BAB I
PENDAHULUAN

1.1. Latar Belakang

Peningkatan mutu pelayanan kesehatan di Indonesia sangat penting, terutama dengan kondisi geografis yang beragam. Pemanfaatan teknologi digital diharapkan dapat meningkatkan efisiensi dan efektivitas layanan kesehatan (Praptana et al., 2021). Kemenkes RI berupaya melakukan tranformasi kesehatan, termasuk tranformasi teknologi informasi kesehatan (Ditjen P2P, 2023). Transformasi digital ini mencakup penerapan teknologi untuk meningkatkan layanan, perawatan pasien, dan operasi administratif, sehingga layanan kesehatan menjadi lebih efisien, mudah diakses, dan berfokus pada pasien (Herlambang et al., 2020; Piduru, 2024).

Rumah sakit termasuk pelayanan kesehatan yang bertransformasi dalam teknologi informasi Kesehatan dengan adanya Sistem Informasi Manajemen Rumah Sakit (SIMRS). Rumah sakit selalu mendapatkan tekanan dari berbagai sisi mulai dari pasien, tenaga kesehatan maupun *stakeholder* dalam memperbaiki pelayanan medis, meminimalisir kesalahan medis, ketepatan waktu dalam akses informasi, dapat memonitor aktifitas pelayanan secara bersamaan dan mampu mengendalikan biaya operasional (Kristanti et al., 2021).

Penggunaan SIMRS sebagai teknologi informasi memiliki berbagai kelebihan, tetapi juga memiliki kekurangan terutama terkait dengan risiko keamanan informasi (Algiffary et al., 2023). Risiko tersebut mencakup ancaman peretasan, pencurian data, dan penyebaran *malware*, yang semuanya merupakan bentuk *cybercrime* (Algiffary et al., 2023).

Pada tahun 2016, terjadi serangan ransomware rekam medis elektronik di *Hollywood Presbyterian Medical Centre* di California. Peretas meminta tebusan sebesar US$3,4 juta dengan bentuk bitcoin (Minnaar & Herbig, 2021). Hal yang sama terjadi juga pada *Brno University Hospital* di Republik Ceko pada tahun 2020. Rumah sakit ini terpaksa seluruh jaringan TI-nya yang terkena serangan siber dan berdampak pada cabang rumah sakit mereka (Gioulekas et al., 2022).

Indonesia menjadi negara kedua dengan kasus serangan siber terbanyak di dunia setelah China pada tahun 2018 (Pratama, 2020). Pada tahun 2023 di Indonesia, terdapat 347 dugaan insiden siber yang dilaporkan oleh Badan Siber

dan Sandi Negara (BSSN) termasuk, *web defacement*, *ransomware,* serangan DdoS dan kebocoran data (BSSN, 2023)

Gambar 1.1 Grafik Aduan Siber di Indonesia tahun 2023
Sumber : (BSSN, 2023)

Sektor kesehatan masuk ke dalam 10 besar sektor yang terkena insiden siber dengan peringkat ke-6 (BSSN, 2023; Herlambang et al., 2020). Salah satu insiden siber yang pernah terjadi di sektor kesehatan adalah Rumah Sakit Harapan Kita dan Rumah Sakit Dharmais di Jakarta. Rumah Sakit ini mengalami serangan *ransomware* yang mengunci seluruh data rekam medis elektronik pasien dan mengganggu sistem informasi kesehatan serta catatan pembayaran rumah sakit (Ramadhan, 2023). Kasus ini mencerminkan risiko tinggi serangan siber yang dihadapi oleh institusi layanan kesehatan, termasuk di Indonesia (Minnaar & Herbig, 2021).

Cybercrime atau serangan siber mengacu pada aktivitas kriminal yang dilakukan oleh individu atau kelompok dengan memanfaatkan komputer, baik sebagai alat kejahatan maupun objek kejahatan (Chirzah & Ramadhan, 2023). Rumah sakit menjadi target dari serangan siber dikarenakan adanya data *privacy* seseorang dengan keamanan yang lemah. Jika serangan tersebut terjadi, maka kepercayaan pasien maupun keluarga pasien menurun sehingga akan mengancam data *privacy* pasien terbongkar dan tersebar luas. Rumah Sakit juga menghadapi kerugian finansial untuk menebus data yang terkunci dan risiko penundaan dalam penyediaan layanan kesehatan (Minnaar & Herbig, 2021). Kejahatan dari serangan siber merupakan hasil dari ketidakpatuhan terhadap hukum dan peraturan perundang-undangan, baik secara material maupun formal yang disebabkan oleh pelanggaran keamanan informasi (Barnes & Daim, 2024; Chirzah & Ramadhan, 2023).

Keamanan informasi adalah langkah untuk melindungi data dari ancaman yang dapat mengganggu operasional dan mengurangi risiko serangan (Renaldy et al., 2023). Menurut SNI ISO/IEC 27000:2014 keamanan informasi mencakup menjaga ketersediaan informasi, integritas, dan kerahasiaan agar organisasi dapat beroperasi dengan efisien dan aman (Nugroho et al., 2024).

Berdasarkan penelitian sebelumnya, pengguna sistem yang sadar akan risiko keamanan dan memahami kebijakan prosedur keamanan informasi merupakan suatu kontrol untuk memastikan keberlangsungan organisasi (Sari et al., 2021). Upaya untuk meningkatkan keamanan sistem informasi dalam sektor kesehatan berfokus pada peningkatan pertahanan teknologi organisasi, sering kali mengabaikan aspek manusia sebagai individu dari keamanan informasi. Pada organisasi, tidak hanya teknologi saja yang dapat memastikan lingkungan aset yang aman tetapi kurangnya pengetahuan, tanggung jawab dan kesadaran dalam individu menjadi faktor lemahnya keamanan informasi. Hal ini mengarah kepada kesadaran keamanan informasi/*information security awareness* (ISA) pengguna untuk meminimalkan risiko terkait pelanggaran keamanan dalam suatu sistem (Hore et al., 2024).

Kesadaran keamanan informasi atau *Information Security Awareness* (ISA) adalah tingkat pemahaman pengguna mengenai pentingnya keamanan informasi. Hal ini mencakup kesadaran akan tanggung jawab mereka dalam melindungi data dan jaringan organisasi (Naga et al., 2024). Titik lemah dalam keamanan informasi adalah perilaku dan kesalahan manusia seperti pemilihan kata sandi yang lemah sehingga mudah diretas, *email phishing* dan *spear phising*. Hal tersebut menandakan kurangnya pengetahuan dan kesadaran keamanan informasi pegawai yang dapat menyebabkan kerentenan risiko keamanan dalam organisasi (Sharifi, 2023).

Keamanan data termasuk isu penting dalam pelayanan publik seperti di rumah sakit. Melindungi informasi pasien merupakan prioritas utama yang harus dijaga dalam sektor kesehatan (Wilar et al., 2023). Pada UU No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi dalam pasal 35-38 menyebutkan bahwa Pengendali Data Pribadi wajib melindungi, mencegah, memastikan Data Pribadi dari pemrosesan yang tidak sah (Presiden RI, 2022). Menurut Permenkes Nomor 82 Tahun 2013 Tentang Sistem Informasi Manajemen Rumah Sakit, Rumah Sakit wajib menyelenggarakan SIM RS (Menteri Kesehatan RI, 2013).

Sistem Informasi Manajemen Rumah Sakit (SIMRS) dengan keamanan yang kuat mampu melindungi data pribadi pasien, memastikan bahwa informasi medis tetap rahasia dan tidak jatuh ke tangan yang salah. Dengan menjaga keamanan data, rumah sakit dapat memberikan pelayanan yang lebih terpercaya, sehingga meningkatkan kepercayaan publik terhadap sistem kesehatan nasional (Wilar et al., 2023). Salah satu rumah sakit yang telah mengimplementasikan SIM RS adalah RSUD Haji Makassar (Meliherdianti et al., 2021).

RSUD Haji Makassar merupakan Rumah Sakit milik pemerintah Provinsi Sulawesi Selatan. RSUD Haji Makassar telah mengimplementasikan SIMRS secara aktif. Peneliti melakukan pengumpulan data awal dengan menggunakan metode penyebaran kuesioner kepada 30 responden yaitu staf/pegawai yang menggunakan SIMRS dalam menjalankan pekerjaan mereka. Kuesioner awal menggunakan item pertanyaan dari penelitian (Yeng et al., 2022) dengan pilihan jawaban Ya/Tidak kemudian dari persentase hasil jawaban pengetahuan, sikap dan perilaku dijadikan rata-rata keseluruhan. Kuesioner awal menunjukkan *Information Security Awareness* (ISA) dibawah standar yaitu 56% (Standar: ≥ 80% oleh (Kruger & Kearney, 2006)). Menurut (McCormac et al., 2017), rendahnya kesadaran keamanan informasi disebabkan oleh budaya keamanan yang rendah dan akan menimbulkan risiko-risiko yang mungkin dihadapi RSUD Haji Makassar terhadap pelanggaran keamanan informasi khususnya pengguna SIMRS yang tidak memprioritaskan keamanan informasi untuk melindungi aset organisasi itu sendiri.

Ada beberapa teori yang membahas tentang kesadaran keamanan informasi yaitu *Theory of Planned Behavior* (TPB) (Ajzen, 1991), Teori *Knowledge-Attitude-Behavior* (KAB) (Kruger & Kearney, 2006) adaptasi dari teori psikologi sosial dan Teori Parsons (K. Parsons et al., 2014). Teori-teori tersebut banyak digunakan untuk mengukur kesadaran keamanan informasi di organisasi-organisasi dunia. Teori TPB menegaskan bahwa niat berperilaku aman terbentuk dari sikap terhadap perilaku, norma sosial, dan kontrol perilaku yang dirasakan. Jika individu merasa tidak mendapat dukungan atau merasa tidak mampu mengendalikan risiko, maka perilaku aman sulit terbentuk (Ajzen, 1991; Yeng et al., 2022).

Menurut teori KAB, ketika pengetahuan staf tentang perilaku keamanan informasi yang aman di tempat kerja meningkat, sikap mereka akan membaik dan

menghasilkan perilaku keamanan informasi yang lebih baik dari sebelumnya (Kruger & Kearney, 2006; McCormac et al., 2017). Parsons et.al mengembangkan pendekatan yang lebih komprehensif terhadap kesadaran keamanan informasi dengan membagi faktor-faktor yang memengaruhinya menjadi tiga domain utama yaitu individu, intervensi dan organisasi (K. Parsons et al., 2014).

Karakteristik personal seperti tingkat pendidikan, kepribadian, pengalaman, dan pengetahuan individu terkait keamanan informasi. Individu dengan tingkat literasi digital rendah cenderung memiliki kesadaran yang lemah. Dalam membentuk sikap dan perilaku berkaitan engan program pelatihan, edukasi, kampanye kesadaran, dan kebijakan organisasi yang diterapkan. Pada sisi organisasi, dalam meningkatkan kesadaran keamanan informasi dipengaruhi oleh budaya keamanan, norma subjektif, penghargaan dan hukuman (McCormac et al., 2017; K. Parsons et al., 2014).

Berdasarkan uraian tersebut, peneliti tertarik untuk mengkaji apa saja yang dapat menyebabkan rendahnya *Information Security Awareness* (ISA) di RSUD Haji Makassar.

1.2. Kajian Masalah

Sistem Manajemen Informasi Rumah Sakit (SIMRS) merupakan salah satu subsistem rumah sakit yang digunakan sangat komprehensif, multifungsi, dan berfokus pada fungsi sebagai sistem informasi dengan maksud untuk mendukung prosedur administrasi, keuangan, klinis Rumah Sakit, dan fasilitas pelayanan kesehatan. SIMRS juga berfungsi sebagai sumber informasi penting untuk perawatan pasien dan integrasi dengan organisasi eksternal seperti jaminan kesehatan dan fasilitas pelayanan kesehatan lainnya yang sering terlibat dalam pertukaran informasi (Mokoagow et al., 2024).

RSUD Haji Makassar merupakan rumah sakit yang memberikan pelayanan kesehatan paripurna, rujukan yang berkualitas dan terjangkau bagi masyarakat. RSUD Haji Makassar saat ini berstatus rumah sakit tipe B pendidikan dan berdiri tahun 1992. Rumah sakit ini memiliki visi menjadi rumah sakit terdepan dalam pelayanan dan pendidikan yang bernilai islami di provinsi Sulawesi Selatan menuju Sulsel sehat untuk semua (*Profil RSUD Haji Makassar*, 2023). RSUD Haji Makassar telah menggunakan sistem informasi manajemen sejak tahun 2018 (Meliherdianti et al., 2021). SIMRS yang sedang dikembangkan adalah kegiatan

pelayanan utama (*front office*) diantaranya Antrian Online dengan pendaftaran poliklinik online (Momen Amalia, 2023).

RSUD Haji Makassar menggunakan *username* dan *password* untuk setiap pengguna dalam mengakses SIMRS. Dalam Permenkes Nomor 82 Tahun 2013 tentang SIMRS mengatur mengenai keamanan SIMRS mengatur bagaimana informasi/data hanya bisa diakses, diubah dan tersedia oleh pihak yang berwewenang (Menteri Kesehatan RI, 2013). Permenhan Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber juga mengatur mengenai kebijakan operasional penyelenggaraan pertahanan siber untuk sistem elektronik termasuk layanan kesehatan. Kebijakan tersebut dimaksudkan dalam kegiatan pengembangan dan pertahanan siber salah satunya adalah pelatihan dan kesadaran keamanan. Regulasi ini juga mengatur mengenai sistem manajemen pengamanan informasi adanya perangkat lunak sebagai pendukung spesifik pertahanan siber (Menteri Pertahanan RI, 2014).

Menurut (Willing et al., 2021), faktor manusia merupakan kunci utama dalam mengurangi risiko keselamatan pasien ketika terjadi serangan siber. Pihak rumah sakit perlu meningkatkan kesadaran dan melatih staf sebagai strategi yang efektif dalam mencegah dan mengatasi insiden *cybercrime* di masa yang akan datang. Upaya yang dapat melindungi rumah sakit dan pengguna SIMRS adalah meningkatkan kesadaran keamanan informasi. Kurangnya kesadaran staf seperti tidak adanya pelatihan, mengganti *password* secara berkala dan pelaporan insiden dapat mengakibatkan pelanggaran keamanan (Hore et al., 2024; Kim & Jeoung, 2015).

Menurut (K. Parsons et al., 2014), *Information security awareness* (ISA) dipengaruhi oleh faktor individu, intervensi, dan organisasi. Demografi, faktor psikologis, dan efikasi diri mempengaruhi ISA secara individu. Selain itu, pendidikan, pelatihan dan pengalaman individu juga mempengaruhi ISA. Rendahnya keamanan informasi juga disebabkan oleh faktor organisasi yaitu dari segi norma subjektif, penghargaan, hukuman dan budaya keamanan informasi (McCormac et al., 2017; K. Parsons et al., 2014). Faktor- faktor tersebut dikemukakan oleh Parsons et.al (2014) yang telah di teliti lebih lanjut oleh beberapa ahli (McCormac et al., 2017; K. Parsons et al., 2014). Faktor-faktor organisasi seperti kebijakan keamanan dan komitmen manajemen berpengaruh

besar dalam kesadaran dan niat kepatuhan keamanan informasi karyawan (Gu & Wang, 2024; Haeussinger & Kranz, 2013).

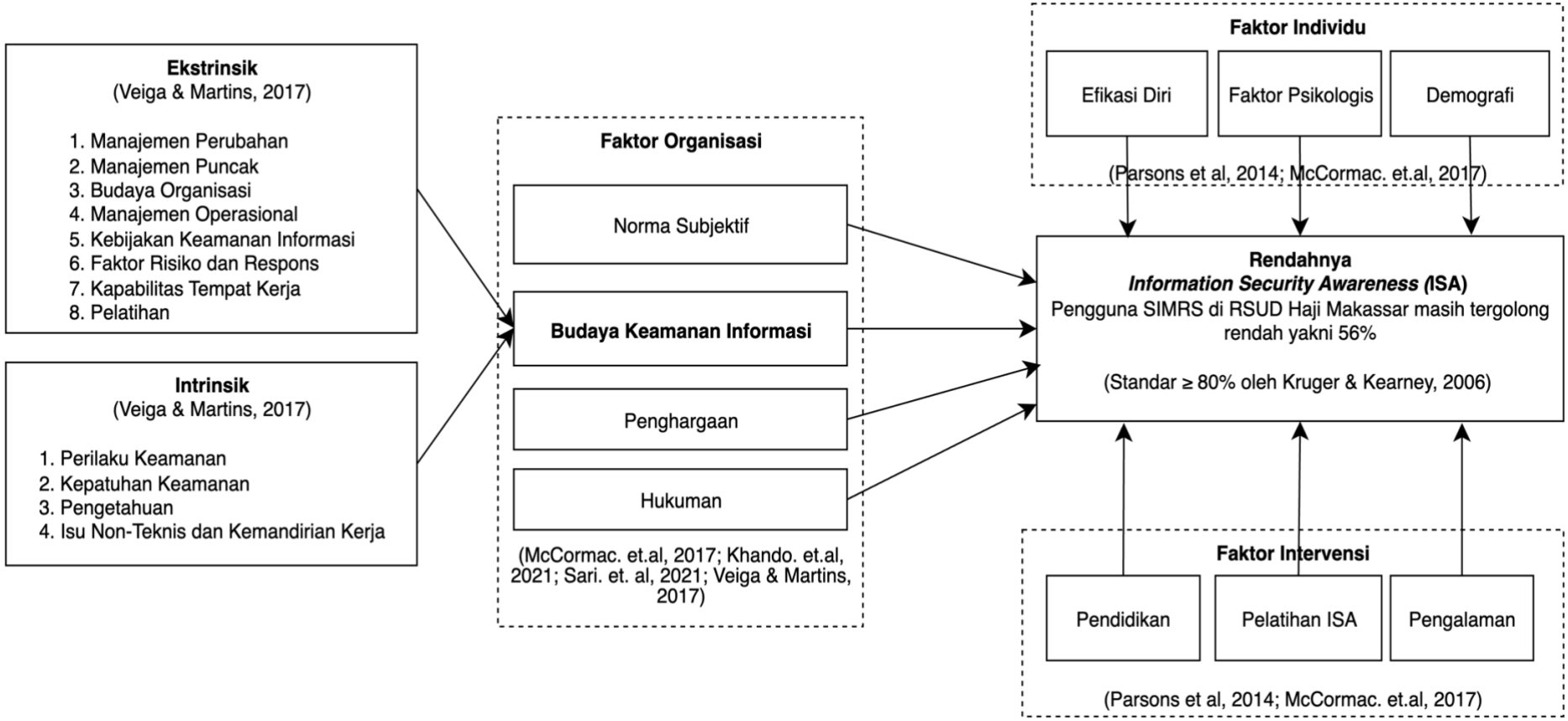
Peneliti menggunakan variabel budaya keamanan informasi dengan model *information security culture assessment* (ISCA) dengan mengadopsi teori *organizational behavior* oleh Stephen P. Robbin (Nasir et al., 2019). Hal ini dikarenakan yang paling mempengaruhi kesadaran dan niat kepatuhan keamanan informasi adalah budaya keamanan (Gu & Wang, 2024). Norma subjektif, penghargaan dan hukuman dapat diperkuat dengan budaya keamanan yang positif (Djotaroeno & Beulen, 2024). Budaya keamanan informasi merupakan komponen penting yang secara efektif mempromosikan perilaku keamanan dan mengelola risiko keamanan dalam organisasi (Nasir et al., 2019). Pegawai dari organisasi budaya keamanan yang baik lebih cenderung memiliki pengetahuan, sikap, dan perilaku sesuai dengan kebijakan dan prosedur keamanan informasi yang diperlukan untuk menjaga keamanan informasi yang baik (Wiley et al., 2020).

Pada penelitian sebelumnya (Sari et al., 2021), dilakukan analisis perbedaan budaya keamanan informasi pada seluruh penyedia layanan kesehatan di Indonesia berdasarkan faktor-faktor yang diambil dari model budaya keamanan informasi oleh (da Veiga & Martins, 2017). Pada model budaya keamanan informasi, ada beberapa faktor yang mempengaruhi budaya keamanan informasi yaitu intrinsik dan ekstrinsik. Faktor ekstrinsik mengacu pada faktor-faktor eksternal dari individu/staf yang dapat mempengaruhi budaya keamanan informasi organisasi. Faktor intrinsik merujuk pada faktor-faktor yang berasal dari dalam individu, seperti kepribadian dan pengalaman pribadi yang dapat memengaruhi cara seseorang memandang keamanan informasi (da Veiga & Martins, 2017).

Penggunaan SIMRS sebagai teknologi informasi memerlukan penerapan keamanan informasi. Hal ini sangat penting untuk melindungi data pasien dan informasi sensitif lainnya dari ancaman siber (Javaid et al., 2023). Oleh karena itu, keamanan informasi berfokus untuk memastikan kerahasiaan, integritas, dan ketersediaan data yang dikelola rumah sakit (Sari et al., 2021).

Berdasarkan survei awal yang dilakukan oleh peneliti, SIMRS pada RSUD Haji Makassar masih dalam proses pengembangan sistem. Instalasi yang telah mengimplementasikan SIMRS adalah pelayanan rawat jalan, pelayanan rawat inap, layanan penunjang (farmasi, laboratorium, radiologi, dan rekam medis) dan

instalasi gawat darurat. Berdasarkan dari kajian masalah tersebut, maka dilakukan analisis pengaruh rendahnya information security awareness (ISA). Berikut gambar kajian penelitian :



Gambar 1 2 Kajian Masalah Penelitian

1.3. Rumusan Masalah

Berdasarkan uraian pada latar belakang bahwa analisis perlu dilakukan untuk menganalisis pengaruh faktor yang mempengaruhi budaya keamanan informasi dan pengaruhnya terhadap *information security awareness* (ISA). Penggunaan aplikasi SIMRS pada RSUD Haji Makassar memiliki manfaat bagi rumah sakit tetapi juga ada risiko keamanan yang akan merugikan. Oleh karena itu, rumusan masalah pada penelitian ini diantaranya :

1. Berapa besarnya pengaruh faktor ekstrinsik terhadap budaya keamanan informasi pada pengguna SIMRS di RSUD Haji Makassar?
2. Berapa besarnya pengaruh faktor intrinsik terhadap budaya keamanan informasi pada pengguna SIMRS di RSUD Haji Makassar?
3. Berapa besarnya pengaruh budaya keamanan informasi terhadap *information security awareness* (ISA) pada pengguna SIMRS di RSUD Haji Makassar?
4. Faktor apa yang paling mempengaruhi budaya keamanan informasi pada pengguna SIMRS di RSUD Haji Makassar?

1.4. Tujuan Penelitian

1.4.1 Tujuan Umum

Untuk menganalisis faktor yang mempengaruhi budaya keamanan informasi dan pengaruhnya terhadap *information security awareness* (ISA) di RSUD Haji Makassar.

1.4.2 Tujuan Khusus

1. Untuk menganalisis besarnya pengaruh faktor ekstrinsik terhadap budaya keamanan informasi di RSUD Haji Makassar.
2. Untuk menganalisis besarnya pengaruh faktor intrinsik terhadap budaya keamanan informasi di RSUD Haji Makassar.
3. Untuk menganalisis besarnya pengaruh budaya keamanan informasi terhadap *information security awareness* (ISA) di RSUD Haji Makassar.
4. Untuk menganalisis faktor yang paling mempengaruhi budaya keamanan informasi pada pengguna SIMRS di RSUD Haji Makassar.

1.5. Manfaat Penelitian

1.5.1 Manfaat Ilmiah

Penelitian ini diharapkan dapat menambah dan memperkaya referensi penelitian terkait Sistem Informasi Manajemen Rumah Sakit khususnya *information security awareness* (ISA) dan sebagai acuan pengembangan penelitian lebih lanjut dalam meningkatkan Sistem Informasi Manajemen Rumah Sakit.

1.5.2 Manfaat Institusi

Penelitian ini diharapkan dapat memberikan masukan bagi pihak manajemen dalam mengevaluasi berbagai faktor yang dapat mempengaruhi *information security awareness* pengguna SIMRS serta dapat digunakan sebagai dasar untuk melakukan perbaikan dan pengembangan yang lebih baik pada SIMRS.

1.5.3 Manfaat Bagi Peneliti

Penelitian ini menjadi pengalaman bagi peneliti dalam melatih kemampuan berpikir secara objektif dan ilmiah. Peneliti dapat mengkaji lebih mendalami tentang teori-teori yang ada serta menghubungkannya dengan realita di lapangan. Selain itu, penelitian ini juga menjadi salah satu persyaratan yang harus dipenuhi oleh peneliti untuk mendapatkan gelar Magister Administrasi Rumah Sakit.

BAB II
TINJAUAN PUSTAKA

2.1 Tinjauan Umum *Information Security*

2.1.1. Definisi *Information Security*

*Information security/*keamanan informasi merupakan tindakan atau sejauh mana setiap anggota staf menyadari pentingnya keamanan informasi, memahami tingkat keamanan yang diperlukan untuk organisasi, mengetahui tanggung jawab dalam hal keamanan, dan berperilaku sesuai dengan pemahaman mereka (Kruger & Kearney, 2006). Menurut G.J. Simons, keamanan informasi atau keamanan data didefinisikan sebagai upaya untuk mencegah atau setidaknya mendeteksi adanya tindakan penipuan (*cheating*) dalam sistem yang berbasis pada informasi (Utomo, 2019). Keamanan informasi bertujuan untuk melindungi informasi secara keseluruhan, termasuk dalam bentuk fisik dan digital (Prathyush & Kumar, 2022).

Menurut standar internasional ISO/IEC 27032:2012, keamanan infromasi didefinisikan sebagai upaya untuk menjaga kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi. 3 konsep kunci ini mencapai sistem keamanan yang ideal yang dikenal sebagai traid CIA. *Confidentiality* mengacu pada kerahasiaan, di mana informasi harus dilindungi agar tidak dapat diakses oleh pengguna yang tidak berwenang. Untuk itu, perlu adanya batasan yang memastikan akses hanya diberikan kepada individu yang memiliki otorisasi. Selain itu, sistem autentikasi sangat penting untuk memverifikasi identitas orang yang diizinkan mengakses data. *Intergrity* yang memastikan bahwa data yang disimpan tetap akurat dan tidak mengalami modifikasi yang tidak sah. Cacat dan kerentanan dalam perangkat lunak dapat menyebabkan kerugian yang tidak diinginkan terhadap integritas data, serta membuka peluang bagi modifikasi yang tidak sah. Umumnya, program mengatur akses baca-tulis ke data tertentu dengan ketat, namun kerentanan perangkat lunak dapat memungkinkan pengguna untuk menghindari kontrol tersebut. *Availability* mengacu pada ketersediaan. Sistem informasi harus selalu dapat diakses oleh pengguna agar dapat memberikan manfaat bagi mereka yang membutuhkannya. Jika sistem yang diperlukan tidak berfungsi atau merespons dengan terlalu lambat, maka sistem tersebut tidak dapat memberikan layanan yang seharusnya (Hanafi, 2022). Dengan adanya kesadaran keamanan dan

mengadopsinya untuk keamanan informasi di antara pengguna adalah salah satu pendekatan terbaik untuk mencegah atau membatasi pelanggaran keamanan dan ancaman serta kejahatan siber (Al-shanfari et al., 2020).

Adapun jenis-jenis ancaman siber dalam dunia maya meliputi:

1. *Malware* adalah suatu bentuk perangkat lunak berbahaya di mana file atau program apa pun dapat digunakan untuk membahayakan pengguna komputer. Hal ini termasuk *worm, virus, Trojan*, dan *spyware*.
2. *Ransomware* adalah jenis malware lainnya. Serangan ini melibatkan penyerang yang mengunci file sistem komputer korban, biasanya melalui enkripsi dan pelaku dapat meminta pembayaran untuk mendekripsi dan membuka kuncinya.
3. *Social engineering* adalah serangan yang mengandalkan interaksi manusia untuk mengelabui pengguna agar melanggar prosedur keamanan untuk mendapatkan informasi sensitif yang biasanya dilindungi.
4. *Phishing* adalah bentuk rekayasa sosial di mana email atau pesan teks palsu yang menyerupai pesan dari sumber yang memiliki reputasi baik atau dikenal dikirim kepada korban. Sering kali dilakukan serangan secara acak, tujuan dari pesan-pesan ini adalah untuk mencuri data sensitif, seperti kartu kredit atau informasi login akun-akun korban.
5. *Spear phishing* adalah jenis serangan phishing yang memiliki target pengguna, organisasi, atau bisnis.
6. *Insider threats* adalah pelanggaran keamanan atau kerugian yang disebabkan oleh manusia. Misalnya, pegawai, kontraktor, atau pelanggan. Serangan ini bisa bersifat jahat atau kelalaian.
7. Serangan *Distributed denial-of-service* (DDoS) adalah serangan yang dilakukan oleh beberapa sistem yang mengganggu lalu lintas sistem yang ditargetkan, seperti server, situs web, atau sumber daya jaringan lainnya. Banyaknya permintaan koneksi atau paket, penyerang dapat memperlambat sistem atau merusaknya, mencegah lalu lintas yang sah menggunakannya.
8. *Advanced persistent threats* (APTs) adalah serangan bertarget yang berkepanjangan di mana penyerang menyusup ke dalam jaringan dan tetap tidak terdeteksi dalam jangka waktu yang lama dengan tujuan untuk mencuri data.

9. *Man-in-the-middle* (MitM) adalah serangan penyadapan yang melibatkan penyerang untuk menyadap dan menyampaikan pesan antara dua pihak yang percaya bahwa mereka sedang berkomunikasi satu sama lain.

Ancaman siber merupakan tantangan yang kompleks bagi keamanan siber dan jumlah serangan siber diperkirakan tidak akan berkurang dalam waktu dekat (Ujjwal Rao, 2023). Upaya organisasi dalam melakukan keamanan informasi salah satunya adalah manajemen risiko keamanan informasi dalam melindungi data dan sistem informasi dalam sebuah organisasi. Pelatihan dan kesadaran keamanan siber juga merupakan aspek penting dari keamanan informasi (Nifakos et al., 2021).

2.2 Tinjauan Umum *Information Security Awareness* (ISA)

2.2.1. Definisi *Information Security Awareness* (ISA)

Kesadaran Keamanan Informasi (*Information Security Awareness*/ISA) adalah proses administrasi dan perlindungan atas informasi pribadi atau aset data perusahaan yang penting dan rahasia. Kesadaran keamanan informasi mencakup pemahaman mengenai kebijakan dan prosedur yang dirancang untuk melindungi data dari akses yang tidak sah, perubahan, atau kerusakan, tanpa memandang bentuknya, baik itu digital, cetak, atau format lainnya (Taherdoost, 2022). Kesadaran keamanan informasi mendalami bagaimana perbedaan individu di antara pegawai mempengaruhi praktik keamanan informasi (Naga et al., 2024).

Definisi kesadaran keamanan informasi terdapat 2 konsep. Konsep kesadaran keamanan informasi pertama kali diperkenalkan oleh Siponen, 2000 yang dimana berfokus pada pemahaman bahwa kesadaran ini mencakup pemahaman pengguna mengenai misi keamanan organisasi. Idealnya, pengguna juga harus berkomitmen untuk mengikuti pedoman keamanan yang telah ditetapkan. Konsep kedua yang diteliti oleh Kruger & Kearney, 2006 berfokus pada sejauh mana pegawai memahami perilaku keamanan informasi yang aman, yang sering kali diuraikan dalam kebijakan, aturan, dan pedoman keamanan informasi organisasi mereka (K. Parsons et al., 2017).

Konsep kesadaran keamanan informasi oleh Siponen, 2000 mengacu pada *theory of reasoned action* (TRA) (Fishbein & Ajzen, 1977)*, theory of planned behaviour* (TPB) (Ajzen, 1991), *intrinsic motivation* (Deci, 1975) yang bertujuan untuk mengubah sikap dan motivasi pengguna. Kemudian pada penelitian Siponen, 2001, menghasilkan dimensi *organizational*, *general public*, *socio-*

political, *computer ethical* dan *institutional education* (Tsohou et al., 2015). Bulgurcu et al. menggabungkan *theory of planned behaviour* (TPB) (Ajzen, 1991) dan *rational choice theory* (Hardin, 2001) yang menggabungkan hasil perilaku sosial dari perilaku individu untuk menguji efek dari kesadaran keamanan informasi terhadap kepercayaan dan sikap. Temuan menunjukkan bahwa kesadaran keamanan informasi mempengaruhi sikap kepatuhan pegawai secara langsung dan tidak langsung melalui keyakinan pegawai (Hwang et al., 2019). Selain itu, *theory of planned behaviour* (TPB) (Ajzen, 1991) juga digunakan meneliti peran kesadaran keamanan informasi pegawai (Grassegger & Nedbal, 2021).

Kruger & Kearney, 2006 mengusulkan yaitu model *Knowledge-Attitude*-Behavior (KAB) untuk mengukur kesadaran keamanan informasi yang kemudian banyak digunakan pada penelitian lain (Fertig & Schutz, 2020). Model tersebut menggunakan teori psikologi sosial membagi tiga komponen untuk mengukur objek yakni *cognition, affection* dan *behaviour* (Akraman et al., 2018). Model KAB menggambarkan bahwa seiring dengan meningkatnya tingkat pengetahuan pengguna komputer akan kebijakan dan prosedur keamanan informasi, maka sikap mereka akan meningkat, yang pada akhirnya akan meningkatkan perilaku keamanan informasi (Fertig & Schutz, 2020; K. Parsons et al., 2017).

Parsons et.al pun mengembangkan pendekatan yang lebih komprehensif terhadap kesadaran keamanan informasi dengan membagi faktor-faktor yang memengaruhinya menjadi tiga domain utama yaitu individu, intervensi dan organisasi (K. Parsons et al., 2014). Karakteristik personal seperti tingkat pendidikan, kepribadian, pengalaman, dan pengetahuan individu terkait keamanan informasi. Individu dengan tingkat literasi digital rendah cenderung memiliki kesadaran yang lemah. Dalam membentuk sikap dan perilaku berkaitan engan program pelatihan, edukasi, kampanye kesadaran, dan kebijakan organisasi yang diterapkan. Pada sisi organisasi, dalam meningkatkan kesadaran keamanan informasi dipengaruhi oleh budaya keamanan, norma subjektif, penghargaan dan hukuman (McCormac et al., 2017; K. Parsons et al., 2014).

2.2.2. Peran Kesadaran Keamanan Informasi

Kesadaran keamanan informasi berperan untuk menguatkan pegawai dengan risiko keamanan informasi dan mendidik mereka tentang peran dan tanggung jawab atas informasi pribadi atau aset data perusahaan yang penting dan rahasia (Hwang et al., 2019).

2.2.3. Faktor-Faktor yang mempengaruhi *Information Security Awareness* (ISA)

Kesadaran Keamanan Informasi (*Information Security Awareness*/ISA) adalah konsep penting yang dapat membantu meminimalkan risiko yang terkait dengan pelanggaran keamanan informasi (Rohan et al., 2023). Dalam upaya mengembangkan dan meningkatkan kesadaran keamanan informasi dalam organisasi maupun kehidupan sehari-hari. Ada beberapa faktor kunci yang dapat memengaruhi tingkat kesadaran keamanan informasi antara lain:

1. Faktor individu

   Insiden keamanan di dalam organisasi ditemukan lebih banyak daripada insiden yang disebabkan oleh pihak eksternal. Temuan menunjukkan bahwa perilaku individu saat ini merupakan sumber dari 34% insiden keamanan (McCormac et al., 2017). Kurangnya kesadaran keamanan informasi pada individu diartikan sebagai rendahnya kapasitas seseorang untuk memahami, mematuhi, dan kebijakan, pedoman, dan peraturan keamanan yang berlaku (Perkasa & Setiawan, 2024).

   Menurut (McCormac et al., 2017), ada beberapa faktor individu yang dapat mempengaruhi kesadaran keamanan informasi, diantaranya demografi, faktor psikologis dan efikasi diri. Penelitian terbaru dalam bidang keamanan informasi menunjukkan adanya perbedaan kecil antara pria dan wanita, serta antara individu dari berbagai kelompok usia. Sebuah studi mengenai *phishing* mengungkapkan bahwa wanita cenderung lebih rentan untuk membuka tautan dalam email *phishing*. Selain itu, individu berusia antara 18 hingga 25 tahun juga ditemukan lebih rentan terhadap *phishing* dibandingkan dengan kelompok usia yang lebih tua (McCormac et al., 2017).

   Menurut (Al-shanfari et al., 2020), faktor psikologi mempengaruhi kesadaran keamanan informasi melalui persepsi risiko; efikasi diri; sikap dan nilai; pengaruh sosial; motivasi; serta pendidikan dan pelatihan. Persepsi risiko yang tinggi, keyakinan pada kemampuan diri, sikap positif terhadap keamanan, dukungan lingkungan kerja, insentif atau ancaman konsekuensi, serta pelatihan yang baik dapat meningkatkan kesadaran dan perilaku keamanan dari individu.

   Efikasi diri atau keyakinan individu terhadap kemampuan mereka berperan penting dalam kesadaran keamanan informasi. Individu dengan efikasi diri yang tinggi cenderung lebih percaya diri dalam menghadapi ancaman

keamanan dan membuat keputusan yang baik terkait perlindungan informasi. Individu lebih mampu menolak tekanan yang dapat membahayakan keamanan dan lebih terlibat dalam pelatihan keamanan. Keyakinan ini juga membuat individu gigih dalam mengatasi tantangan dan lebih konsisten menerapkan praktik keamanan yang tepat. Efikasi diri yang meningkat dapat memperkuat perilaku keamanan informasi pada individu (Al-shanfari et al., 2020).

2. Faktor Intervensi

   Faktor Intervensi dipengaruhi oleh pendidikan, pelatihan dan pengalaman individu terhadap keamanan informasi. Pelatihan memiliki korelasi yang signifikan secara statistik dengan peningkatan tingkat kesadaran keamanan informasi. Misalnya, karyawan yang menjalani pelatihan menunjukkan perilaku keamanan informasi yang lebih baik dibandingkan dengan mereka yang tidak melakukannya (Susanto & Maulana, 2024). Pengalaman juga mempengaruhi individu yang telah merasakan kerugian oleh segala jenis insiden keamanan seperti serangan siber dalam konteks pribadi maupun pekerjaan. Pengalaman tersebut “seperti pernah dirugikan oleh serangan siber atau dihukum karena tidak mematuhi peraturan dan regulasi keamanan dapat meningkatkan kesadaran keamanan informasi seseorang (Al-Shanfari et al., 2022).

3. Faktor organisasi

   Faktor-faktor organisasi memainkan peran kunci dalam membentuk dan mempengaruhi tingkat kesadaran keamanan informasi suatu organisasi. Menurut (McCormac et al., 2017), Faktor-faktor tersebut diantaranya budaya keamanan, norma subjektif, penghargaan, dan hukuman. Budaya organisasi dapat mempengaruhi kesadaran keamanan informasi dengan menetapkan norma dan harapan terkait kepatuhan terhadap kebijakan keamanan informasi. Budaya keamanan mempengaruhi bagaimana individu dalam organisasi memahami dan mempraktikkan keamanan informasi dalam aktivitas sehari-hari mereka. Organisasi dengan budaya keamanan yang kuat cenderung memiliki pegawai yang lebih sadar akan risiko keamanan dan lebih

bertanggung jawab dalam mengamankan informasi dan sistem mereka (Wiley et al., 2020).

Norma subjektif dalam organisasi mempengaruhi kesadaran keamanan informasi individu melalui ekspektasi sosial dan budaya organisasi. Jika pemimpin menekankan pentingnya keamanan, pegawai akan merasa terdorong untuk mengikuti aturan tersebut. Kepemimpinan yang efektif dapat membentuk norma sosial yang menekankan pentingnya keamanan informasi, sehingga pegawai merasa berkewajiban untuk mematuhi kebijakan yang ada (Al-Shanfari et al., 2022).

Sebuah organisasi memberikan penghargaan kepada pegawai yang menunjukkan perilaku keamanan informasi yang baik (Huang & Pearlson, 2019). Menurut (Godson et al., 2023), individu akan merasa lebih positif dalam mempromosikan dan berpartisipasi dalam tindakan keamanan informasi yang tepat jika mereka diajari, diakui dan diberi penghargaan yang Baik.

Ada konsekuensi yang diberikan jika pegawai terbukti melanggar pedoman keamanan informasi yang telah ditetapkan berupa teguran (Huang & Pearlson, 2019). Kurangnya tanggung jawab dan komitmen pegawai dalam menerapkan praktik-praktik keamanan informasi yang baik juga akan menjadi bagian dari penilaian kinerja mereka. Kegagalan dalam memenuhi tanggung jawab tersebut dapat mengakibatkan hukuman atau konsekuensi bagi pegawai yang bersangkutan (Mwim et al., 2023).

2.2.4. Dimensi dan Pengukuran *Information Security Awareness* (ISA)

Berbagai penelitian telah dilakukan untuk mengukur *Information Security Awareness* (ISA). Alat ukur yang sering digunakan diantaranya HAIS-Q, UISAQ dan SeBIS (K. Parsons et al., 2017).

Salah satunya adalah penelitian Galba et al., 2015 dengan menggunakan instrumen *User Information Security Awareness Questionnaire* (UISAQ). UISAQ terdiri dari 33 item yang mencakup perilaku, pengetahuan, serta kesadaran yang berpotensi menimbulkan risiko. Dimensi yang digunakan kuesioner ini adalah, faktor kesadaran, pengetahuan, dan perilaku pengguna internet (Velki et al., 2014). Egelman et al., 2016 telah mengembangkan *Security Behavior Intentions Scale* (SeBIS), yang berfokus pada kepatuhan pegawai terhadap praktik keamanan pada perangkat komputer, seperti kesadaran akan keamanan, pembuatan kata sandi, dan pembaruan (Egelman et al., 2016).

Namun, sejauh ini kuesioner HAIS-Q (*Human Aspects of Information Security Questionnaire)* paling banyak digunakan dalam suatu organisasi termasuk layanan kesehatan (Alkhazi et al., 2022; Yeng et al., 2019). Menurut kutipan dari (Ranas et al., 2020), HAIS-Q telah dinilai secara komprehensif untuk pegawai sementara UISAQ dan SeBIS masih dalam tahap awal pengembangan.

HAIS-Q menggunakan model KAB yang dimana menurut (K. Parsons et al., 2017) HAIS-Q telah menunjukkan adanya hubungan yang kuat antara pengetahuan, sikap, dan perilaku. Responden diinstruksikan untuk menanggapi sejumlah pernyataan dalam skala lima poin dari “1 = Sangat Tidak Setuju” hingga “5 = Sangat Setuju”. Nilai yang lebih rendah dikaitkan dengan kecenderungan untuk terlibat dalam perilaku yang berpotensi berisiko (Hore et al., 2024).

2.3 Tinjauan Umum Budaya Keamanan Informasi (*Information Security Culture*)

2.3.1. Definisi Budaya Keamanan Informasi

Dalam menghadapi tantangan seperti ancaman siber, organisasi tidak hanya mengandalkan teknologi keamanan yang canggih, tetapi juga partisipasi aktif dan keterlibatan individu dalam membentuk budaya keamanan informasi yang kuat. Budaya keamanan informasi mencakup sikap, nilai, dan perilaku individu dalam menangani risiko keamanan informasi. Hal ini melibatkan pemahaman individu tentang pentingnya keamanan informasi, tingkat kepatuhan mereka terhadap kebijakan dan prosedur keamanan, dan partisipasi aktif mereka dalam upaya menjaga keamanan informasi (Prasetyo et al., 2023).

Budaya keamanan Informasi diadaptasi dari konsep teori *Organizational Culture* (OC) (Schein, 2004), *Corporate Culture* (Schein, 1985) , dan *Organizational Behavior*. Teori *Organizational Culture* (OC) oleh Schein, 2004 dikembangkan berdasarkan memiliki tiga dimensi yang merepresentasikan tiga tingkatan, yaitu Artifak dan Kreasi; Nilai, Norma, dan Pengetahuan Kolektif; serta Asumsi Dasar dan Keyakinan (Nasir et al., 2019). Kemudian dikembangkan oleh (Van Niekerk & Von Solms, 2006) untuk menciptakan kepatuhan keamanan informasi yang dapat mengarah pada pengembangan budaya keamanan informasi (Da Veiga & Martins, 2015). Pada teori *Corporate Culture* (Schein, 1985) dikembangkan dengan budaya keamanan informasi oleh (Schlienger & Teufel, 2003). Teori ini didasarkan pada pemasaran internal untuk menganalisis budaya keamanan informasi suatu organisasi, dalam rangka menciptakan, mengubah, dan memelihara budaya keamanan informasi dengan lima fase utama: pra-

evaluasi, perencanaan strategis, perencanaan operasional, implementasi, dan pasca-evaluasi (Alhogail & Mirza, 2014b).

Teori *Organizational Behavior* (Robbins, 2002) diadaptasi menjadi sebuah model pengukuran budaya keamanan informasi dalam organisasi. Model ini terdiri dari tiga dimensi, yaitu Organisasi; Kelompok; dan Individu. Setiap level memiliki sub-dimensi masing-masing yaitu kebijakan dan prosedur; analisis risiko; tolok ukur; anggaran; manajemen; kepercayaan; kesadaran; perilaku etis; dan perubahan (Nasir et al., 2019). Teori ini menyelidiki perilaku pegawai dan interaksi mereka dengan sistem informasi di organisasi (Da Veiga & Martins, 2015).

2.3.2. Peran Budaya Keamanan Informasi

Budaya keamanan informasi yang kuat berperan sebagai pelindung terhadap ancaman dari manusia dalam perlindungan data, sehingga mengurangi jumlah insiden atau pelanggaran. Hal ini melibatkan pengembangan kesadaran, pengetahuan, dan perilaku pegawai yang sejalan dengan kebijakan keamanan informasi organisasi (Da Veiga et al., 2020).

2.3.3. Faktor-faktor yang Mempengaruhi Budaya Keamanan Informasi

Adapun faktor-faktor yang mempengaruhi budaya keamanan informasi diantaranya manajemen perubahan; manajemen puncak; budaya organisasi; manajemen operasional; kebijakan keamanan informasi; faktor risiko dan tindakan; kemampuan di tempat kerja, pelatihan dan kesadaran; perilaku keamanan; kepatuhan keamanan; pengetahuan; serta isu non-teknis dan kemandirian kerja. Faktor-faktor ini dikelompokkan menjadi faktor intrinsik dan ekstrinsik (da Veiga & Martins, 2017; Sari et al., 2021).

Kemudian, pada penelitian (Da Veiga et al., 2020) faktor-faktor tersebut dikembangkan menjadi faktor eksternal dan internal. Faktor eksternal meliputi budaya nasional; faktor politik dan hukum; faktor ekonomi; faktor sosial budaya; serta faktor teknis dan teknologi. Sedangkan faktor internal meliputi faktor organisasi, manajemen, manusia dan *mutual trust.*

2.3.4. Dimensi dan Pengukuran Budaya Keamanan Informasi

Berbagai penelitian telah dilakukan untuk mengukur budaya keamanan informasi. Alat ukur yang sering digunakan diantaranya, *The Socio-Cultural Dimension*, Von Solms' *security culture framework,* ISCA dan ISCF (Nasir et al., 2019).

The Socio-Cultural Dimension digunakan oleh Schlienger & Teufel, 2002 sebagai dimensi untuk mengukur budaya keamanan informasi dengan terdiri dari tiga dimensi yaitu politik perusahaan; manajemen; dan individu. Dimensi tersebut berasal dari teori *Organizational Culture* (OC) (Nasir et al., 2019). Sama halnya dengan Von Solms' *security culture framework* oleh Van Niekerk & Von Solms, 2006*,* yang meneliti dimensi budaya keamanan informasi. Ada tiga dimensi yang digunakan berdasarkan program keamanan informasi yaitu kebijakan keamanan, SETA, dan pemantauan komputer (Nasir et al., 2019).

Information Security Culture Framework (ISCF) dikembangkan oleh Alhogail dengan lima dimensi diantaranya : strategi, teknologi, organisasi, orang, dan lingkungan. Kerangka ini menggabungkan empat domain utama dari faktor manusia seperti kesiapsiagaan, tanggung jawab, manajemen, serta masyarakat dan peraturan. Selain itu, kerangka kerja ini juga menggabungkan prinsip-prinsip manajemen perubahan yang memandu pengembangan budaya keamanan informasi (Alhogail & Mirza, 2015).

Instrumen *Information Security Culture Assesment* (ISCA) mengadopsi teori *Organizational Behavior* (OB) oleh Robbins dan instrumen ISCF (Nasir et al., 2019). Martins & da Veiga, 2015 telah terbukti secara statistik bahwa dimensi yang sama dapat diterapkan pada organisasi internasional yang beroperasi di negara yang berbeda, dengan mempertimbangkan tingkat kematangan perlindungan data yang bervariasi. ISCA berfokus pada elemen manusia dengan menyediakan pendekatan yang dapat digunakan untuk mengembangkan, menilai, dan memantau budaya keamanan informasi (Da Veiga & Martins, 2015). Ada 10 dimensi yang digunakan dalam mengukur budaya keamanan informasi diantaranya : manajemen aset informasi, manajemen keamanan informasi, perubahan, manajemen pengguna, kebijakan keamanan informasi, kepercayaan, kepemimpinan keamanan informasi, pelatihan dan kesadaran, privasi dan program keamanan informasi (da Veiga & Martins, 2017).

2.4 Tinjauan Umum Faktor Intrinsik dan Ekstrinsik

Menurut (Sari et al., 2021) ada dua faktor mempengaruhi budaya keamanan informasi khususnya pada layanan kesehatan. Adapun dua faktor yang mempengaruhi budaya keamanan informasi, diantaranya :

1. Faktor Intrinsik

Faktor intrinsik merujuk pada faktor-faktor yang berasal dari dalam individu, seperti kepribadian dan pengalaman pribadi yang dapat memengaruhi cara seseorang memandang keamanan informasi (da Veiga & Martins, 2017). Pada penelitian (Sari et al., 2021) dalam faktor intrinsik terdapat faktor-faktor diantaranya:

a) Perilaku Keamanan

Setiap individu dalam organisasi, meskipun memiliki niat baik untuk mengikuti kebijakan keamanan informasi, tetap dianggap sebagai titik lemah dalam perlindungan keamanan informasi. Hal ini disebabkan oleh kemungkinan perilaku keamanan yang mereka lakukan tidak sejalan dengan perilaku yang diharapkan (Shropshire et al., 2015). Perilaku keamanan dapat membantu menumbuhkan budaya keamanan (Hassan et al., 2017).

b) Kepatuhan Keamanan

Kepatuhan terhadap kebijakan keamanan informasi dapat menurunkan risiko pelanggaran keamanan informasi dalam organisasi (Safa et al., 2016). Pemahaman pegawai tentang prosedur dan kebijakan keamanan akan berdampak positif pada sikap sehinggan menghasilkan kepatuhan sebagai ciri khas dari budaya keamanan informasi yang kuat (Sari et al., 2021).

c) Pengetahuan

Pemahaman individu mencakup pengetahuan tentang risiko dan ancaman potensial terhadap keamanan informasi, serta praktik dan kebijakan yang harus dipatuhi (Prasetyo et al., 2023). Budaya keamanan informasi yang efisien bergantung pada pemahaman pegawai terhadap keamanan informasi karena setiap pegawai memiliki pengetahuan yang berbeda dan setiap organisasi memiliki praktik keamanan yang unik (Sari et al., 2021).

d) Isu Non-Teknis dan Kemandirian Kerja

Masalah-masalah yang dihadapi pegawai, seperti paparan terhadap ancaman data, insiden keamanan, liputan media, kepentingan pribadi, dan kesadaran kelompok atau masyarakat, dapat mempengaruhi budaya keamanan informasi. Selain itu, kepribadian pegawai dan pengalaman

mereka dalam insiden keamanan juga berperan dalam mempengaruhi perilaku mereka terhadap kebijakan dan praktik keamanan di dalam organisasi, yang pada gilirannya berdampak pada budaya keamanan secara keseluruhan (Sari et al., 2021).

2. Faktor Esktrinsik

Faktor ekstrinsik mengacu pada faktor-faktor eksternal dari individu/staf yang dapat mempengaruhi budaya keamanan informasi organisasi (da Veiga & Martins, 2017). Pada penelitian (Sari et al., 2021) dalam faktor intrinsik terdapat faktor-faktor diantaranya:

a) Manajemen Perubahan

Prosedur manajemen perubahan perlu mendukung adopsi teknologi baru dan membantu staf dalam mengintegrasikan serta menerima perubahan tersebut agar menjadi bagian dari budaya organisasi. Penerapan teknologi yang tepat dapat meningkatkan keamanan, kualitas, efektivitas, dan keandalan, yang secara signifikan mempengaruhi fungsionalitas, kegunaan, privasi, dan keamanan informasi (da Veiga & Martins, 2017). Manajemen perubahan sering diidentifikasi sebagai kunci keberhasilan sistem informasi, didukung dengan komitmen manajemen dan kepemimpinan (Sari et al., 2021).

b) Manajemen Puncak

Manajemen puncak memainkan peran penting dalam pembentukan budaya keamanan. Komitmen yang kuat dari manajemen dan kepemimpinan diperlukan sejak tahap awal untuk memastikan keberhasilan jangka panjang dalam menciptakan budaya keamanan informasi. Selain itu, manajemen puncak dapat mendukung pelatihan pengguna, mempromosikan kesadaran akan keamanan, serta memastikan bahwa kebijakan keamanan tetap relevan, *up to date*, dan dilaksanakan secara berkelanjutan (Alnatheer, 2015).

c) Budaya Organisasi

Budaya organisasi menurut (Schein, 1985) merupakan bagaimana seorang pegawai memandang organisasi. Pemahaman mengenai budaya organisasi mengarah pada pengelolaan budaya keamanan informasi yang tepat. Namun, tiap individu dalam setiap organisasi dipengaruhi oleh beberapa budaya etika, nasional dan organisasi yang akan

mempengaruhi cara mereka menafsirkan makna dan pentingnya keamanan informasi (Alnatheer, 2015).

d) Manajemen Operasional

Organisasi perlu menerapkan pendekatan komprehensif dalam mengelola dan mengatur sistem informasi dengan berfokus pada penilaian risiko. Melalui manajemen yang efektif, tinjauan berkala, audit, dan pemantauan yang tepat, organisasi dapat membangun dan memelihara budaya keamanan informasi yang positif (da Veiga & Martins, 2017).

e) Kebijakan Keamanan Informasi

Kebijakan keamanan adalah persyaratan keamanan yang paling penting bagi semua organisasi yang mengakses informasi. Kebijakan keamanan tidak hanya mengacu pada satu jenis kebijakan standar, tetapi harus dioptimalkan sesuai dengan tugas, tujuan, dan fitur organisasi seperti jenis, ukuran, peran, dan manajemen sistem informasi (Kim & Jeoung, 2015). Partisipasi aktif terhadap kebijakan keamanan informasi mencakup perilaku individu dalam menerapkan kebijakan keamanan informasi (Prasetyo et al., 2023).

f) Faktor Risiko dan Tindakan

Faktor risiko dan tindakan berfokus pada upaya meminimalkan risiko keamanan informasi. Cara organisasi dalam mengidentifikasi, mencegah, mendeteksi, dan menanggapi insiden keamanan secara langsung mempengaruhi budaya keamanan informasi (Sari et al., 2021).

g) Kemampuan di Tempat Kerja

Kemampuan di tempat kerja mencakup berbagai sub-faktor, antara lain kegunaan sistem, tingkat pergantian pegawai, ketergantungan pada tenaga kerja sementara, kompetensi pegawai, efektivitas prosedur pemantauan, kepuasan kerja, tekanan dalam tugas, signifikansi tugas, praktik keamanan, prosedur disipliner, pemantauan keamanan, pengawasan, kinerja, dan penghargaan (Ali et al., 2020). Sub-faktor tersebut dapat memengaruhi budaya keamanan dan perilaku keamanan pegawai (Sari et al., 2021).

h) Pelatihan

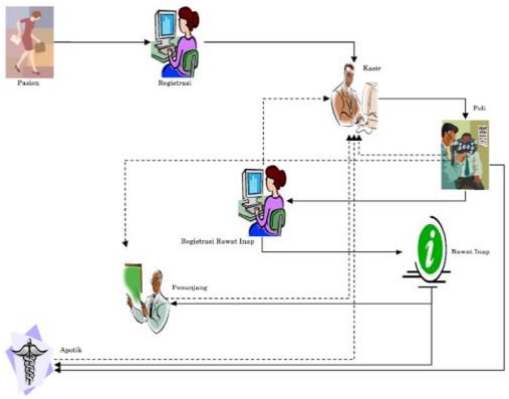
Kesadaran terhadap keamanan informasi mengacu pada berbagi informasi melalui pendidikan dan pelatihan pegawai tentang risiko kerahasiaan data, integritas, dan upaya untuk melindungi keamanannya. Karakter yang positif akan dipahami oleh seseorang melalui proses yang panjang atau latihan kebiasaan. Oleh karena itu, pendidikan karakter menjadi penting untuk menanamkan nilai-nilai menjaga kerahasiaan informasi (Budiningsih et al., 2019). Kesadaran dan pelatihan tentang keamanan informasi harus dilakukan agar pegawai memahami risiko terkait data, prosedur pemeriksaan yang tepat, serta kebijakan yang harus diikuti dalam budaya keamanan informasi. Dalam konteks pengguna sistem informasi rumah sakit, pelatihan harus secara kreatif menekankan pentingnya membangun kesadaran di kalangan staf (Sari et al., 2021).

Faktor-faktor tersebut merupakan disimpulkan oleh (da Veiga & Martins, 2017) yang dapat mempengaruhi budaya keamanan informasi pada bank global berbagai negara Sebagian besar di Afrika Selatan. Menurut (Sari et al., 2021), Afrika Selatan merupakan negara berkembang seperti Indonesia dan keamanan informasi layanan kesehatan memiliki tingkat urgensi yang sama dengan perbankan. Keamanan informasi layanan kesehatan memiliki nilai kerahasiaan, ketersediaan, dan integritas data yang sangat tinggi (Sari et al., 2021).

2.5 Tinjauan Umum Sistem Informasi Manajemen Rumah Sakit (SIM RS)

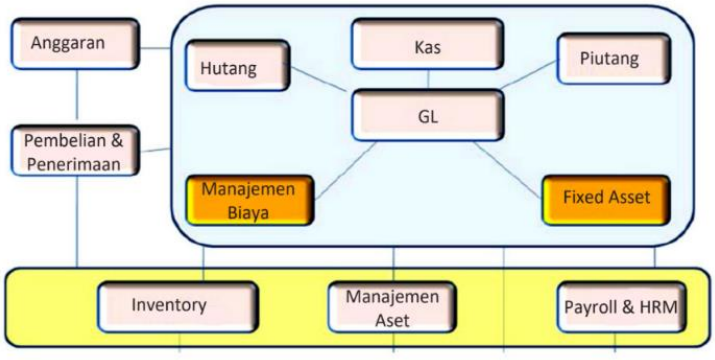
SIMRS merupakan salah satu bagian dari implementasi program e-health yaitu teknologi informasi dan komunikasi yang terintegrasi untuk memproses dan mengkoordinasikan seluruh alur proses pelayanan di rumah sakit. SIMRS berfungsi sebagai jaringan yang menghubungkan berbagai prosedur administrasi dan pelaporan, dengan tujuan untuk memperoleh informasi secara tepat dan akurat. (Menteri Kesehatan RI, 2013). Peraturan Kementerian Kesehatan RI Nomor 82 Tahun 2013 menegaskan seluruh Rumah Sakit Indonesia wajib untuk mengadopsi dan mengimplementasikan SIMRS dengan tujuan untuk meningkatkan dan memastikan integritas data pasien yang ada dalam lingkungan rumah sakit (Yunus et al., 2023). Regulasi tersebut juga menjelaskan arsitektur SIMRS paling sedikit terdiri atas kegiatan pelayanan utama (*front office*); kegiatan administratif (*back office*); komunikasi dan kolaborasi.

Rumah sakit secara umum memiliki prosedur pelayanan teintegrasi yang sama mulai dari proses pendaftaran, proses rawat (jalan atau inap) hingga proses pemulangan pasien. SIMRS harus dapat mengakomodasi kebutuhan minimum untuk kegiatan poliklinik pada pelayanan rawat jalan. Selama proses perawatan, pasien akan menggunakan berbagai sumber daya dan mendapatkan layanan serta tindakan dari unit-unit seperti farmasi, laboratorium, radiologi, gizi, bedah, invasif, diagnostik, non-invasif, dan lainnya. Unit-unit tersebut menerima pesanan/order dari dokter (misalnya resep untuk farmasi, formulir laboratorium, dll.) dan perawat, yang dapat ditangani melalui sistem komunikasi order (*Order Communication System* atau OCS) (Handayani, 2021).



Gambar 2.1 Prosedur Umum Pelayanan Terintegrasi dalam Kegiatan Pelayanan Utama

Rumah sakit juga melakukan kegiatan administratif seperti perencanaan, pembelian/pengadaan, pemeliharaan stok/investori, pengelolaan aset, pengelolaan SDM, pengelolaan uang (utang, piutang, kas, buku bekas dan lainnya). Proses *back office* yang bersifat administratif ini harus terhubung dan terintegrasi dengan proses *front office* yang berhubungan dengan pelayanan klinis kepada pasien (Handayani, 2021).



Gambar 2.2 Hubungan antar Proses *Back Office* di Rumah Sakit

Rumah sakit juga harus memiliki standar pertukaran data yang dapat digunakan untuk dapat berkomunikasi satu aplikasi dengan aplikasi lainnya yaitu *Health Level* 7 (HL7), DICOM dan XML (*Extensible Markup Language*) (Handayani, 2021).

2.6 Implementasi Kesadaran Keamanan Informasi di Rumah Sakit

Sejak terjadinya pandemi COVID-19, tingkat adopsi teknologi pada industri kesehatan semakin diimplementasikan secara cepat. Menurut *World Health Organization* (WHO), teknologi informasi semakin umum digunakan dalam perawatan kesehatan primer, termasuk perangkat seperti ponsel pintar, tablet, dan komputer laptop. Teknologi digital memungkinkan pengelolaan kesehatan yang lebih efektif, diagnosis yang lebih baik, dan pemantauan dampak kebijakan kesehatan.

Keamanan informasi sangat penting untuk Sistem Informasi Manajemen Rumah Sakit (SIMRS) karena melibatkan informasi sensitif pasien, data medis, dan informasi penting lainnya (Nifakos et al., 2021). Pada Permenkes Nomor 82 Tahun 2013 tentang Sistem Informasi Manajemen Rumah Sakit, ada beberapa poin yang memperkuat bahwa keamanan siber penting tersedia di Rumah Sakit diantaranya :

1. Kerahasiaan Data

   Data pasien dan informasi medis yang disimpan dalam SIMRS harus dijaga kerahasiaannya agar tidak disalahgunakan atau diakses oleh pihak yang tidak berwenang (Nifakos et al., 2021). Hal ini sesuai dengan Pasal 7 yang mengamanatkan SIMRS harus memenuhi unsur keamanan secara fisik, jaringan, dan sistem aplikasi (Menteri Kesehatan RI, 2013). Pada UU No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi dalam pasal 35-38 menyebutkan bahwa Pengendali Data Pribadi wajib melindungi, mencegah, memastikan Data Pribadi dari pemrosesan yang tidak sah (Presiden RI, 2022).
2. Integritas Data

   Penting untuk memastikan bahwa data dalam SIMRS tidak diubah tanpa izin, sehingga informasi yang disediakan tetap akurat dan dapat dipercaya (Nifakos et al., 2021). Hal ini sesuai dengan Pasal 4 yang menekankan pentingnya pengelolaan dan pengembangan SIMRS (Menteri Kesehatan RI, 2013).

3. Perlindungan Terhadap Serangan

   Peningkatan ancaman serangan siber, seperti *malware* dan *ransomware*, perlindungan sistem SIMRS menjadi krusial untuk mencegah kerugian dan gangguan dalam operasional rumah sakit (Nifakos et al., 2021). Hal ini dibahas dalam Bab II tentang keamanan sistem informasi manajemen rumah sakit, termasuk kebijakan hak akses dan keamanan jaringan untuk mencegah penyalahgunaan sumber daya jaringan (Menteri Kesehatan RI, 2013).

4. Kepatuhan Regulasi

   Rumah sakit diwajibkan untuk mematuhi regulasi terkait keamanan data pasien , seperti Undang-Undang Kesehatan dan peraturan lainnya, sehingga keamanan keamanan informasi menjadi bagian integral dari kepatuhan tersebut (Panattoni, 2020). Hal ini sesuai dengan Pasal 5 yang mengharuskan Rumah Sakit untuk berintegrasi dengan program pemerintah dan pemerintah daerah (Menteri Kesehatan RI, 2013).

Menurut (Yeng et al., 2019), sektor kesehatan memiliki data 10 kali lipat lebih mahal daripada data kartu kredit dari bank dalam pasar siber. Hal ini dikarenakan data perawatan kesehatan dapat digunakan untuk melakukan berbagai pencurian identitas termasuk pembuatan klaim asuransi kesehatan palsu, kartu identitas palsu untuk membeli obat-obatan dan peralatan medis. Data kesehatan yang dicuri juga dapat digunakan untuk mendapatkan perawatan medis dan mendapatkan akses ke informasi data lainnya. Dengan manusia sebagai mata rantai yang paling rentan dalam rantai keamanan, siber beralih untuk mengeksplorasi pada individu dan masuk ke dalam sistem. Praktik staf layanan kesehatan juga dapat dengan sengaja atau tidak sengaja menyebabkan pelanggaran keamanan internal dan konsekuensinya berkisar dari penipuan hingga hilangnya nyawa manusia (Yeng et al., 2019).

2.7 Review Penelitian Terkait

Berdasarkan hasil kajian peneliti, maka berikut review dari hasil penelitian yang terkait:

Tabel 2.1 Review Penelitian Terkait

No	Penulis	Judul	Variabel Dependen	Variabel Independen	Populasi dan Sampel	Metode	Hasil Penelitian	Persamaan dan Perbedaan
1	Yeng, et al., (2022)	*A Comprehensive Assessment of Human Factors in Cyber Security Compliance toward Enhancing the Security Practice of Healthcare Staff in Paperless Hospitals*	*Security Practice* staf layanan kesehatan di Rumah Sakit	1. *Risk perseption* 2. *Information Security Culture* 3. *Personality Factors* 4. *Information Security Knowledge* 5. *Information Security Attitude* 6. *Self-Reported Conscious Care Security Behavior*	212 responden yang terdiri dari staf kesehatan RS seperti dokter, perawat, personel laboratorium klinis, personel IT, dan lainnya.	Kuantitatif	Pada level individual, aspek-aspek seperti pengetahuan, sikap, dan perilaku kesadaran keamanan informasi, serta dimensi kepribadian seperti kesadaran dan keterbukaan, memainkan peran penting dalam menentukan risiko keamanan. Sementara, pada level kontekstual, kondisi kerja yang menantang, seperti keadaan darurat dan beban kerja darurat, juga terbukti berkontribusi secara signifikan terhadap praktik keamanan staf kesehatan.	Persamaan : Penelitian ini melihat faktor-faktor yang mempengaruhi kesadaran dan perilaku keamanan informasi pada staf kesehatan Perbedaan : Penelitian ini melihat dampak dari faktor kerja seperti beban kerja dan keadaan darurat kerja dan terdapat faktor ciri-ciri kepribadian.
2	Parsons et al., (2017)	*The Human Aspects of Information Security Questionnaire*	Tingkat kepatuhan terhadap kebijakan	Informasi keamanan kesadaran individu	Pekerja di berbagai organisasi pemerintah Australia	Analisis faktor, uji reliabilitas internal	Studi 1, peserta dengan skor lebih Baik pada HAIS-Q menunjukkan kinerja yang lebih baik dalam	Persamaan : Penelitian ini menggunakan HAIS-Q untuk melihat hubungan

No	Penulis	Judul	Variabel Dependen	Variabel Independen	Populasi dan Sampel	Metode	Hasil Penelitian	Persamaan dan Perbedaan
		(HAIS-Q): Two further validation studies.	keamanan informasi				eksperimen phishing. Hal ini menunjukkan bahwa HAIS-Q dapat memprediksi aspek tertentu dari perilaku keamanan informasi, serta mendukung validitas konvergensinya. Sementara itu, Studi 2 menunjukkan bahwa analisis faktor dan teknik statistik lainnya memberikan bukti yang mendukung HAIS-Q sebagai alat ukur yang efektif untuk kesadaran keamanan informasi.	pengetahuan sikap individu Perbedaan : Penelitian ini menggunakan sampel dari pekerja berbagai organisasi pemerintah Australia
3	Naga et al., (2024)	*Investigating the Relationship Between Personality Traits and Information Security Awareness*	Perilaku Pengambilan Risiko Keamanan Informasi	1. Komponen KAB (*Knowledge, Attitude, and Behavior*) 2. *The Big Five Personality Traits* (BFI) seperti - *Neuroticism* - *Extraversion* - *Openness* - *Agreeableness*	311 responden dengan populasi dari 7.718 mahasiswa sarjana dari berbagai tingkat tahun di tujuh fakultas di institusi yang bersangkutan.	Kuantitatif	Penelitian ini menemukan bahwa korelasi antara karakteristik *Big Five Inventory* (BFI) dengan perilaku risiko *information security* pengguna akhir. Sifat-sifat seperti *agreeableness, antagonism, neuroticism, lack of direction*, dan *extraversion* memiliki hubungan yang	Persamaan : Penelitian ini juga menggunakan model KAB untuk mengukur kesadaran keamanan informasi Perbedaan : Penelitian ini dihubungkan dengan *personality traits* individu

No	Penulis	Judul	Variabel Dependen	Variabel Independen	Populasi dan Sampel	Metode	Hasil Penelitian	Persamaan dan Perbedaan
				- *Conscientiousness*			signifikan dengan perilaku *information security*.	
4	Sari et al., (2021)	*Information Security Cultural Differences Among Health Care Facilities In Indonesia*	Budaya Keamanan Informasi	1. *Top Management Support* 2. *Workplace Capabilities* 3. *Risk and Response Factors* 4. *Operational Management* 5. *Change Management* 6. *Organizational Culture* 7. *Information Security Policies* 8. *Training and Awareness* 9. *Security Behavior* 10. *Soft Issues and Workplace Independence* 11. *Security Compliance* 12. *Knowledge*	470 responden terdiri pegawai yang bekerja di berbagai fasilitas kesehatan di Indonesia, khususnya di kota Bandung	Kuantitatif	Penelitian ini menemukan perbedaan signifikan dalam faktor budaya keamanan informasi di berbagai jenis fasilitas kesehatan, dengan faktor seperti dukungan manajemen puncak, manajemen perubahan, dan pengetahuan menunjukkan perbedaan yang jelas, sementara kemampuan tempat kerja, faktor tindakan risiko, dan manajemen operasional menunjukkan kesamaan di semua jenis fasilitas tersebut.	Persamaan : Penelitian ini juga menggunakan faktor intrinsik dan ekstrinik sebagai variabel independen dan dilakukan pada rumah sakit Perbedaan : Penelitian ini berfokus pada budaya keamanan informasi di layanan kesehatan tidak hanya rumah sakit

No	Penulis	Judul	Variabel Dependen	Variabel Independen	Populasi dan Sampel	Metode	Hasil Penelitian	Persamaan dan Perbedaan
5	Da Veiga & Martins, (2017)	*Defining and Identifying Dominant Information Security Cultures and Subcultures*	Budaya Keamanan Informasi	- *Employee Behavior* - *IS Policies* - *IS Strategy and Vision of Management*	Semua pegawai di organisasi mencakup semua 22 kantor yang terpisah secara geografis di 12 negara	Kuantitatif	Penelitian ini menunjukkan bahwa tingkat kesadaran pegawai terhadap kebijakan keamanan informasi cukup Baik, dengan sebagian besar pegawai merasa bahwa isi kebijakan tersebut mudah dipahami. Selain itu, penelitian ini mengidentifikasi perbedaan dalam persepsi budaya keamanan informasi di antara berbagai subkultur dalam organisasi. Metode survei yang digunakan terbukti efektif dalam mengumpulkan data dari populasi yang besar dan beragam.	Persamaan : Penelitian ini juga menggunakan faktor intrinsik dan ekstrinik pada perilaku pegawai sebagai faktor budaya keamanan informasi Perbedaan : Penelitian ini memvalidasi intrumen yang digunakan untuk mengukur budaya keamanan informasi di beberapa negara
6	McCormac et al., (2017)	*Individual Differences and Information Security Awareness*	*Information Security Awareness*	- *Demographics* - *Personality and The Big Five Model* - *Risk-taking Propensity*	505 responden terdiri dari pekerja di Australia	Kuantitatif	Penelitian ini menunjukkan hubungan antara perbedaan individu, seperti kepribadian dan persepsi pengambilan risiko dengan kesadaran keamanan informasi. Kemudian, ditemukan	Persamaan : Penelitian ini juga berfokus pada *information security awareness* dari persepsi individu dan organisasi Perbedaan : Penelitian ini lebih menekankan pada

No	Penulis	Judul	Variabel Dependen	Variabel Independen	Populasi dan Sampel	Metode	Hasil Penelitian	Persamaan dan Perbedaan
							bahwa kelompok usia 18-29 tahun memiliki skor ISA lebih Kurang Baik, dan faktor *conscientiousness* serta *emotional stability* berhubungan positif dengan ISA, sementara persepsi pengambilan risiko berhubungan negatif.	perbedaan individu di organisasi negara Australia
7	Da Veiga et al., (2020)	*Defining Organisational Information Security Culture— Perspectives from Academia and Industry*	Budaya Keamanan Informasi	- Faktor Intrinsik - Faktor Ekstrinsik	261 responden yang berpartisipasi dalam penelitian ini berasal dari berbagai tingkat manajemen, termasuk manajemen eksekutif, manajemen puncak, dan staf operasional. Responden juga mencakup organisasi yang beroperasi di	*Mix Method*	Hasil penelitian menunjukkan bahwa pendidikan, pelatihan, dan kesadaran tentang keamanan informasi memiliki pengaruh positif, dan merekomendasikan studi empiris lebih lanjut setelah langkah-langkah peningkatan kesadaran diambil. Selain itu, pengetahuan tentang kebijakan keamanan informasi dapat meningkatkan sikap pegawai terhadap kepatuhan, mencerminkan budaya keamanan informasi yang kuat.	Persamaan : Penelitian ini juga berfokus pada pengaruh faktor-faktor yang mempengaruhi budaya keamanan informasi Perbedaan : Penelitian ini membuat kerangka pembaharuan dari ISCA yang dapat digunakan dalam organisasi

No	Penulis	Judul	Variabel Dependen	Variabel Independen	Populasi dan Sampel	Metode	Hasil Penelitian	Persamaan dan Perbedaan
					berbagai sektor industri, terutama yang berbasis di Afrika Selatan.			
8	Alkhazi et al., (2022)	*Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior*	KAB	*Information Security Awareness Training*	140 responden yang direkrut dari empat lembaga pemerintah yang berbeda	Kuantitatif	Penelitian ini menunjukkan bahwa semua metode pelatihan yang diterapkan berhasil meningkatkan pengetahuan peserta tentang keamanan informasi dalam metode pelatihan berdampak positif pada sikap peserta, serta metode berbasis teks dan permainan menghasilkan perubahan perilaku yang lebih baik.	Persamaan : Penelitian ini juga berfokus pada *information security awareness* Perbedaan : Penelitian ini lebih menekankan efektivitas metode pelatihan, seperti berbasis teks dan permainan di berbagai lembaga pemerintah
9	Wiley et al., (2020)	*More Than The Individual: Examining The Relationship Between Culture and Information Security Awareness*	*Information Security Awareness*	- *Organisational Culture* - *Security Culture*	508 responden terdiri dari pekerja di Australia yang terlibat dalam berbagai industri.	Kuantitatif	Penelitian ini menunjukkan bahwa budaya organisasi dan budaya keamanan memiliki pengaruh signifikan terhadap *information security awareness* di kalangan pekerja, di	Persamaan : Penelitian ini juga berfokus budaya keamanan terhadap *information security awareness* Perbedaan : Penelitian ini menggunakan

No	Penulis	Judul	Variabel Dependen	Variabel Independen	Populasi dan Sampel	Metode	Hasil Penelitian	Persamaan dan Perbedaan
							mana budaya yang mendukung praktik keamanan cenderung meningkatkan kesadaran dan kepatuhan terhadap kebijakan.	sampel dari pekerja berbagai industri di Australia
10	Chua et al., (2021)	*Identifying the Effect of Data Breach Publicity on Information Security Awareness Using Hierarchical Regression*	*Information Security Awareness*	- *Demographic* - *Known ISA* - *Data Breach Publicity*	529 responden survei online terdiri dari individu yang bekerja di berbagai industri di Malaysia	Kuantatif	Penelitian ini menemukan bahwa peningkatan kesadaran tentang insiden pelanggaran data dapat meningkatkan pemahaman individu tentang keamanan informasi dengan DBR memiliki koefisien terBaik dibandingkan faktor-faktor lain,	Persamaan : Penelitian ini juga berfokus pada *information security awareness* Perbedaan : Penelitian ini meneliti *Data Breach Publicity* sebagai faktor baru yang mempengaruhi ISA

Berdasarkan tabel review penelitian terkait, keseluruhan jurnal tersebut dari berhubungan dengan penelitian yang peneliti lakukan tetapi yang paling mendekati adalah jurnal penelitian (da Veiga & Martins, 2017; Sari et al., 2021; Wiley et al., 2020).

2.8 Mapping Teori

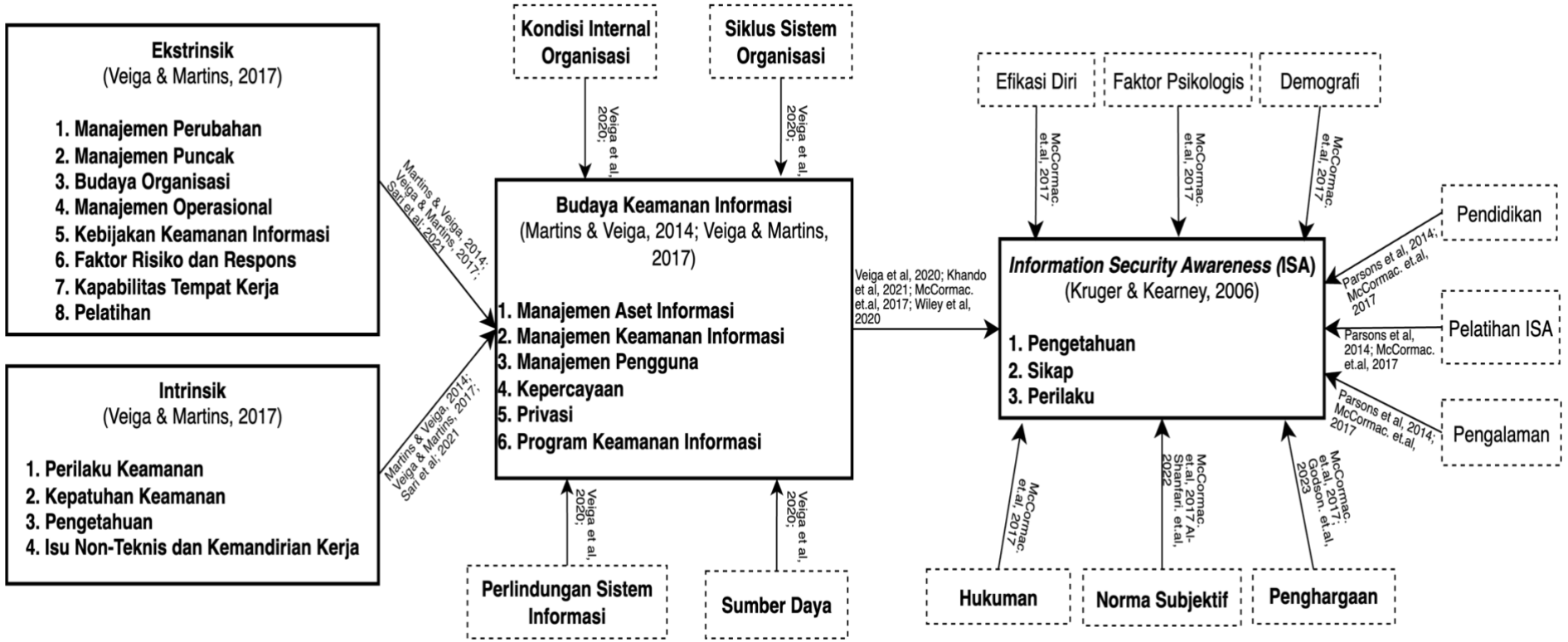
Berdasarkan hasil kajian peneliti, berikut gambaran teori penelitian:

Tabel 2.2 Mapping Teori

Information Security Awareness (*ISA*)	**Budaya Keamanan Informasi**	**Ekstrinsik**	**Intrinsik**
(Kruger & Kearney, 2006) **1. Pengetahuan** **2. Sikap** **3. Perilaku** (M. Siponen, 2001) *1. Organizational* *2. General Public* *3. Socio-Political,* *4. Computer Ethical* *5. Institutional Education* (Ajzen, 1991) *1. Attitude* *2. Subjective norms* *3. Perceived behavioral control*	**(Da Veiga & Martins, 2014)** **1. Manajemen Aset Informasi** **2. Manajemen Keamanan Informasi** 3. Manajemen Perubahan **4. Manajemen Pengguna** 5. Kebijakan Keamanan informasi 6. Kepercayaan **7. Kepemimpinan Keamanan Informasi** 8. Pelatihan dan Kesadaran **9. Privasi** **10. Program Keamanan Informasi** (Schlienger & Teufel, 2002) 1. Politik Perusahaan 2. Manajemen 3. Individu (Van Niekerk & Von Solms, 2006) 1. Kebijakan Keamanan 2. Pendidikan, Pelatihan dan Kesadaran Keamanan	**(da Veiga & Martins, 2017)** **1. Manajemen Perubahan** **2. Manajemen Puncak** **3. Budaya Organisasi** **4. Manajemen Operasional** **5. Kebijakan Keamanan Informasi** **6. Faktor Risiko dan Tindakan** **7. Kemampuan di Tempat Kerja** **8. Pelatihan**	**(da Veiga & Martins, 2017)** 1. **Perilaku Keamanan** 2. **Kepatuhan Keamanan** 3. **Pengetahuan** 4. **Isu Non-Teknis dan Kemandirian Kerja**

	3. Pemantauan Komputer (Alhogail & Mirza, 2015) 1. Strategi 2. Teknologi 3. Organisasi 4. Manusia 5. Lingkungan		

2.9 Kerangka Teori Penelitian



Gambar 2.3 Kerangka Teori Penelitian

Sumber : ISA modifikasi dari *theory of reasoned action* (TRA) (Fishbein & Ajzen, 1977)*, theory of planned behaviour* (TPB) (Ajzen, 1991), *intrinsic motivation* (Deci, 1975)*;* Budaya Kemanan Informasi Modifikasi dari Teori Perilaku Organisasi (Stephen et al., 2003).

Berdasarkan hasil *literature review* yang dilakukan oleh peneliti terhadap beberapa penelitian terdahulu menunjukkan adanya beberapa faktor orgnanisasi yang dapat mempengaruhi *Information Security Awareness* (ISA) di Rumah Sakit diantaranya: penghargaan (Godson et al., 2023; McCormac et al., 2017), hukuman (McCormac et al., 2017), norma subjektif (Al-Shanfari et al., 2022; McCormac et al., 2017) dan budaya keamanan informasi (McCormac et al., 2017; Wiley et al., 2020).

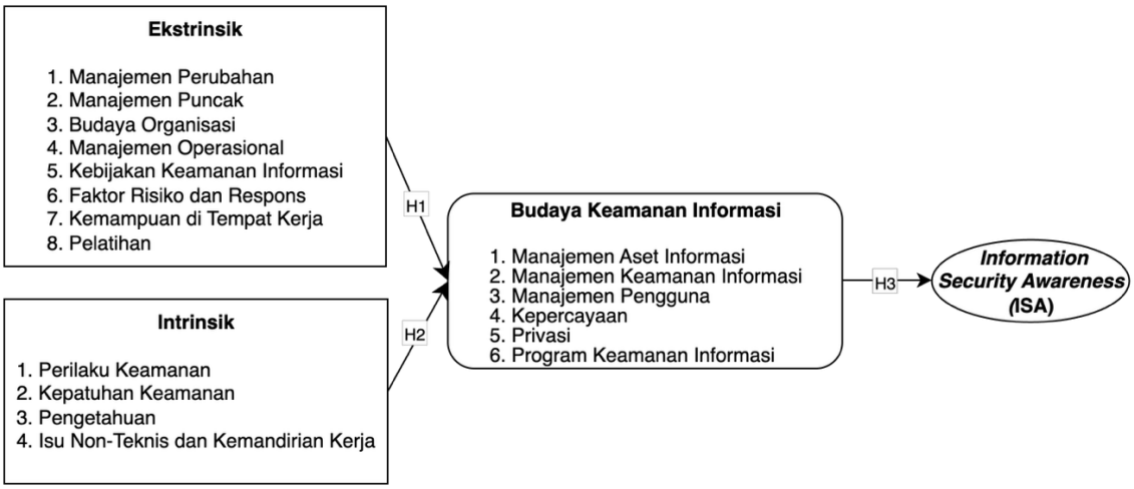
Adanya beberapa faktor organisasi yang mempengaruhi *Information Security Awareness* (ISA) pengguna SIMRS di Rumah Sakit, peneliti memilih menggunakan variabel budaya keamanan informasi untuk mengkaji *Information Security Awareness* (ISA). Hal ini disebabkan karena menurut penelitian sebelumnya menyebutkan bahwa saat ini budaya keamanan informasi merupakan komponen penting yang secara efektif mempromosikan perilaku keamanan dan mengelola risiko keamanan dalam organisasi (Nasir et al., 2019). Faktor utama yang mempengaruhi kesadaran dan niat untuk mematuhi keamanan informasi adalah budaya keamanan Karyawan di organisasi dengan budaya keamanan yang baik cenderung memiliki pengetahuan, sikap, dan perilaku yang sejalan dengan kebijakan serta prosedur keamanan informasi yang diperlukan untuk menjaga keamanan yang efektif (Wiley et al., 2020).

Menurut penelitian sebelumnya, terdapat faktor-faktor yang dapat mempengaruhi budaya keamanan informasi pada layanan kesehatan termasuk Rumah Sakit. Faktor-faktor tersebut diantaranya manajemen perubahan; manajemen puncak; budaya organisasi; manajemen operasional; kebijakan keamanan informasi; faktor risiko dan tindakan; kemampuan di tempat kerja, pelatihan dan kesadaran; perilaku keamanan; kepatuhan keamanan; pengetahuan; serta isu non-teknis dan kemandirian kerja. Faktor-faktor ini dikelompokkan menjadi faktor intrinsik dan ekstrinsik (da Veiga & Martins, 2017; Sari et al., 2021). Kedua faktor tersebut dapat mewakili beberapa faktor lain yang mempengaruhi budaya keamanan informasi.

Hasil penelitian ini diharapkan dapat memberikan kontribusi yang signifikan bagi RSUD Haji Makassar dalam meningkatkan keamanan informasi dan melindungi data pasien. Selain itu, temuan-temuan dalam penelitian ini juga diharapkan dapat menjadi referensi bagi rumah sakit lain dalam mengembangkan program peningkatan ISA yang efektif. Dengan demikian, penelitian ini tidak hanya

bertujuan untuk menyelesaikan masalah yang dihadapi oleh RSUD Makassar, tetapi juga diharapkan dapat memberikan kontribusi bagi pengembangan ilmu pengetahuan di bidang keamanan informasi, khususnya dalam konteks Rumah Sakit.

2.10 Kerangka Konsep



Keterangan :

= Variabel independent

= Variabel intervening

= Variabel dependen

Gambar 2.4 Kerangka Teori Penelitian

2.11 Hipotesis Penelitian

1. Hipotesis Null/Awal (H0)
    a. Faktor ekstrinsik tidak berpengaruh signifikan terhadap budaya keamanan informasi pada pengguna SIMRS di RSUD Haji Makassar.
    b. Faktor intrinsik tidak berpengaruh signifikan terhadap budaya keamanan informasi pada pengguna SIMRS di RSUD Haji Makassar.
    c. Budaya keamanan informasi tidak berpengaruh signifikan terhadap *Information Security Awareness* (ISA) pada pengguna SIMRS di RSUD Haji Makassar.
2. Hipotesis Alternatif (Ha)
    a. Faktor ekstrinsik berpengaruh signifikan terhadap budaya keamanan informasi pada pengguna SIMRS di RSUD Haji Makassar.
    b. Faktor intrinsik berpengaruh signifikan terhadap budaya keamanan informasi pada pengguna SIMRS di RSUD Haji Makassar.
    c. Budaya keamanan informasi berpengaruh signifikan terhadap *Information Security Awareness* (ISA) pada pengguna SIMRS di RSUD Haji Makassar.

2.12 Definisi Operasional dan Kriteria Objektif

Tabel 2.3 Definisi Operasional

No.	Variabel	Definisi Teori	Definisi Operasional	Alat dan Cara Pengukuran	Kriteria Objektif	Skala
1	Ekstrinsik	Faktor-faktor eksternal dari individu/staf yang dapat mempengaruhi budaya keamanan informasi organisasi (da Veiga & Martins, 2017)	Persepsi individu terhadap faktor eksternal di lingkungan kerja rumah sakit, melalui dukungan manajemen, pelatihan serta adanya kebijakan keamanan informasi dengan indikator: 1. Manajemen Perubahan Penilaian terhadap persepsi pengguna mengenai kemampuan dan kesiapan organisasi serta karyawan dalam melakukan perubahan cara kerja, seperti penggantian kata sandi, cadangan data, dan peningkatan keamanan informasi, guna melindungi informasi penting. 2. Manajemen Puncak Penilaian terhadap persepsi pengguna mengenai komitmen, pandangan penting, dan penjelasan pimpinan RS kepada karyawan terkait keamanan informasi sebagai bentuk dukungan terhadap pelaksanaan perlindungan data.	Kuesioner sebanyak 24 pertanyaan dengan pilhan jawaban: 4 = Sangat Setuju 3 = Setuju 2 = Tidak Setuju 1 = Sangat Tidak Setuju	Skor tertinggi = (24x4) = 96 Skor terendah = (24x1) = 24 Skor standar = 96-24 = 72 Interval Skor = 72/2 = 36 Skor = 96-36 = 60 Kriteria Objektif: Baik: Jika skor total jawaban dari responden >60 Kurang Baik: Jika skor total jawaban dari responden ≤60	Likert

			3. Budaya Organisasi Penilaian terhadap persepsi pengguna mengenai pengetahuan, keterampilan, dan keseriusan karyawan dalam menjaga dan melindungi keamanan informasi di lingkungan organisasi. 4. Manajemen Operasional Penilaian terhadap persepsi pengguna mengenai upaya rumah sakit dalam menjaga keamanan informasi melalui peninjauan sistem informasi, audit eksternal/internal, dan pengaturan kontrak pihak ketiga yang mencakup aspek keamanan informasi. 5. Kebijakan Keamanan Informasi Penilaian terhadap persepsi pengguna mengenai kemampuan kebijakan keamanan informasi yang diterapkan, dipahami, dan praktis, sehingga mendukung pelaksanaan perlindungan data dalam aktivitas sehari-hari di rumah sakit. 6. Faktor Risiko dan Tindakan Penilaian terhadap persepsi pengguna mengenai langkah rumah sakit dalam melakukan analisis risiko, mengurangi			

No.	Variabel	Definisi Teori	Definisi Operasional	Alat dan Cara Pengukuran	Kriteria Objektif	Skala
			risiko, dan memberikan informasi aturan dan sanksi kepada karyawan untuk mendukung keamanan informasi. 7. Kemampuan di Tempat Kerja Penilaian terhadap persepsi pengguna mengenai kebijakan dan tindakan di tempat kerja yang mencakup perjanjian kerahasiaan, hukuman pelanggaran, dan pemeriksaan rutin sistem untuk menjaga keamanan informasi. 8. Pelatihan Penilaian terhadap persepsi pengguna mengenai kebutuhan, pentingnya, dan manfaat pelatihan atau kampanye untuk menjaga informasi dan mengenali ancaman keamanan informasi.			
2	Intrinsik	Faktor-faktor yang berasal dari dalam individu, seperti kepribadian dan pengalaman pribadi yang	Persepsi individu terhadap faktor internal pada diri individu lain di lingkungan kerja rumah sakit melalui tingkat pengetahuan, kepatuhan, perilaku dan isu-isu keamanan informasi dengan indikator :	Kuesioner sebanyak 12 pertanyaan dengan pilhan jawaban: 4 = Sangat Setuju 3 = Setuju 2 = Tidak Setuju	Skor tertinggi = (12x4) = 48 Skor terendah = (12x1) = 12 Skor standar = 47-12 = 35 Interval Skor = 35/2 = 18 Skor = 48-18 = 30 Kriteria Objektif: Baik: Jika skor total jawaban	Likert

No.	Variabel	Definisi Teori	Definisi Operasional	Alat dan Cara Pengukuran	Kriteria Objektif	Skala
		dapat memengaruhi cara seseorang memandang keamanan informasi (da Veiga & Martins, 2017)	1. Perilaku Keamanan Informasi Penilaian pengguna mengenai kepatuhan dan kehati-hatian lingkungan kerja dalam menjaga informasi, memeriksa keamanan, dan mempertimbangkan dampak negatif sebelum melakukan tindakan yang berkaitan dengan keamanan data dan media sosial. 2. Kepatuhan terhadap Kebijakan Keamanan Penilaian pengguna mengenai kepatuhan lingkungan kerja terhadap arahan, aturan, dan tanggung jawab dalam menjaga keamanan informasi berdasarkan kebijakan yang ditetapkan organisasi atau rumah sakit. 3. Pengetahuan Penilaian pengguna mengenai pemahaman lingkungan kerja tentang informasi pribadi, risiko dan dampak, serta tanggung jawab terkait keamanan informasi di lingkungan organisasi.	1 = Sangat Tidak Setuju	dari responden >30 Kurang Baik: Jika skor total jawaban dari responden ≤30	

No.	Variabel	Definisi Teori	Definisi Operasional	Alat dan Cara Pengukuran	Kriteria Objektif	Skala
			4. Isu Non-Teknis dan Kemandirian Kerja Penilaian pengguna mengenai kesadaran dan kemandirian karyawan dalam menyadari dampak, menggunakan antivirus, dan merespons gangguan luar yang memengaruhi cara pandang terhadap keamanan informasi.			
3	Budaya Keamanan Informasi	Sikap, nilai, dan perilaku individu dalam menangani risiko keamanan informasi (Prasetyo et al., 2023).	Persepsi pegawai tentang manajerial dalam melindungi informasi organisasi dengan indikator : 1. Manajemen Aset Informasi Penilaian terhadap persepsi pengguna mengenai penyalahan informasi terhadap aset di unit kerja. 2. Manajemen Keamanan Informasi Penilaian terhadap persepsi pengguna pentingnya pemantauan kepatuhan kebijakan keamanan informasi 3. Manajemen Pengguna Penilaian terhadap kesadaran pengguna mengenai fungsi pekerjaannya dalam penggunaan SIMRS.	Kuesioner sebanyak 6 pertanyaan dengan pilhan jawaban: 4 = Sangat Setuju 3 = Setuju 2 = Tidak Setuju 1 = Sangat Tidak Setuju	Skor tertinggi = (6x4) = 24 Skor terendah = (6x1) = 6 Skor standar = 24-6 = 18 Interval Skor = 18/2 = 9 Skor = 24-9 = 15 Kriteria Objektif: Baik: Jika skor total jawaban dari responden >15 Kurang Baik: Jika skor total jawaban dari responden ≤15	Likert

No.	Variabel	Definisi Teori	Definisi Operasional	Alat dan Cara Pengukuran	Kriteria Objektif	Skala
			4. Kepercayaan Penilaian terhadap persepsi pengguna mengenai keamanan kerahasiaan informasi pribadi. 5. Privasi Penilaian terhadap persepsi pengguna mengenai arahan perlindungan informasi. 6. Program Keamanan Informasi Penilaian terhadap persepsi pengguna mengenai pentingya keterlibatan semua orang terhadap keamanan informasi			
4	*Information Security Awareness (*ISA)	Pemahaman pegawai dalam perilaku keamanan informasi yang aman terhadap kebijakan, aturan, dan pedoman keamanan informasi organisasi (K. Parsons et al., 2017)	Persepsi pegawai mengenai sejauh mana individu memahami, menyikapi, dan berperilaku sesuai dengan kebijakan, aturan, dan pedoman keamanan informasi yang berlaku dalam organisasi dengan indikator : 1. Pengetahuan Persepsi responden mengenai tindakan-tindakan yang dapat menimbulkan risiko keamanan data seperti mengakses situs web, adanya peringatan dan membuka email yang tidak dikenali. 2. Sikap Persepsi responden tentang keamanan informasi, seperti	Kuesioner sebanyak 9 pertanyaan dengan pilhan jawaban: 4 = Sangat Setuju 3 = Setuju 2 = Tidak Setuju 1 = Sangat Tidak Setuju	Skor tertinggi = (9x4) = 36 Skor terendah = (9x1) = 9 Skor standar = 36-9 = 27 Interval skor = 27/2 = 13 Skor = 36–13 = 23 Kriteria Objektif: Tinggi: Jika skor total jawaban dari responden >23 Rendah: Jika skor total jawaban dari responden ≤23	Likert

No.	Variabel	Definisi Teori	Definisi Operasional	Alat dan Cara Pengukuran	Kriteria Objektif	Skala
			keyakinan tidak bisa menjadi korban serangan siber saat menggunakan SIMRS, pentingnya membaca email peringatan keamanan data, dan anggapan tidak ada hal buruk jika membuka tautan dari pengirim tidak dikenal. 3. Perilaku Persepsi responden yang mencerminkan kebiasaan dalam penggunaan komputer RS untuk akses situs pribadi, membaca peringatan keamanan, serta membuka tautan email dari pengirim tidak dikenal yang berpotensi memengaruhi keamanan informasi.			