam pembangunan model kematangan PKM yang dicadang. Penggunaan kesemua faktor yang disenarai adalah kerana faktor tersebut merangkumi pelbagai aspek yang menyumbang kepada kematangan dan keberkesanan amalan PKM. Pembangunan model kematangan PKM turut bersandar kepada piawaian antarabangsa ISO / IEC 33004:2015 *Information technology — Process assessment — Requirements for process reference, process assessment and maturity models* serta teori pengukuran Stevens (1946) dan Sarle (1995) yang menetapkan dua ciri dalam sesebuah pengukuran iaitu pemboleh ubah (objek) serta alat pengukur (instrumen). Faktor berserta elemennya dari Jadual 2.7 dijadikan pemboleh ubah yang diukur manakala skala pengukuran ordinal merupakan instrumen untuk mengukur faktor dan elemen tersebut.

Model kematangan PKM digambarkan seperti di Rajah 2.17 yang menggambarkan ringkasan idea terhadap kajian ini yang mana faktor kejayaan diukur untuk menentukan tahap kematangan PKM.



Rajah 2.17 Model konsep penilaian kematangan PKM

2.6 KESIMPULAN

Bab ini membincangkan sorotan susastera mengenai PKM. Dapatan kajian mendapati pengukuran kematangan adalah penting untuk menilai amalan semasa pelaksanaan PKM bagi mengurangi insiden dan perlanggaran keselamatan. Bagi tujuan tersebut, pelbagai model kematangan telah dibangun dalam kajian lepas. Namun begitu, kebanyakan model bukan merupakan model terbaik untuk menilai secara keseluruhan amalan PKM. Ini kerana kebanyakan model mengukur kematangan melalui perspektif tertentu. Sehubungan itu, model pengukuran kematangan berasaskan faktor kejayaan yang meliputi pelbagai aspek perlu dibangunkan. Soroton susastera mendapati terdapat pelbagai faktor kejayaan yang terangkum dalam PKM. Dapatan kajian teoritikal ini diuji secara empirikal dan dibincang di Bab IV.

BAB III

METODOLOGI KAJIAN

3.1 PENGENALAN

Bab ini menyentuh dengan lebih mendalam pendekatan yang diguna untuk mencapai objektif kajian. Bab ini dimulakan dengan membentang metodologi keseluruhan kajian pada bahagian 3.2. Ini diikuti dengan fasa kajian pada bahagian 3.3 sehingga 3.6 yang menghuraikan kaedah, pensampelan, instrumen, protokol dan analisis kajian.

3.2 METODOLOGI KESELURUHAN

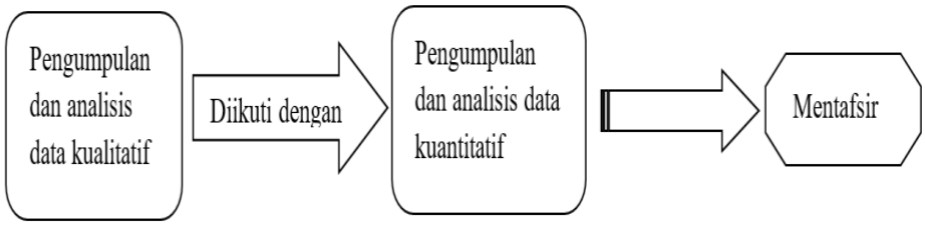
Metodologi kajian ditakrif sebagai kaedah saintifik dalam mereka bentuk, mengumpul dan menganalisis data bagi menghasilkan bukti yang boleh menyokong sesuatu kajian. Kaedah ini terbahagi kepada tiga iaitu kaedah kualitatif, kaedah kuantitatif dan kaedah mod campuran yang menggabungkan kaedah kualitatif dengan kuantitatif (Creswell 2014). Kaedah kualitatif merupakan kaedah yang diguna apabila penyelidik ingin membentuk teori asas, menjelas kefahaman atau memperoleh data yang mendalam terhadap domain yang dikaji. Kaedah kuantitatif pula diguna apabila penyelidik ingin menguji teori atau hipotesis, menunjukkan perhubungan faktor atau mengukur model komplek (Creswell 2014).

Metodologi bagi kajian ini adalah kaedah mod campuran. Kaedah mod campuran dipilih kerana pengunaan satu jenis kaedah kajian tidak mencukupi untuk menjawab persoalan kajian. Dapatan daripada data kualitatif dan kuantitatif mungkin berbeza dan tidak dapat diketahui dengan hanya mengumpul data daripada satu kaedah

sahaja. Oleh itu, kaedah mod campuran diguna kerana data daripada gabungan kaedah kualitatif dan kuantitatif dapat memberi memberi jawapan yang menyeluruh kepada persoalan kajian di samping membantu meningkatkan tahap pengesahan kajian (Creswell 2014; Marfizah 2016).

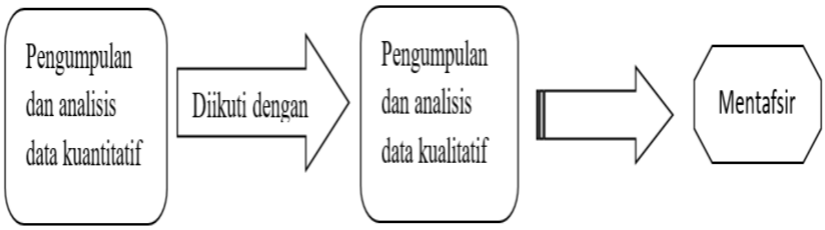
Kaedah mod campuran mengandungi empat jenis reka bentuk iaitu reka bentuk berurutan penerokaan (exploratory sequential design), reka bentuk berurutan penerangan (explanatory sequential design), reka bentuk selari bertumpu (convergent parallel design) dan reka bentuk penerapan (embedded design) (Creswell 2014; Cameron 2009).

Reka bentuk berurutan penerokaan bermula dengan pengumpulan dan analisis data kualitatif diikuti dengan kaedah pengumpulan dan analisis data kuantitatif. Tujuan reka bentuk penerokaan ini adalah untuk mengesah atau mengukur hasil kualitatif. Berdasarkan hasil kedua-dua kaedah, tafsiran dilakukan. Rajah 3.1 menunjukkan reka bentuk berurutan penerokaan.



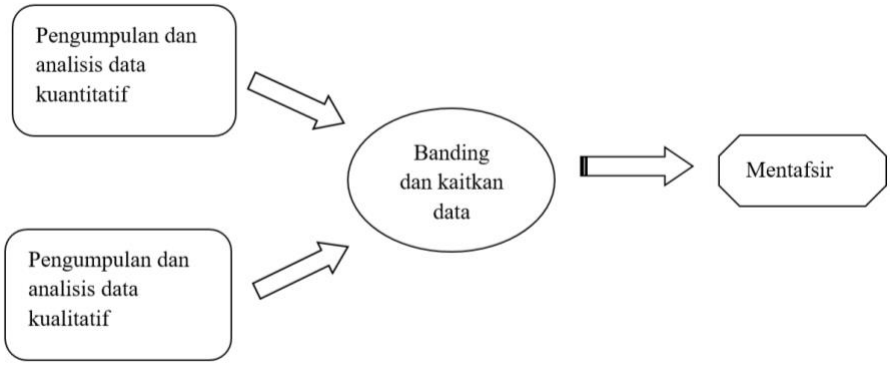
Rajah 3.1 Reka bentuk berurutan penerokaan

Reka bentuk berurutan penerangan dimulai dengan pengumpulan dan analisis data kuantitatif diikuti dengan pengumpulan dan analisis data secara kualitatif. Tujuan reka bentuk berurutan penerangan ini adalah untuk menjelaskan keputusan kuantitatif. Tafsiran dilaksana berdasarkan hasil kedua-dua kaedah. Rajah 3.2 menggambarkan reka bentuk berurutan penerangan.



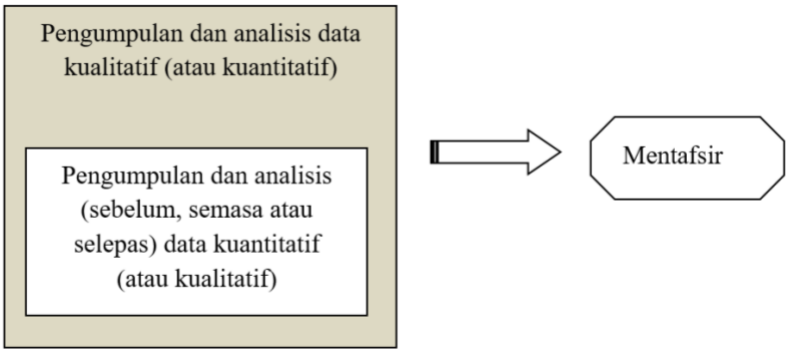
Rajah 3.2 Reka bentuk berurutan penerangan

Reka bentuk selari bertumpu (convergent parallel design) melibatkan pengumpulan data serta analisis data kualitatif dan kuantitatif secara serentak. Hasil daripada kedua-dua kaedah ini dibuat perbandingan dan dikait antara satu sama lain. Seterusnya, tafsiran dilaksana. Reka bentuk selari bertumpu digambarkan seperti Rajah 3.3.



Rajah 3.3 Reka bentuk selari bertumpu

Reka bentuk penerapan pula merupakan kaedah kualitatif yang diterap di dalam kaedah kuantitatif atau sebaliknya. Reka bentuk penerapan diguna apabila penyelidik memerlukan penerokaan awal sebelum melaksana kajian, memerlukan pemahaman yang lebih lengkap mengenai pelaksanaan kajian dan memerlukan penjelasan susulan selepas pelaksanaan kajian. Rajah 3.4 menunjukkan reka bentuk penerapan.



Rajah 3.4 Reka bentuk penerapan

Gabungan reka bentuk berurutan penerokaan dan berurutan penerangan dipilih sebagai reka bentuk kaedah mod campuran bagi kajian ini. Oleh kerana kajian ini melibatkan pelbagai aspek seperti pengumpulan dan pengesahan faktor kejayaan serta penentuan pengukuran dan tahap kematangan, maka gabungan reka bentuk berurutan penerokaan dan berurutan penerangan ini adalah sesuai digunakan. Gabungan kedua-dua reka bentuk ini diguna pada tiga sub-kajian empirikal iaitu kajian empirikal A, B, dan C seperti yang ditunjukkan dalam Rajah 3.5. Penerangan terperinci penggunaan gabungan kedua-dua reka bentuk ini diterang pada bahagian 3.4.

Kajian mod campuran ini melibatkan empat fasa utama iaitu kajian teoritikal, kajian empirikal, pembangunan model dan penilaian model. Kajian dimulakan dengan fasa kajian teoritikal yang merupakan kajian sorotan susastera. Ini diikuti dengan fasa kajian empirikal yang dibahagi kepada tiga sub-kajian iaitu kajian empirikal A, B dan C. Hasil daripada kajian empirikal dibawa kepada fasa seterusnya iaitu pembangunan model. Kajian ini diakhiri dengan fasa penilaian model yang melibatkan penilaian melalui pakar bidang dan kajian kes untuk menilai ketepatan dan kebolehlaksanaan model yang dibangan.

Rajah 3.5 menunjukkan metodologi kajian keseluruhan yang merangkumi kesemua fasa yang terlibat disusuli oleh penerangan terperinci bagi setiap fasa di bahagian seterusnya.

Fasa 1: Kajian Teoritikal	Fasa 2: Kajian Empirikal Empirikal A, B dan C	Fasa 3: Pembangunan model	Fasa 4: Penilaian model
Tujuan: Memperoleh kefahaman awal mengenai bidang kajian. Aktiviti: Menjalankan kajian susastera untuk penyataan masalah, persoalan kajian, objektif dan skop kajian. Menjalankan kajian susastera untuk mengenal pasti faktor kejayaan PKM dan model kematangan sedia ada. Menganalisis hasil kajian dengan menggunakan kaedah analisis kandungan. Hasil: Penyataan masalah, persoalan kajian, objektif, skop dan model konsep.	**Kajian empirikal A** Tujuan: Mengesah faktor kejayaan PKM yang diperoleh daripada kajian teoritikal dan mengenal pasti faktor kejayaan PKM yang baharu melalui kajian empirikal A. Aktiviti: Merancang kajian empirikal A: pensampelan, protokol, instrumen dan ujian rintis. Menjalankan kajian kualitatif secara temu bual individu dan kumpulan fokus. Menganalisis data kajian mengguna kaedah analisis kandungan. **Kajian empirikal B** Tujuan: Mengesah faktor kejayaan PKM yang diperoleh daripada hasil kajian empirikal A. Aktiviti: Merancang kajian empirikal B: pensampelan, protokol, instrumen dan ujian rintis. Menjalankan kajian kuantitatif secara soal selidik. Menganalisis data kajian menggunakan kaedah analisis statistik. **Kajian empirikal C** Tujuan: Menentu pengukuran dan tahap kematangan. Aktiviti: Merancang kajian empirikal C: pensampelan, protokol, instrumen dan ujian rintis. Menjalankan kajian kualitatif secara temu bual pakar. Menganalisis data kajian menggunakan kaedah analisis kandungan. Hasil: Faktor kejayaan, pengukuran dan tahap kematangan (Objektif i dan ii).	Tujuan: Membangunkan model kematangan PKM. Aktiviti: Membangunkan model kematangan dengan menggabung faktor kejayaan PKM, pengukuran dan tahap kematangan setiap faktor. Menentukan kaedah untuk mendapatkan tahap kematangan keseluruhan. Hasil: Cadangan Model Kematangan PKM (Objektif iii dan Objektif iv).	Tujuan: Menilai ketepatan dan kebolehlaksanaan model. Aktiviti: Merancang penilaian: pensampelan, instrumen, dan protokol Menjalankan penilaian model secara temu bual pakar dan kajian kes Menganalisis data penilaian menggunakan kaedah analisis kandungan. Hasil: Model Kematangan PKM (Objektiv v).

Rajah 3.5 Metodologi keseluruhan kajian

3.3 FASA 1 - KAJIAN TEORITIKAL

Tujuan kajian teoritikal dilaksana adalah untuk memberi kefahaman awal mengenai bidang kajian. Kajian teoritikal memberi tumpuan kepada pemahaman konsep secara meluas dalam memahami isu dan permasalahan semasa bidang yang dikaji. Isu dan permasalahan yang diperoleh disimpulkan menjadi pernyataan masalah, diikuti dengan penjanaan persoalan serta objektif kajian, penentuan skop kajian dan pembangunan model konsep.

Pelaksanaan kajian teoritikal ini melibatkan sorotan susastera terhadap dokumen yang diterbitkan dan tidak diterbitkan. Dokumen terdiri daripada buku rujukan yang berkaitan dengan bidang kajian, artikel jurnal dan prosiding yang diperoleh melalui carian pelbagai pangkalan data atas talian seperti ACM Digital Library, Scopus, Science Direct, Web of Science, Proquest, CiteSeer dan Google Scholar, tesis penyelidikan, piawaian antarabangsa, laporan tahunan dan dasar keselamatan yang dikeluarkan oleh organisasi tertentu. Bagi menjamin dokumen yang diperoleh adalah bersesuaian dengan persoalan dan objektif kajian, pencarian dokumen dilaksana dengan menetap beberapa kriteria seperti berikut:

a) Merangka kata kunci utama

Kata kunci utama dirangka bagi memudahkan pencarian dokumen. Kata kunci yang dirangka adalah “Pengurusan Keselamatan Maklumat”, “Faktor Kajayaan”, dan “Model Kematangan”. Ketiga-tiga kata kunci ini kemudiannya diterjemah ke dalam Bahasa Inggeris berikutan kebanyakan artikel jurnal dan prosiding diterbit di dalam bahasa tersebut. Kata kunci yang diterjemah menjadi: “Information Security Management”, “Success Factors” dan “Maturity Model”.

b) Mengenal pasti perkataan lain yang sinonim dengan kata kunci

Perkataan lain yang sinonim dengan kata kunci juga dikenal pasti untuk pencarian dokumen yang lebih menyeluruh. Jadual 3.1 menyenarai kata kunci dan istilah yang sinonim dengannya.

Jadual 3.1 Kata kunci dan sinonim

Kata Kunci	Istilah Sinonim / singkatan
"Information Security Management"	"Information Security", "Information Management", "ISM", "IS"
"Success Factors"	"Key Factors", "Critical Factors", "Factors"
"Maturity Model"	"Maturity Framework"

c) Membentuk rentetan pertanyaan carian

Rentetan pertanyaan carian dibentuk berdasarkan senarai kata kunci yang dikenal pasti. Retetan pertanyaan carian dibentuk mengguna operator asas Boolean. Antara rentetan pertanyaan carian yang dibentuk adalah seperti berikut:

i. ("*Information Security Management*" OR "*Information Security*" OR "*Information Managemen*t" OR "ISM" OR "IS") AND ("*Success Factors*" OR "*Key Factors*" OR "*Critical Factors*" OR "*Factors*")

ii. ("*Information Security Management*" OR "*Information Security*" OR "*Information Management*" OR "ISM" OR "IS") AND ("*Maturity Model*" OR "*Maturity Framework*")

d) Menentukan kriteria penerimaan dan penolakan

Kriteria penerimaan merupakan ciri yang perlu ada pada sesebuah dokumen yang diterima sebagai rujukan dalam penyelidikan manakala kriteria penolakan adalah ciri yang menyebabkan dokumen tersebut disingkir daripada senarai rujukan penyelidikan.

Kriteria penerimaan bagi kajian ini adalah seperti berikut:

i. Dokumen yang membincangkan faktor dan elemen kejayaan PKM.

ii. Dokumen yang membincangkan model kematangan PKM.

Kriteria penolakan bagi rujukan kajian ini adalah seperti berikut:

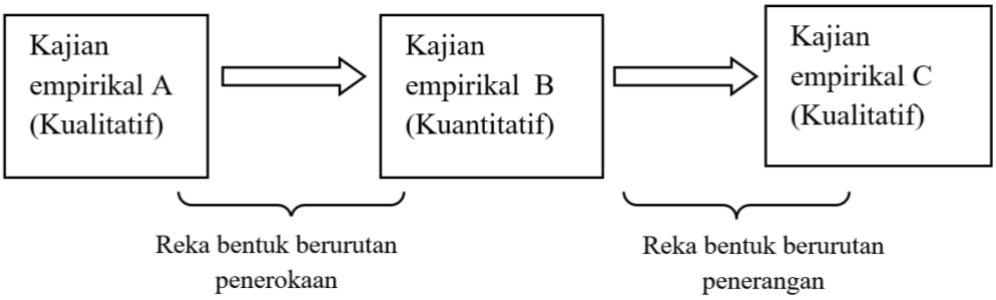
i. Dokumen yang tidak berpadanan dengan kriteria penerimaan kajian.

ii. Dokumen yang tidak disertakan dengan teks penuh.

Setelah melaksanakan kriteria penerimaan dan penolakan rujukan, dokumen yang menepati kriteria pencarian yang ditetapkan kemudiannya dimuat turun dan dianalisis mengguna kaedah analisis kandungan. Kaedah analisis kandungan adalah kaedah kualitatif yang diguna untuk menganalisis data penulisan, data lisan atau mesej komunikasi secara visual (Krippendorff 2013; Elo & Kyngas 2007). Ia merupakan kaedah untuk mengkategori teks dalam konsep dan kod yang tertentu secara sistematik dan berulang. Penerangan kaedah ini akan diterang di bahagian 3.4.1 (d). Hasil daripada analisis adalah model konsep seperti yang ditunjuk di Bab II bahagian 2.5.

3.4. FASA 2 - KAJIAN EMPIRIKAL

Kajian empirikal merupakan penyelidikan yang mengumpul data melalui proses pemerhatian, pengalaman atau pengukuran fenomena yang dikutip secara lansung daripada informan atau responden kajian. Fasa kajian empirikal bagi kajian ini bertujuan untuk mengenal pasti dan mengesah faktor kejayaan PKM, memperoleh pengukuran kematangan dan tahap kematangan bagi setiap faktor. Faktor kejayaan, pengukuran kematangan dan tahap kematangan yang dikenal pasti meliputi ciri utama keselamatan maklumat dan komponen utama PKM. Oleh kerana kajian empirikal ini melibatkan pelbagai aspek iaitu faktor kejayaan, pengukuran kematangan dan tahap kematangan, kajian empirikal ini dibahagi kepada tiga sub-kajian iaitu kajian empirikal A, kajian empirikal B dan kajian empirikal C. Reka bentuk berurutan penerokaan dan berurutan penerangan digabung dan diaplikasi dalam kajian ini. Rajah 3.6 menunjukkan gabungan reka bentuk berurutan penerokaan dan berurutan penerangan yang diguna dalam sub-kajian empirikal A, B dan C.



Rajah 3.6 Gabungan reka bentuk penerokaan dan penerangan

Reka bentuk berurutan penerokaan diguna pada kajian empirikal A dan B manakala reka bentuk berurutan penerangan diaplikasi pada kajian empirikal B dan C. Kajian dimulakan dengan kajian empirikal A melalui kaedah kualitatif diikuti dengan kajian empirikal B yang menggunakan kaedah kuantitatif. Hasil daripada kajian empirikal B kemudiannya diguna untuk melaksana kajian empirikal C yang melibatkan kaedah kualitatif.

3.4.1 Kajian Empirikal A

Kajian empirikal A dijalankan mengguna kaedah kualitatif. Kaedah kualitatif diguna bagi mendapatkan mendapatkan kefahaman yang mendalam serta maklumat terperinci terhadap sesuatu perkara yang dikaji (Fatin 2015). Kajian ini melibatkan temu bual individu dan temu bual kumpulan fokus bersama informan. Informan terdiri daripada kalangan pengamal industri yang berpengalaman dalam PKM. Tujuan temu bual diadakan adalah untuk mengesah faktor kejayaan PKM yang diperoleh daripada kajian teoritikal di samping memperoleh faktor kejayaan PKM yang baharu. Aktiviti di dalam kajian empirikal A ini merangkumi perancangan temu bual, pelaksanaan temu bual dan menganalisis data temu bual. Ia merangkumi pensampelan, instrumen, protokol dan analisis kajian.

a) Pensampelan

Terdapat dua jenis pensampelan dalam sesuatu penyelidikan iaitu pensampelan kebarangkalian (rawak) dan pensampelan bukan kebarangkalian (tidak rawak). Pensampelan kebarangkalian biasanya digunakan dalam kajian kuantitatif dan

pensampelan bukan kebarangkalian pula lazimnya diguna pakai dalam kajian kualitatif (Denzin & Lincoln 2005).

Oleh kerana kajian Empirikal A ini merupakan kajian kualitatif, maka pensampelan yang digunakan adalah pensampelan bukan kebarangkalian. Pensampelan bukan kebarangkalian terbahagi kepada beberapa teknik seperti pensampelan mudah, pensampelan berkuota, pensampelan bertujuan (purposive sampling) dan pensampelan bola salji (snowball). Kajian ini mengguna teknik pensampelan bertujuan. Pensampelan bertujuan diguna untuk memilih sekumpulan subjek yang mempunyai kriteria tertentu yang ditetapkan oleh keperluan kajian untuk dijadikan informan kajian (Chua 2011a). Pemilihan informan yang bersesuaian adalah penting kerana ia membolehkan objektif kajian dicapai (Fatin 2016).

Penetapan kriteria bagi pemilihan informan yang bersesuaian ditentukan berdasar kepada pengalaman dan pengetahuan informan dalam bidang kajian. Bagi kajian empirikal A ini, informan yang dipilih adalah daripada kalangan pengamal industri yang terlibat dalam PKM yang terdiri daripada beberapa kategori seperti berikut:

i. **Pengurusan atasan:** Individu yang memegang jawatan penting di dalam bahagian yang melaksana PKM. Mempunyai pengalaman dalam mengetuai PKM.

ii. **Ahli pasukan penyelaras:** Individu yang mempunyai pengalaman dalam mengurus dan menyelaras aktiviti PKM.

iii. **Ahli pasukan pelaksana:** Individu yang bertanggungjawab dalam melaksana operasi keselamatan maklumat.

iv. **Ahli pasukan audit:** Individu yang bertanggungjawab untuk memantau dan menilai perlaksanaan PKM.

Pemilihan informan dijalankan secara berterusan sehingga data yang diperolehi mencapai tahap ketepuan (Creswell 2014). Tahap ketepuan merupakan tahap di mana

data yang sama dan berulang diberi oleh informan kajian serta tiada lagi data baharu yang ditemui. Kajian ini mencapai tahap ketepuannya setelah sembilan informan ditemu bual sebagai sampel kajian. Maklumat informan bagi temu bual individu adalah seperti di Jadual 3.2 manakala maklumat informan bagi temu bual kumpulan fokus pula adalah seperti di Jadual 3.3.

Jadual 3.2 Latar belakang informan temu bual secara individu

Kod Informan	**Jawatan**	**Kategori**	**Pengalaman dalam PKM**	**Organisasi**
INF 1	Penolong Pengarah Kanan	Ahli pasukan penyelaras	6 tahun	Sektor Awam
INF 2	Pegawai Teknologi Maklumat	Ahli pasukan pelaksana	3 tahun	Sektor Awam
INF 3	Pegawai Teknologi Maklumat	Ahli pasukan pelaksana	5 tahun	Sektor Awam
INF 4	Pegawai Teknologi Maklumat Kanan	Ahli pasukan audit	4 tahun	Badan Berkanun
INF 5	Ketua Penolong Setiusaha Kanan	Pengurusan atasan	6 tahun	Sektor Awam

Jadual 3.3 Latar belakang informan temu bual secara kumpulan fokus

Kod Informan	**Jawatan**	**Kategori**	**Pengalaman dalam PKM**	**Organisasi**
FG 1	Setiausaha Bahagian	Pengurusan atasan	6 tahun	Sektor Awam
FG 2	Penolong Setiausaha Kanan	Ahli pasukan penyelaras	6 tahun	Sektor Awam
FG 3	Penolong Pengarah Kanan	Ahli pasukan pelaksana	5 tahun	Sektor Awam
FG 4	Penolong Pengarah Kanan	Ahli pasukan audit	6 tahun	Sektor Awam

b) Instumen kajian

Soalan berbentuk temu bual diguna sebagai instrumen dalam temu bual individu dan kumpulan fokus. Soalan temu bual direka berdasar kepada model konsep yang dibangun hasil daripada kajian teoritikal. Soalan adalah berkisar berkenaan faktor kejayaan PKM. Soalan temu bual telah disemak dan diuji bersama dua ahli bidang dan empat penyelidik lain dalam satu sesi ujian rintis. Ujian rintis ini dilaksana untuk menilai kesesuaian dan pemahaman soalan serta mengenal pasti kelemahan yang timbul sebelum sesi temu bual yang sebenar dijalankan. Antara maklum balas yang diterima daripada ujian rintis tersebut ialah penyediaan faktor atau rajah model konsep untuk tatapan informan

sebelum mengajukan soalan temu bual. Selain itu, definisi ringkas setiap faktor perlu disediakan bagi melancar urusan temu bual. Keseluruhan soalan temu bual adalah seperti di Lampiran A.

c) Protokol

Bagi temu bual individu, persetujuan daripada informan diperoleh sebelum melaksana temu bual. Temu janji dilakukan terlebih dahulu bagi menetapkan tarikh, masa dan tempat yang bersesuaian untuk melaksana temu bual. Informan diberi penerangan ringkas berkenaan tujuan temu bual tersebut. Setelah persetujuan diterima, jemputan rasmi melalui surat dan e-mel dihantar kepada informan.

Sesi temu bual individu telah dilaksana pada bulan Februari, Mac, Mei dan Jun 2016. Sebelum memulakan sesi temu bual, informan diberi sekali lagi penerangan ringkas berkenaan objektif temu bual dan peranan informan dalam sesi temu bual tersebut. Kesemua informan telah memberi komitmen yang tinggi dalam setiap sesi temu bual. Keseluruhan sesi temu bual telah dirakam mengguna rakaman audio dan catatan data. Setiap sesi temu bual mengambil masa purata dalam lingkungan 50 minit hingga 90 minit.

Bagi sesi temu bual kumpulan fokus, persetujuan daripada informan turut diperoleh terlebih dahulu sebelum melaksana sesi temu bual tersebut. Dua minggu sebelum sesi kumpulan fokus dijalankan, surat jemputan yang mempunyai maklumat tentang objektif, tarikh, masa dan tempat dihantar kepada informan. Dua hari sebelum sesi kumpulan fokus dilaksana, informan diberi peringatan mesra melalui panggilan telefon dan e-mel mengenai sesi yang akan diadakan. Sesi kumpulan fokus berlangsung pada 14 Mei 2016 jam 10.00 pagi. Sebelum sesi kumpulan fokus dimulakan, tatacara perlaksanaan sesi kumpulan fokus diterang kepada semua informan. Semasa temu bual kumpulan fokus berlangsung, informan bebas untuk memberi pendapat dan cadangan terhadap elemen dan faktor lain yang dirasa berkaitan. Rakaman audio dan video dibuat untuk merekod keseluruhan sesi kumpulan fokus. Sesi kumpulan fokus mengambil masa selama hampir tiga jam.