Asia-Pacific Journal of Information Technology and Multimedia 15(1) 2026: 123 – 139
https://doi.org/10.17576/apjitm-2026-1501-07

Development of a Governance-Based Strategic Information Security Policy Implementation Framework for the Malaysian Public Sector

Pembangunan Kerangka Pelaksanaan Polisi Keselamatan Maklumat Strategik Berasaskan Tadbir Urus bagi Sektor Awam Malaysia

Surayahani Hasnul Bhaharin[1], Umi Asma' Mokhtar[1], Maryati Mohd Yusof[1], Rossilawati Sulaiman[1], Megat Zuhairy Megat Tajuddin[2], Nuraishah Mokhtar[2]*

[1]Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi, Selangor, Malaysia

[2]National Cyber Security Agency (NACSA), Malaysia

**Corresponding author: Umi Asma' Mokhtar (umi.mokhtar@ukm.edu.my)*

Received 20 February 2026
Accepted 27 April 2026, Available online 30 June 2026

ABSTRACT

Strategic information security has become a critical priority for organizations as senior management bears the responsibility for protecting organizational information assets. Despite the proliferation of international information security frameworks and standards, organizations continue to struggle with effective implementation due to the lack of practical guidance. This study addresses key gaps in information security management research by developing a comprehensive strategic information security policy implementation framework. Through systematic analysis of six established information security governance frameworks and validation by five information security experts using a case study approach, this research employs process mapping methodology grounded in Activity Theory and information governance theory. The proposed framework identifies core governance processes, stakeholder groups, and critical success factors for implementation. The framework integrates four key design principles: organizational-wide governance aligned with business objectives, risk management as the foundation, clearly defined processes and stakeholder responsibilities, and iterative processes for continuous improvement. The study contributes both theoretically and practically by providing an empirically validated, process-oriented framework that bridges the gap between policy formulation and effective implementation, specifically addressing the unique contextual requirements of strategic information security management.

Keyword: strategic information security implementation framework, activity theory, case study, information security, implementation

ABSTRAK

Keselamatan maklumat strategik telah menjadi keutamaan kritikal bagi organisasi kerana pengurusan atasan menanggung tanggungjawab untuk melindungi aset maklumat organisasi. Walaupun terdapat banyak kerangka dan piawaian keselamatan maklumat antarabangsa, organisasi terus bergelut dengan pelaksanaan yang berkesan disebabkan kekurangan panduan praktikal. Kajian ini menangani jurang utama dalam kajian pengurusan keselamatan maklumat dengan membangun kerangka pelaksanaan polisi keselamatan maklumat strategik yang komprehensif. Melalui analisis sistematik terhadap enam rangka kerja tadbir urus keselamatan maklumat dan pengesahan oleh lima pakar keselamatan maklumat menggunakan pendekatan kajian kes, kajian ini menggunakan metodologi pemetaan proses yang berasaskan Teori Aktiviti dan teori tadbir urus maklumat. Kerangka yang dicadang mengenal pasti proses teras tadbir urus, kumpulan pihak berkepentingan, dan faktor kejayaan kritikal untuk pelaksanaan. Kerangka ini menyepadukan empat prinsip reka bentuk utama: tadbir urus menyeluruh organisasi yang selaras dengan objektif perniagaan, pengurusan risiko sebagai asas, proses dan tanggungjawab pihak berkepentingan yang ditakrifkan dengan jelas, dan proses berulang untuk penambahbaikan berterusan. Kajian ini menyumbang secara teoretikal dan praktikal dengan menyediakan kerangka berorientasikan proses yang disahkan secara empirikal yang merapatkan jurang antara perumusan polisi dan pelaksanaan yang berkesan, khususnya menangani keperluan kontekstual unik pengurusan keselamatan maklumat strategik.

Kata kunci: kerangka pelaksanaan keselamatan maklumat strategik, teori aktiviti, kajian kes, keselamatan maklumat, pelaksanaan

PENGENALAN

Keselamatan maklumat strategik menjadi keutamaan dalam organisasi. Keutamaan ini timbul kerana ia telah menjadi tanggungjawab pengurusan atasan untuk melindungi maklumat strategik organisasi. Pelbagai kerangka keselamatan maklumat yang telah diperkenalkan oleh piawaian antarabangsa dan badan profesional untuk membantu organisasi melaksana pengurusan keselamatan maklumat. Namun, kerangka ini hanya memberi tumpuan kepada menentukan keperluan pengurusan keselamatan maklumat, dan tidak memberi panduan secara praktikal tentang cara melaksanakannya. Walaupun organisasi menyedari kepentingan pengurusan keselamatan maklumat dan keperluan pelaksanaan yang semakin meningkat, organisasi menghadapi cabaran kerana kekurangan panduan yang relevan bagaimana untuk mempraktik pengurusan keselamatan maklumat strategik dengan berkesan.

Kajian lampau telah mengenal pasti jurang utama dalam bidang kajian pengurusan keselamatan maklumat:

1. Kekurangan kerangka atau model pengurusan keselamatan maklumat holistik menggabung bidang pengurusan keselamatan maklumat yang luas.
2. Kekurangan panduan bagaimana melaksana pengurusan keselamatan maklumat strategik.
3. Kerangka atau model pengurusan keselamatan maklumat strategik berasas kajian emperikal yang terhad.
4. Kekurangan kerangka atau model yang mengenal pasti proses yang perlu dilaksana oleh pelbagai kumpulan pihak berkepentingan yang terlibat dalam pengurusan keselamatan maklumat strategik.

Motivasi untuk menangani masalah pelaksanaan polisi keselamatan maklumat strategik dan jurang kajian telah dibincang di dalam kajian ini. Kajian ini telah membangun kerangka pelaksanaan polisi keselamatan maklumat berdasar kajian susastera dan berasas data empirikal yang bertujuan menjawab persoalan kajian, iaitu bagaimana kerangka pelaksanaan polisi keselamatan maklumat strategik dibangunkan.

ANALISIS KERANGKA DAN MODEL

Analisis kerangka dan model telah mengenal pasti ciri utama, persamaan, perbezaan dan jurang yang memudahkan penentuan komponen utama yang diperlukan dalam membangun model konseptual pelaksanaan polisi keselamatan maklumat strategik. Enam kerangka ini dipilih berdasarkan kriteria berikut: (i) kerangka tersebut diiktiraf secara antarabangsa atau telah melalui proses semakan rakan sejawat; (ii) kerangka ini merangkumi dimensi tadbir urus keselamatan maklumat yang relevan dengan konteks sektor awam; dan (iii) kerangka ini telah dirujuk secara meluas dalam kajian-kajian pengurusan keselamatan maklumat terdahulu. Pemilihan ini bertujuan memastikan analisis perbandingan yang menyeluruh dan bersandarkan asas ilmiah yang kukuh.

Jadual 1 menunjukkan rumusan analisis kerangka dan model yang terpilih berdasarkan kepada komponen tadbir urus. Terdapat enam komponen tadbir urus yang dikenal pasti untuk menilai enam kerangka/ model yang dipilih iaitu (i) objektif pelaksanaan keselamatan maklumat, (ii) tadbir urus maklumat, (iii) proses, (iv) proses, fungsi, aktiviti utama, (v) hubungan antara komponen, dan (vi) pihak berkepentingan utama.

JADUAL 1. Rumusan analisis kerangka dan model terpilih

Komponen tadbir urus	**Flowerday & Tuyikeze (2016)**	**ISACA (2010)**	**Gashgari et al. (2017)**	**Ohki et al. (2009)**	**Veiga & Eloff (2007)**	**ARMA (2022)**
1. Objektif pelaksanaan keselamatan maklumat	✓	✓		✓	✓	✓
2. Tadbir urus maklumat	✓	✓	✓	✓	✓	✓
3. Berpandukan proses apa	✓			✓	✓	✓
4. Mengenal pasti proses/fungsi/aktiviti utama pengurusan keselamatan maklumat						
• Jaminan keselamatan		✓		✓	✓	✓
• Kepimpinan pelaksanaan	✓			✓	✓	✓
• Pemantauan dan kawalan		✓	✓	✓	✓	✓
• Melibatkan pihak berkepentingan	✓		✓	✓	✓	✓
• Pengurusan risiko	✓		✓	✓	✓	✓
• Pematuhan	✓	✓	✓	✓	✓	✓
• Penetapan hala tuju	✓	✓	✓	✓	✓	✓
5. Menunjukkan hubungan di antara komponen	✓			✓	✓	
6. Mengenal pasti penglibatan pihak berkepentingan utama	✓			✓	✓	✓

Kerangka dan model yang telah dianalisis adalah kerangka atau model yang mengenal pasti komponen utama tadbir urus keselamatan maklumat dan apa yang perlu dan mesti dilakukan untuk melaksana tadbir urus keselamatan maklumat. Empat kerangka, iaitu kerangka tadbir urus keselamatan maklumat oleh Ohki et al. (2009), Kerangka kitar hayat pembangunan polisi keselamatan maklumat oleh Flowerday dan Tuyikeze (2016), model bisnes keselamatan maklumat oleh ISACA (2010) dan model pelaksanaan tadbir urus maklumat oleh ARMA International (2022), bertujuan memudahkan pelaksanaan polisi keselamatan maklumat iaitu dengan mengenal pasti komponen yang perlu dipertimbang dalam tadbir urus keselamatan maklumat tetapi tidak mengenal pasti "bagaimana" untuk melaksanakannya.

METODOLOGI

Pembangunan kerangka ini dimulai dengan cadangan pembangunan kerangka konseptual yang digarap dari kajian lampau, dan kemudian dinilai oleh lima orang pakar dari kajian kes. Kerangka konseptual pelaksanaan polisi keselamatan maklumat strategik ini telah dibangun dengan menggabung pengetahuan daripada bidang tadbir urus maklumat dan domain keselamatan maklumat yang berkaitan dan Teori Aktiviti. Pengetahuan dibina daripada tinjauan susastera terperinci, proses dan fungsi utama tadbir urus keselamatan maklumat yang dikenal pasti, dan analisis enam kerangka terpilih. Enam kerangka tersebut adalah dari Da Veiga & Eloff, (2007); ISACA, (2010); Ohki et al., (2009); Flowerday & Tuyikeze, (2016); Gashgari et al., (2017); ARMA International (2022) sebagai asas untuk membangunkan rangka kerja pelaksanaan polisi keselamatan maklumat strategik.

Tujuan kerangka pelaksanaan adalah untuk menyediakan kerangka yang diterima, iaitu pemahaman bersama tentang bagaimana sesuatu kerja dapat dilaksana (Davenport, 1993; Kalman, 2002).

Kajian ini telah menggunakan pendekatan pemetaan proses untuk menentu dan memetakan proses teras tadbir urus keselamatan maklumat yang membentuk kerangka pelaksanaan polisi keselamatan maklumat strategik yang diperlukan untuk memudahkan pematuhan polisi keselamatan maklumat strategik. Pemetaan proses membolehkan pihak berkepentingan dan proses teras yang dikenal pasti didokumenkan. Gambaran secara grafik menunjukkan aliran kerja dan interaksi proses dengan pihak berkepentingan yang dipermudah dalam bentuk diagram fungsi (Accorsi et al. 2015; Burgelman 1996; Knapp et al. 2009; Nicho 2018).

Kerangka konseptual ini diberi kepada lima orang pakar keselamatan maklumat bagi mendapatkan pandangan awal pakar mengenai keperluan dan kesesuaian kerangka. Pandangan pakar ini diambil kira di dalam pembangunan kerangka pelaksanaan polisi keselamatan maklumat strategik dan diguna sebagai input bagi pembangunan protokol temu bual untuk kajian kes pada peringkat seterusnya dalam menguji dan mengesahkan kerangka pelaksanaan polisi keselamatan maklumat strategik secara empirikal.

Lima orang pakar keselamatan maklumat telah dipilih berdasarkan kriteria berikut: (i) sekurang-kurangnya 10 tahun pengalaman dalam bidang keselamatan maklumat atau tadbir urus IT di sektor awam Malaysia; (ii) pernah terlibat secara langsung dalam pembangunan atau pelaksanaan polisi keselamatan maklumat strategik; dan (iii) memegang jawatan pengurusan

pertengahan hingga pengurusan tertinggi dalam organisasi masing-masing. Profil pakar terdiri daripada pegawai keselamatan maklumat kanan, pegawai tadbir urus IT, dan pengamal audit keselamatan. Maklum balas pakar dianalisis secara tematik dengan mengenal pasti tema-tema utama, persetujuan dan perbezaan pandangan, serta cadangan penambahbaikan yang dikemukakan terhadap kerangka konseptual yang dicadangkan. Jadual 2 menunjukkan profil pakar yang terlibat dalam pengesahan kerangka ini.

JADUAL 2. Profil Pakar Pengesahan Kerangka

Kod	Peranan	Pengalaman	Kepakaran
IA1	Ketua Pegawai Maklumat	20	Tadbir Urus IT dan Keselamatan Maklumat
IA2	Pengurus Keselamatan IT	15	Pengurusan Risiko dan Polisi IS
IA3	Pegawai Audit Keselamatan	12	Audit dan Jaminan IS
IA4	Pegawai Tadbir Urus IT	18	Pematuhan dan Tadbir Urus
IA5	Pengarah Keselamatan Maklumat	22	Pengurusan Strategik IS

Bagi memastikan kebolehpercayaan dapatan kajian kualitatif ini, strategi triangulasi data telah digunakan, iaitu dengan menggabungkan maklum balas daripada pelbagai pakar, analisis dokumen kerangka keselamatan maklumat terpilih, dan semakan semula interpretasi bersama informan terpilih. Pendekatan ini selaras dengan prinsip kebolehpercayaan dan kebolehsahihan dalam penyelidikan kualitatif sebagaimana yang dikemukakan oleh Lincoln dan Guba (1985).

Berikut merupakan langkah pemetaan proses bagi membangun kerangka konseptual yang dikenal pasti melalui kajian susastera dan analisis kerangka:

1. Langkah 1: Pengesahan prinsip reka bentuk utama yang memandu pembangunan kerangka pelaksanaan polisi keselamatan maklumat strategik.
2. Langkah 2: Pemetaan pihak berkepentingan utama yang terlibat dalam tadbir urus keselamatan maklumat.
3. Langkah 3: Pemetaan semua proses tadbir urus keselamatan teras dan pemilik proses (pihak berkepentingan) yang diperlukan untuk perlaksanaan tadbir urus keselamatan maklumat.
4. Langkah 4: Mengenal pasti hubungan dan interaksi antara proses tadbir urus keselamatan maklumat.

PROSES PEMBANGUNAN KERANGKA KONSEPTUAL PELAKSANAAN POLISI KESELAMATAN MAKLUMAT STRATEGIK

PENGESAHAN PRINSIP UTAMA REKA BENTUK KERANGKA

Kerangka konseptual pelaksanaan polisi keselamatan maklumat yang dicadang adalah kerangka berasaskan proses kerana ia mengenal pasti semua proses tadbir urus, menggambar hubungan proses yang jelas antara mekanisme pengurusan dan tadbir urus, dan menyokong aliran maklumat merentasi fungsi seluruh organisasi.

Berikut merupakan prinsip reka bentuk yang diguna untuk memandu pembangunan kerangka konseptual berdasar kepada empat prinsip utama yang dikenal pasti.

Prinsip 1: Tadbir urus keselamatan maklumat melibatkan keseluruhan organisasi dan dipandu oleh bisnes utama organisasi.
Keselamatan maklumat menjadi keutamaan dalam organisasi, maka tadbir urus keselamatan maklumat perlu menyeluruh dan mempertimbang strategi organisasi, objektif bisnes dan semua aspek yang berkaitan dengan organisasi.

Prinsip 2: Pengurusan risiko adalah asas kepada tadbir urus keselamatan maklumat.
Keselamatan maklumat adalah salah satu risiko utama kepada organisasi, maka tadbir urus keselamatan maklumat perlu menerima guna kerangka pengurusan risiko yang selaras dengan tadbir urus korporat.

Prinsip 3: Kerangka tadbir urus keselamatan maklumat perlu mengenal pasti dengan jelas proses tadbir urus, peranan dan tanggungjawab; dan pihak berkepentingan yang berkaitan.
Tadbir urus keselamatan maklumat perlu mempunyai proses tadbir urus yang dikenal pasti dengan jelas. Pihak berkepentingan juga perlu dikenal pasti dengan jelas dan bertanggungjawab di dalam proses tadbir urus.

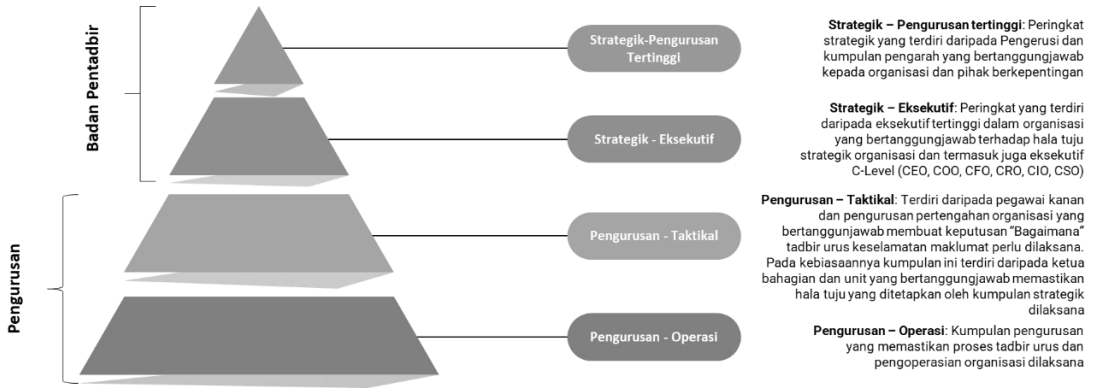
Prinsip 4: Tadbir urus keselamatan maklumat terdiri daripada proses yang berulang yang mendorong penambahbaikan secara berterusan dalam memenuhi objektif keselamatan maklumat organisasi.
Tadbir urus keselamatan maklumat menetapkan hala tuju keselamatan maklumat organisasi. Selain itu, tindakan yang telah dilaksana perlu disemak dari semasa ke semasa supaya tindakan tersebut selari dengan objektif keselamatan maklumat yang telah ditetapkan.

MENGENAL PASTI PIHAK BERKEPENTINGAN

Kerangka konseptual yang dibangun mengguna pakai tahap pengurusan daripada R. Von Solms dan Von Solms (2006) iaitu tiga tahap sebagai asas untuk mengenal pasti pihak berkepentingan. Manakala dalam tadbir urus korporat, tahap pengurusan strategik diperluaskan kepada dua kumpulan berasingan, iaitu "strategik – lembaga pengarah" dan "strategik - eksekutif"; dan mempunyai peranan yang berbeza (Y. Kim & Kim 2021; Kozlov & Noga 2019). Walaupun kedua-dua kumpulan ini bertanggungjawab terhadap hala tuju strategik keseluruhan organisasi, kumpulan "strategik-lembaga pengarah" pada umumnya merupakan ahli lembaga bukan eksekutif dan memberi khidmat nasihat kepada kumpulan "strategik-eksekutif".

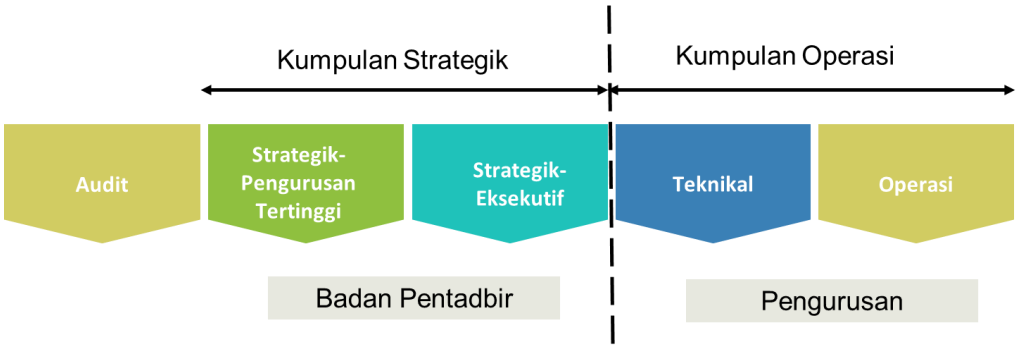
Dalam kerangka pelaksanaan polisi keselamatan maklumat strategik yang dicadangkan, kumpulan "strategik- lembaga pengarah" dan kumpulan "strategik-eksekutif" dikenali sebagai "badan pentadbir" iaitu kumpulan yang bertanggungjawab terhadap prestasi dan pematuhan polisi oleh organisasi. Bagaimanapun, bagi kajian ini, kumpulan “strategik-lembaga pengarah” akan dinyatakan sebagai “strategik-pengurusan tertinggi” bersesuaian dengan skop kajian. Dua peringkat pengurusan yang lain adalah "pengurusan - teknikal" dan "pengurusan - operasi" (R. Von Solms & Von Solms 2006) yang diberi tanggungjawab oleh "badan pentadbir" untuk pelaksanaan strategi dan polisi.

RAJAH 1 menunjukkan kumpulan pihak berkepentingan yang dikenal pasti dalam kerangka konseptual pelaksanaan polisi keselamatan maklumat strategik. Peranan dan tanggungjawab yang jelas antara badan pentadbir dan pengurusan, dan merentasi pelbagai kumpulan pihak berkepentingan, menggalakkan pengasingan tugas. Ia merupakan prinsip utama dalam struktur tadbir urus serta menyokong aliran maklumat merentasi fungsi di dalam organisasi secara keseluruhan.



RAJAH 1. Pihak berkepentingan dalam pelaksanaan polisi keselamatan maklumat strategik

Selain itu, peranan pihak berkepentingan dari luar organisasi juga penting dalam pengauditan dan jaminan keselamatan (K. Allen 2008; ISO/IEC 27014 n.d.; Ohki et al. 2009). Kumpulan ini juga menjadi entiti luar yang menjalankan audit atau persijilan terhadap kedudukan keselamatan maklumat sesebuah organisasi. Lima kumpulan pihak berkepentingan dipetakan bersama peranan yang dilaksana seperti dalam
RAJAH 2.



RAJAH 2. Pihak berkepentingan dan peranan yang dilaksana

PROSES TERAS DAN AKTIVITI PELAKSANAAN POLISI KESELAMATAN MAKLUMAT STRATEGIK

Proses teras dan aktiviti pelaksanaan yang menyokong pelaksanaan polisi keselamatan maklumat dikenal pasti melalui ulasan susastera dan kerangka keselamatan maklumat terpilih. Walaupun nama proses dan aktiviti teras ini berbeza dalam kerangka yang dipilih, tetapi definisi dan peranan proses ini konsisten dan bertujuan untuk mencapai objektif yang sama. Proses teras daripada kerangka dan model terpilih seperti di dalam Jadual 3.

JADUAL 3. Proses teras dari kajian lepas

Ohki et al. (2009)	Da Veiga & Eloff (2007)	Gashgari et al. (2017)	ARMA (2022)	Objektif	Kerangka Konseptual (Proses yang dicadang)
Hala tuju	Strategi	Pelarasan strategik	Pemandu	Memberi panduan dan arahan keseluruhan supaya pihak pengurusan dapat melaksanakan prinsip keselamatan maklumat	Penetapan hala tuju dan keberhasilan
-	Kepimpinan dan Tadbir urus	Penglibatan dan kepimpinan	Kepimpinan dan pengurusan	memandu keputusan berkaitan tadbir urus maklumat.	Kepimpinan pelaksanaan
Pelaporan	-	Komunikasi Efektif	Komunikasi	Menggambar akauntabiliti dan ketelusan melalui pelaporan dan komunikasi mengenai program keselamatan maklumat yang dijalankan dalam melindungi organisasi dan tindak balas terhadap insiden keselamatan.	Komunikasi
-	Penilaian risiko	Pengurusan risiko	Toleransi risiko	Proses mengenal pasti risiko, menilai kesan risiko dan mengambil tindakan untuk mengawal risiko ke tahap yang boleh diterima	Pengurusan risiko
Pemantauan	Pemantauan	Tinjauan	Kawalan	Menilai pencapaian / kemajuan objektif keselamatan maklumat seperti yang ditakrifkan dalam arahan.	Pemantauan, kawalan dan penilaian
Validasi	Audit	-	Penanda Aras	Menjalankan pemeriksaan dan pengesahan oleh pihak bebas (contohnya ulasan, audit dan persijilan) untuk memastikan pematuhan pada tahap keselamatan maklumat yang dikehendaki.	Jaminan keselamatan

Huraian mengenai enam proses yang dicadangkan dalam kerangka konseptual pelaksanaan polisi keselamatan maklumat strategik adalah seperti berikut:

1. Penetapan Hala Tuju dan Keberhasilan

Tadbir urus berkait rapat dengan pencapaian matlamat bisnes organisasi (Datta et al. 2019; Merkus et al. 2019), proses penetapan hala tuju merangkumi aktiviti memahami visi, misi dan strategi bisnes organisasi supaya inisiatif keselamatan maklumat dapat dikenal pasti dan diselaras. Persoalan utama dalam memandu aktiviti dalam proses ini ialah Apakah hala tuju keselamatan maklumat strategik organisasi? Mengapa keselamatan maklumat strategik perlu diberi perlindungan sewajarnya? Proses ini adalah untuk menetapkan skop pelaksanaan dan

memastikan pihak berkepentingan serta kumpulan yang terlibat sepadan dengan keperluan pelaksanaan polisi.

2. Kepimpinan Pelaksanaan

Proses kedua ialah mengenal pasti pihak berkepentingan iaitu menjawab persoalan Siapakah pihak berkepentingan dan kumpulan yang terlibat dengan polisi keselamatan maklumat strategik? Apakah impak dan risiko pelaksanaan polisi ini? Proses ini adalah untuk meninjau tahap komitmen pihak berkepentingan dan tahap kesediaan kumpulan yang terlibat dalam melaksana polisi ini. Analisis dibuat ke atas pihak berkepentingan dan kumpulan yang terlibat untuk diguna sebagai asas membentuk strategi dan pelan pelaksanaan.

3. Pengurusan Risiko

Proses yang ketiga ialah merangka strategi berdasarkan hasil dapatan analisis. Strategi yang dirangka perlu selari dengan visi dan misi organisasi disamping mengambil kira risiko keselamatan maklumat strategik. Proses ini juga merangkumi mengenal pasti tahap risiko yang boleh diterima oleh organisasi supaya strategi yang ditetapkan relevan dengan pengurusan risiko (Joshi & Singh 2017; Maynard et al. 2018; Silva & Soares 2018; Yaokumah et al. 2016). Hala tuju dan pengurusan risiko yang saling menyokong akan memacu semua piawaian keselamatan maklumat, polisi, prosedur dan inisiatif yang dilaksana untuk organisasi. Selain itu, proses ini juga melibatkan pembangunan pelan pelaksanaan yang mengandungi pelan tindakan bersesuaian seperti komunikasi, program kesedaran/pendidikan dan latihan.

4. Pemantauan, Kawalan dan Penilaian

Proses pemantauan ialah menilai hala tuju yang telah ditetapkan dilaksana dan dipatuhi. Ia juga merupakan proses pematuhan bagi memastikan organisasi mematuhi polisi, piawaian dan prosedur keselamatan maklumat dalam mencapai objektif keselamatan maklumat yang telah ditetapkan. Proses penilaian pula ialah menilai hasil pematuhan dan menentukan perubahan serta pelarasan yang diperlukan yang untuk memenuhi keperluan keselamatan maklumat semasa dan akan datang. Prestasi pelaksanaan diukur dan pelan diperkemas serta mengulang aktiviti pelaksanaan untuk meningkatkan pematuhan kepada polisi.

5. Komunikasi

Ketelusan dan pendedahan (*disclosure)* adalah salah satu lagi prinsip utama dalam kerangka tadbir urus di mana pendedahan yang tepat dan tepat pada masanya perlu dibuat bagi semua perkara penting (Merkus et al. 2019; Soma et al. 2016; Tallon et al. 2013). Komunikasi yang jelas adalah prinsip tadbir urus yang baik dan kerangka yang dicadangkan oleh Ohki et al. (2009) dan ISO 27014 (Tadbir Urus Keselamatan Maklumat) telah mengambil kira perkara ini yang dikenal pasti sebagai proses laporan dan komunikasi. Kajian lepas turut menegaskan bahawa proses komunikasi yang sistematik dapat meningkatkan kesedaran keselamatan maklumat dan mengurangkan ketidakpatuhan di kalangan pengguna (Singh et al., 2020). Di samping itu, proses komunikasi adalah secara dua hala yang mana komunikasi termasuk pelaksanaan peraturan yang berkuat kuasa dan jangkaan hasil oleh pihak berkepentingan terhadap keselamatan maklumat.

6. Jaminan Keselamatan

Proses terakhir ialah jaminan keselamatan yang merupakan proses tadbir urus berkaitan pemeriksaan dan pengesahan yang dilaksana oleh pihak bebas seperti audit, semakan dan persijilan. Ini dapat membantu memastikan organisasi mematuhi piawaian standard keselamatan maklumat.

HUBUNGAN ANTARA PERANAN PIHAK BERKEPENTINGAN DAN PROSES TERAS

Kerangka tadbir urus keselamatan maklumat yang berkesan perlu mempunyai definisi yang jelas mengenai proses tadbir urus dan hubungan antara satu sama lain bagi menyediakan kerangka yang boleh memandu organisasi dalam pelaksanaan polisi keselamatan maklumat. Proses penetapan hala tuju, kawalan, pemantauan dan penilaian saling berinteraksi antara satu sama lain. Inisiatif tadbir urus keselamatan maklumat boleh diselaras secara berkala bagi memenuhi keperluan keselamatan maklumat organisasi yang sering berubah mengikut situasi semasa (Gashgari et al. 2017; Ohki et al. 2009). Selain itu, interaksi antara proses teras tadbir urus dan pihak berkepentingan juga kritikal. Interaksi jelas menunjukkan pengasingan peranan dan tanggungjawab yang perlu dilaksana. Proses ini selaras dengan aliran proses dan interaksi seperti yang terdapat dalam model dari ARMA International (2022) dan Ohki et al. (2009).

Rajah 3 menunjukkan proses teras dan aktiviti utama yang perlu dilaksana dengan teratur. Langkah seterusnya dalam membangun kerangka konseptual pelaksanaan polisi keselamatan maklumat strategik ialah menterjemah hubungan antara pihak berkepentingan dan proses teras serta aktiviti yang terlibat.

Penetapan Hala Tuju	Kepimpinan pelaksanaan	Pengurusan Risiko	Pemantauan, Kawalan dan Penilaian	Komunikasi	Jaminan Keselamatan
1. Melaksana penilaian asas a. Objektif keselamatan maklumat b. Skop keselamatan Maklumat c. Kewangan/baj et 2. Menubuhkan pasukan tadbir urus keselamatan maklumat	3. Melaksana analisis pihak berkepentingan 4. Melaksana analisis kesan pelaksanaan 5. Melaksana analisis kesediaan pelaksanaan	6. Membangun pelan pengurusan risiko yang meliputi pelan tindakan dalam aspek: a. Komunikasi risiko b. Pendidikan dan latihan c. Mengurus risiko	7. Melaksana polisi keselamatan maklumat strategik 8. Memantau pematuhan polisi 9. Menilai hasil pematuhan 10. Menentukan perubahan atau pelarasan yang diperlukan	11. Pelaporan secara berkala kepada pihak berkepentingan berkaitan pelaksanaan dan pencapaian pematuhan	12. Pelaksanaan Audit luar dan dalam 13. Persijilan di bawah domain keselamatan maklumat

RAJAH 3. Proses teras dan aktiviti utama

PEMBANGUNAN KERANGKA PELAKSANAAN POLISI KESELAMATAN STRATEGIK

Bahagian ini membincangkan bagaimana kerangka pelaksanaan polisi keselamatan strategik dicadang sebagai kerangka konseptual berdasarkan analisis kajian lampau, kemudian melalui proses pengesahan pakar.

KERANGKA KONSEPTUAL PELAKSANAAN POLISI KESELAMATAN STRATEGIK

Kerangka konseptual pelaksanaan polisi keselamatan maklumat strategik telah dibangun dengan menggunakan pendekatan pemetaan proses di mana kumpulan pihak berkepentingan dan proses teras tadbir urus dan faktor kejayaan pelaksanaan polisi dipetakan pada Rajah 4. Kerangka konseptual ini menunjukkan proses teras tadbir urus, aktiviti yang terlibat dan lima (5) kumpulan pihak berkepentingan. Kumpulan pihak berkepentingan (audit, strategik – pengurusan tertinggi, strategik - eksekutif, teknikal dan operasi) digambarkan pada baris mendatar atas, dan pihak berkepentingan yang dikenal pasti pula (pengurusan tertinggi, ketua pegawai maklumat, ketua keselamatan maklumat, jawatankuasa keselamatan maklumat strategik, jawatankuasa tadbir urus teknologi makumat, penyedia perkhidmatan maklumat, pentadbir maklumat, pengelola maklumat dan; pengguna dan pemula maklumat) di bahagian tengah.

Proses teras pula (jaminan keselamatan, komunikasi, kepimpinan pelaksanaan, pengurusan risiko; dan pemantauan, kawalan dan penilaian) ditunjukkan di sebelah kiri kerangka konseptual. Manakala di sebelah kanan pula ialah faktor kejayaan kritikal (strategi, teknologi, organisasi, manusia, persekitaran dan proses).

RAJAH 4. Cadangan Kerangka Konseptual Pelaksanaan Polisi Keselamatan Maklumat Strategik

PENGESAHAH PAKAR

Cadangan kerangka awal pelaksanaan polisi keselamatan maklumat strategik ini telah diberikan kepada lima (5) orang pakar keselamatan maklumat bagi mendapatkan pandangan awal mengenai keperluan dan kebolehgunaan kerangka dalam membantu pembangunan protokol temu bual bagi kajian kes peringkat berikutnya. 4 menunjukkan komen dan maklum balas yang diterima daripada kajian awal terhadap cadangan kerangka konseptual ini.

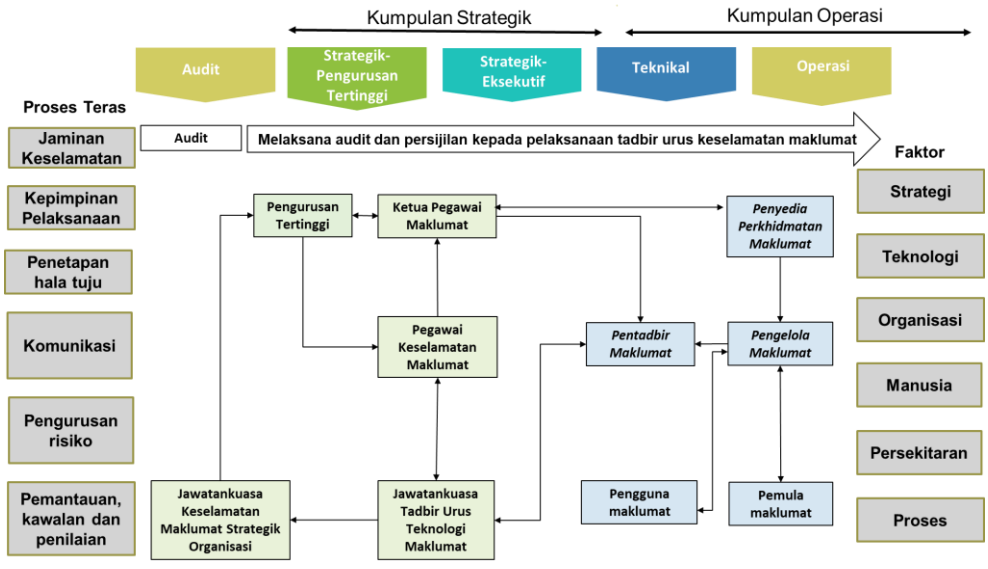
JADUAL 4. Pandangan awal Kerangka Konseptual Pelaksanaan Polisi Keselamatan Maklumat Strategik

Bil	Perkara	Komen
1	Pihak berkepentingan dikenal pasti dengan jelas	*..mempunyai struktur dikenal pasti dan jelas. Saya percaya peranan dan tanggungjawab sering menjadi isu seterusnya ... perlu ada akauntabiliti dan pengawasan oleh pihak atasan. (IA2)* *Sama seperti tadbir urus korporat ia bermula dari atas, iaitu pengurusan tertinggi. Pada pandangan saya, tadbir urus keselamatan maklumat memerlukan struktur yang betul di mana pengurusan tertinggi mengawal selia keseluruhan tadbir urus maklumat organisasi. (IA1)*
2	Proses dan aktiviti teras	*Inisiatif keselamatan maklumat kami dipacu dari strategi urusniaga utama jabatan ... keperluan urusniaga utama akan memacu peruntukan kewangan keselamatan maklumat dan keutamaan projek keselamatan maklumat" (IA2)* *Proses dan aktiviti kebanyakkannya didorong oleh keperluan utama jabatan, peraturan yang berkuat kuasa dan pengurusan risiko yang berkaitan. (IA4)*
3	Penetapan hala tuju dan keberhasilan	*Pengurusan atasan harus bertanggungjawab untuk memantau dan membuat keputusan secara keseluruhan iaitu termasuk meluluskan peruntukan kewangan bagi keselamatan maklumat, meluluskan pengurusan risiko dan memastikan jabatan memberi fokus serta keutamaan kepada keselamatan maklumat. (IA2)* *Hala tuju yang jelas amat penting bagi memastikan inisiatif keselamatan yang direncana selari dengan objektif utama jabatan. (IA1)* *Pengurusan tertinggi memainkan peranan penting sama ada berjaya atau tidak inisiatif pengurusan keselamatan maklumat. (IA5)*
4	Komunikasi	*Pengurusan tertinggi perlu sentiasa dikemas kini, memastikan mereka menyedari kemajuan terkini di jabatan dan dalam industri ... Ini juga bertindak sebagai sesi)* *awareness kepada pengurusan tertinggi untuk memastikan mereka mengetahui aktiviti yang berlaku di jabatan. (IA3* *Komunikasi adalah untuk memastikan kemas kini berterusan kepada pengurusan atasan. (IA5)* *Proses di mana pengurusan tertinggi sentiasa dikemas kini dan aware. bagi membantu pengurusan tertinggi terlibat dalam proses membuat keputusan. (IA1)* *Kumpulan pengurusan kanan mengemas kini pengurusan tertinggi supaya apa yang berlaku di jabatan diketahui. (IA2)*
5	Pengurusan risiko	*Ketua Pegawai Maklumat ... Salah satu peranan utama adalah untuk memastikan semua risiko mesti mempunyai polisi dan kerangka yang betul, dikaji semula, diperbaharui dari semasa ke semasa. (IA1)* *Pasukan khas bagi pengurusan risiko amat penting bagi memastikan risiko jabatan di tangani dengan baik dan tersusun. Ia bukanlah tanggungjawab satu pihak tetapi memerlukan kerjasama dari seluruh. (IA3)*

6	Pemantauan, kawalan dan penilaian	*Pentadbir maklumat akan memastikan pematuhan dan bertindak apabila terdapat ketidakpatuhan dengan mengambil tindakan pembetulan yang sewajarnya" (IA5)* *Sebarang ketidakpatuhan akan dibangkitkan dalam mesyuarat pengurusan atau pengurusan tertinggi.* *Jawatankuasa akan menyiasat ketidakpatuhan dan mengambil tindakan yang perlu" (IA3).* *Proses pematuhan perlu dilaksana secara proaktif, maka penubuhan jawatankuasa dapat membantu memantau pelaksanaan polisi dan pematuhan" (IA2)*
7	Jaminan keselamatan	*Audit luar akan menilai pelaksanaan pengurusan keselamatan maklumat mengikut piawaian yang telah ditetapkan. Jabatan juga mempunyai juruaudit dalaman yang melaksanakan audit meliputi keselamatan maklumat sebagai sebahagian daripada skop jaminan keselamatan untuk keseluruhan jabatan. (IA4)* *Terdapat lapisan yang berbeza, iaitu pengguna di barisan hadapan, pengurusan risiko dan fungsi pematuhan; dan audit atau jaminan keselamatan... Tadbir urus keselamatan maklumat menggunakan pendekatan yang sama. (IA1)*

KERANGKA PELAKSANAAN POLISI KESELAMATAN STRATEGIK

Rajah 5 merupakan Kerangka pelaksanaan polisi keselamatan maklumat strategik ini telah dibangun dengan input daripada Teori Aktiviti dan teori tadbir urus maklumat. Teori-teori ini telah diambil kira di dalam kerangka pelaksanaan polisi bagi memperluas kebolehgunaannya dari perspektif tadbir urus. Kerangka ini sejajar dengan prinsip utama teori tadbir urus maklumat, iaitu memberi tumpuan kepada pengurusan risiko, kawalan dan pemantauan, mengimbangi keperluan pihak berkepentingan, dan peningkatan prestasi melalui penyelarasan perancangan strategik organisasi. Pemahaman teori tadbir urus maklumat telah menghasilkan kerangka pelaksanaan polisi, yang mengenal pasti kumpulan pihak berkepentingan dan menerangkan bagaimana proses teras dan faktor pelaksanaan, bersama-sama dengan aliran maklumat dan komunikasi.



RAJAH 5. Pembangunan Kerangka Pelaksanaan Polisi Keselamatan Maklumat

Reka bentuk kerangka pelaksanaan polisi keselamatan maklumat yang dicadang menggabungkan komponen utama pengurusan dan tadbir urus keselamatan maklumat yang diekstrak daripada kajian susastera serta disokong oleh amalan sebenar yang ditemui di dalam kajian kes yang dilaksana. Komponen utama pengurusan dan tadbir urus keselamatan maklumat terdiri daripada kumpulan pihak berkepentingan, proses teras serta faktor pelaksanaan polisi. Jadual 5 menunjukkan ringkasan integrasi antara teoretikal (kajian susastera) dan praktikal (amalan sebenar).

JADUAL 5. Integrasi teoretikal dan praktikal kerangka pelaksanaan polisi keselamatan maklumat strategik

Komponen utama pengurusan keselamatan dan tadbir urus maklumat strategik	**Teoretikal**	**Praktikal**
Prinsip kerangka pelaksanaan polisi keselamatan maklumat strategi	Reka bentuk kerangka yang diekstrak daripada kajian susastera.	Reka bentuk kerangka yang diguna pakai melalui kajian kes dan dinilai oleh kumpulan pakar serta pelaksana.
Berpacu kepada bisnes utama dan pelaksanaan merentasi keseluruhan organisasi	ARMA International (2022); Atoum	Diamalkan di semua peringkat organisasi dan dipacu oleh keperluan bisnes utama. Pengurusan keselamatan maklumat menjadi agenda utama di dalam mesyuarat pengurusan tertinggi organisasi.
Pengurusan risiko dan tadbir urus adalah asas kepada pengurusan keselamatan maklumat	Joshi & Singh (2017); N. Mayer & De Smet (2017); Shepherd, Sexton,	Mengguna pakai prinsip utama tadbir urus maklumat.
Mengenal pasti proses tadbir urus berserta peranan dan tanggungjawab	Ohki et al. (2009); Sohrabi Safa et al. (2016); B. Von Solms & Von Solms (2018); R. Von Solms et al. (2011) Ohki et al. (2009); Samonas et al. (2020); Sohrabi Safa et al. (2016)	Proses pengurusan dan tadbir urus keselamatan maklumat dikenal pasti dan dilaksana oleh pelbagai pihak berkepentingan.
Pihak berkepentingan dan struktur tadbir urus		Mengenal pasti kumpulan strategik yang terdiri daripada badan pentadbir. Kumpulan operasi yang terdiri daripada pengurusan Pihak audit yang terdiri daripada audit dalam dan luar
Proses teras	Proses teras yang dikenal pasti adalah konsisten dengan kajian sarjana terdahulu	Enam proses teras telah dikenal pasti dan disahkan melalui kajian kes dan pemerhatian di lapangan.

KESIMPULAN

Kajian ini telah berjaya membangunkan kerangka pelaksanaan polisi keselamatan maklumat strategik yang komprehensif dan berasaskan bukti empirikal. Kerangka ini menggabungkan perspektif tadbir urus maklumat dengan amalan sebenar sektor awam Malaysia, sesuatu yang

kurang diperhalusi dalam kajian-kajian terdahulu (Von Solms & Von Solms, 2018; Ohki et al., 2009). Berbanding kerangka sedia ada seperti ISACA (2010) dan ARMA International (2022) yang lebih bersifat preskriptif, kerangka yang dicadang dalam kajian ini bersifat konteksual dan berorientasikan proses, sekali gus membolehkan organisasi mengadaptasikannya mengikut keperluan dan kapasiti masing-masing. Selain itu, pengesahan oleh lima pakar memastikan kerangka ini relevan untuk diamalkan. Dari perspektif teoritikal, penggunaan Teori Aktiviti sebagai asas analisis proses memberikan dimensi baru dalam memahami hubungan antara pihak berkepentingan dan proses teras keselamatan maklumat strategik (De Haes et al., 2020; Singh et al., 2020).

Pelaksanaan inisiatif Kerajaan Digital dan penggunaan teknologi secara meluas mengakibat peningkatan penghasilan dan penggunaan maklumat strategik secara digital dalam penyampaian perkhidmatan kerajaan. Keutamaan yang diberi oleh kerajaan kepada tadbir urus yang telus, cekap dan berintegriti telah meningkat kebergantungan kepada persekitaran digital yang selamat dan mewajar inisiatif pengurusan serta tadbir urus keselamatan maklumat strategik. Namun strategi yang hanya tertumpu kepada pendekatan konvensional, pematuhan mandat dan bersendirian tidak merangsang pelaksanaan inisiatif pengurusan dan tadbir urus keselamatan maklumat strategik. Dalam hal ini, kerangka yang dicadang dapat dilihat sebagai satu kerangka yang berupaya memberi idea asas memahami kewajaran perlaksanaan pengurusan dan tadbir urus keselamatan maklumat. Tambahan sebagai panduan kepada penggubalan mandat, pihak berkepentingan, dan pembangunan modul kompetensi dalam merangka pelan strategi yang lebih praktikal serta mudah dilaksanakan dalam pelbagai situasi.

Dari perspektif amalan, kerangka ini boleh diaplikasikan dalam organisasi sebenar melalui beberapa pendekatan. Pertama, organisasi boleh menggunakan kerangka ini sebagai rujukan asas dalam merangka atau menyemak semula polisi keselamatan maklumat sedia ada. Kedua, proses teras yang dikenal pasti dalam kerangka ini boleh dijadikan panduan dalam pembahagian peranan dan tanggungjawab kepada pihak berkepentingan yang relevan. Ketiga, faktor kejayaan kritikal yang dikenal pasti dapat membantu organisasi menyediakan persekitaran yang kondusif untuk pelaksanaan polisi yang berkesan.

RUJUKAN

Accorsi, R., Lehmann, A. & Lohmann, N. 2015. Information leak detection in business process models: Theory, application, and tool support. *Information Systems* 47: 244–257.

Allen, J.H. & Westby, J.R. 2007. *Characteristics of Effective Security Governance*. Technical Note CMU/SEI-2007-TN-024. Pittsburgh: Software Engineering Institute, Carnegie Mellon University.

Allen, K. 2008. Information governance and information security--hand in hand. *Journal (Institute of Health Record & Information Management)* 49(2): 28–29.

ARMA International. 2022. *Information Governance Maturity Model*. ARMA International.

Burgelman, R.A. 1996. A process model of strategic business exit: Implications for an evolutionary perspective on strategy. *Strategic Management Journal* 17(Suppl. Summer): 193–214.

Datta, R., Valavala, M. & Haris Uddin Sharif, M. 2019. Information governance: A necessity in today's business environment. *International Journal of Computer Science and Mobile Computing* 8(8): 67–76.

Davenport, T.H. 1993. *Process Innovation: Reengineering Work through Information Technology*. Boston: Harvard Business School Press.

Da Veiga, A. & Eloff, J.H.P. 2007. An information security governance framework. *Information Systems Management* 24(4): 361–372.

De Haes, S., Van Grembergen, W. & Debreceny, R.S. 2020. COBIT 2019 as the foundation for enterprise governance of IT. *EDPACS* 61(3): 1–14.

Engeström, Y. 2001. Expansive learning at work: Toward an activity theoretical reconceptualization. *Journal of Education and Work* 14(1): 133–156.

Flowerday, S. & Tuyikeze, T. 2016. Information security policy development and implementation: The what, how and who. *Computers & Security* 61: 169–183.

Gashgari, G., Walters, R. & Wills, G. 2017. A proposed framework for information security governance: Managing conflicts. *Journal of Systems and Information Technology* 19(3/4): 227–245.

ISACA. 2010. *The Business Model for Information Security*. ISACA. https://www.isaca.org/resources/isaca-journal/past-issues/2010/the-business-model-for-information-security

ISO/IEC. 2013. *ISO/IEC 27014:2013 Information Technology – Security Techniques – Governance of Information Security*. Geneva: International Organization for Standardization.

Joshi, C. & Singh, U.K. 2017. Information security risks management framework – A step towards mitigating security risks in university network. *Journal of Information Security and Applications* 35: 128–137.

Kalman, M.E. 2002. Organizational change through design. *Journal of Organization Design* 1(1): 23–38.

Kim, Y. & Kim, B. 2021. The effective factors on continuity of corporate information security management: Based on TOE framework. *Information* 12(11): 446.

Knapp, K.J., Franklin Morris, R., Marshall, T.E. & Byrd, T.A. 2009. Information security policy: An organizational-level process model. *Computers & Security* 28(7): 493–508.

Kozlov, A. & Noga, N. 2019. The method of assessing the level of compliance of divisions of the complex network for the corporate information security policy indicators. *2019 Twelfth International Conference "Management of Large-Scale System Development" (MLSD)*, hlm. 1–5. IEEE.

Kuutti, K. 1996. Activity theory as a potential framework for human-computer interaction research. Dlm. Nardi, B.A. (pnyt.). *Context and Consciousness: Activity Theory and Human-Computer Interaction*, hlm. 17–44. Cambridge: MIT Press.

Lincoln, Y.S. & Guba, E.G. 1985. *Naturalistic Inquiry*. Newbury Park: Sage Publications.

Mayer, N. & De Smet, D. 2017. Systematic literature review and ISO standards analysis to integrate IT governance and security risk management. *International Journal for Infonomics* 10(1): 1255–1263.

Maynard, S.B., Tan, T., Ahmad, A. & Ruighaver, T. 2018. Towards a framework for strategic security context in information security governance. *Pacific Asia Journal of the Association for Information Systems* 10(4): 65–88.

Merkus, J., Helms, R. & Kusters, R.J. 2019. Data governance and information governance: Set of definitions in relation to data and information as part of DIKW. *ICEIS 2019 – Proceedings of the 21st International Conference on Enterprise Information Systems*, hlm. 143–154. SCITEPRESS – Science and Technology Publications.

Nicho, M. 2018. A process model for implementing information systems security governance. *Information and Computer Security* 26(1): 10–38.

OECD. 2015. *G20/OECD Principles of Corporate Governance*. Paris: OECD Publishing.

Ohki, E., Harada, Y., Kawaguchi, S., Shiozaki, T. & Kagaya, T. 2009. Information security governance framework. Dlm. *Proceedings of the First ACM Workshop on Information Security Governance*, hlm. 1–6. ACM.

Samonas, S., Dhillon, G. & Almusharraf, A. 2020. Stakeholder perceptions of information security policy: Analyzing personal constructs. *International Journal of Information Management* 50: 144–154.

Singh, A.N., Gupta, M.P. & Ojha, A. 2020. Identifying factors of organizational information security management. *Journal of Enterprise Information Management* 33(1): 180–222.

Silva, E. & Soares, B.H. 2018. Governance and management of organizations with cloud supported services recommendations for risks of information security. *2018 13th Iberian Conference on Information Systems and Technologies (CISTI)*, hlm. 1–8. IEEE.

Shepherd, E., Sexton, A., Duke-Williams, O. & Eveleigh, A. 2019. Risk identification and management for the research use of government administrative data. *Records Management Journal*.

Sohrabi Safa, N., Von Solms, R. & Furnell, S. 2016. Information security policy compliance model in organizations. *Computers & Security* 56: 1–13.

Soma, K., Termeer, C.J.A.M. & Opdam, P. 2016. Informational governance – A systematic literature review of governance for sustainability in the information age. *Environmental Science and Policy* 56: 89–99.

Tallon, P.P., Ramirez, R.V. & Short, J.E. 2013. The information artifact in IT governance: Toward a theory of information governance. *Journal of Management Information Systems* 30(3): 141–178.

Von Solms, B. & Von Solms, R. 2018. Cybersecurity and information security – What goes where? *Information & Computer Security* 26(1): 2–9.

Von Solms, R. & Von Solms, S.H. 2006. Information security governance: A model based on the direct-control cycle. *Computers & Security* 25(6): 408–412.

Ward, J. & Peppard, J. 2002. *Strategic Planning for Information Systems*. Edisi ke-3. Chichester: John Wiley & Sons.

Yaokumah, W., Brown, S. & Dawson, A.A. 2016. Towards modelling the impact of security policy on compliance. *Journal of Information Technology Research* 9(2): 1–16.