BAB I
PENDAHULUAN

1.1 Latar Belakang

Kesadaran terhadap keamanan informasi (*Information Security Awareness*) di era digital sangat penting, terutama dalam konteks organisasi seperti rumah sakit. Dalam lingkungan rumah sakit, data pasien merupakan salah satu aset yang paling sensitif dan harus dijaga kerahasiaannya. Kesadaran akan keamanan informasi di kalangan staf rumah sakit dapat mengurangi risiko insiden keamanan yang dapat merugikan pasien dan organisasi itu sendiri. Penelitian menunjukkan bahwa tingkat kesadaran yang rendah dapat menyebabkan banyaknya insiden keamanan informasi, yang berpotensi mengancam integritas dan kerahasiaan data pasien (Dafid & Dorie, 2020).

Data pasien tidak hanya mencakup informasi medis, tetapi juga data pribadi yang sangat sensitif. Oleh karena itu, pengelolaan data dan informasi di rumah sakit harus dilakukan dengan sangat hati-hati. Sistem Informasi Manajemen Rumah Sakit (SIMRS) berperan penting dalam pengelolaan data pasien, dan pentingnya pengelolaan ini semakin meningkat seiring dengan kemajuan teknologi informasi (Putu et al., 2024).

Dengan demikian, rumah sakit perlu mengembangkan kebijakan dan prosedur yang jelas untuk melindungi data pasien dari ancaman yang mungkin timbul. Selain itu, kesadaran akan keamanan informasi juga berkontribusi pada reputasi dan kepercayaan pasien terhadap rumah sakit. Penelitian menunjukkan bahwa reputasi dan kepercayaan pelanggan adalah faktor penting dalam penilaian risiko keamanan informasi di rumah sakit (Matondang et al., 2018). Ketika pasien merasa bahwa data mereka aman, mereka lebih cenderung untuk mempercayai layanan yang diberikan oleh rumah sakit. Oleh karena itu, pelatihan dan pendidikan tentang keamanan informasi bagi staf rumah sakit sangat penting untuk memastikan bahwa mereka memahami pentingnya menjaga kerahasiaan data pasien dan dapat mengenali potensi ancaman terhadap keamanan informasi (Novianto et al., 2023).

Rumah sakit sebagai institusi kesehatan sangat rentan terhadap berbagai ancaman keamanan informasi, termasuk serangan siber, pencurian data, dan kesalahan manusia. Ancaman ini semakin meningkat seiring dengan adopsi teknologi informasi yang lebih luas dalam pengelolaan data pasien dan sistem informasi rumah sakit. Penggunaan SIMRS yang mengintegrasikan berbagai fungsi operasional rumah sakit, mulai dari administrasi hingga pelayanan medis, menjadikan data pasien sangat berharga dan sekaligus menjadi target utama bagi pelaku kejahatan siber (Fitri et al., 2022; Pharmaheru et al., 2023).

siber terhadap rumah sakit dapat beragam, mulai dari *ransomware* akses ke data penting hingga serangan yang bertujuan untuk si pribadi pasien. Menurut penelitian, sektor kesehatan merupakan r yang paling sering diserang, dengan kerentanan yang diakibatkan pengelolaan risiko keamanan informasi yang memadai (Budi et al., , 2022). Selain itu, kesalahan manusia, seperti kelalaian dalam

pengelolaan data atau penggunaan kata sandi yang lemah, juga dapat membuka celah bagi serangan siber (Kusmiranti et al., 2022; Septian & Novaria Kunang, 2024). Untuk itu, sangat penting untuk membangun budaya keamanan informasi yang kuat di dalam organisasi.

Budaya keamanan informasi mencakup nilai-nilai dan norma yang dianut oleh organisasi dalam mengelola dan melindungi informasi. Sebuah studi menunjukkan bahwa budaya organisasi yang mendukung keamanan informasi dapat meningkatkan efektivitas sistem keamanan yang diterapkan, seperti ISO 27001, yang merupakan standar internasional untuk manajemen keamanan informasi (Aurabillah et al., 2024; Pulungan et al., 2023). Dalam hal ini, pelatihan dan pendidikan karyawan berperan penting sebagai faktor kunci untuk memperkuat budaya keamanan. Karyawan yang terlatih dengan baik cenderung lebih peka terhadap potensi risiko dan lebih mampu menerapkan praktik keamanan yang tepat (Akhsan & Pendrian, 2024; Nurillah & Trihandoyo, 2024).

Budaya Keamanan Informasi (ISC) yang baik sangat penting untuk melindungi aset informasi organisasi dan memastikan kepatuhan terhadap kebijakan keamanan. ISC merupakan komponen integratif dari budaya organisasi yang melibatkan pengetahuan kolektif, persepsi, keyakinan, dan sikap karyawan terhadap keamanan informasi. Pembentukan ISC dipengaruhi oleh faktor eksternal dan internal, termasuk peran manajemen, perilaku karyawan, dan kebijakan organisasi. Manajemen puncak memiliki peran penting dalam menciptakan dan mempertahankan ISC dengan menetapkan strategi, kebijakan, serta alokasi sumber daya untuk keamanan informasi (Đukić & Vuletić, 2022; Nasir et al., 2022). Kepemimpinan harus secara aktif mendukung dan melaksanakan program untuk meningkatkan tingkat ISC, memastikan keselarasan dengan tujuan organisasi (Đukić & Vuletić, 2022).

Selain itu, pelatihan kesadaran secara teratur sangat penting untuk menanamkan norma-norma etika dan perilaku yang menjaga privasi di kalangan karyawan. Program pelatihan ini harus fokus pada peningkatan pemahaman karyawan mengenai kebijakan keamanan serta keyakinan dan etika pribadi mereka yang berkaitan dengan keamanan informasi (Mikuletič et al., 2024). Oleh karena itu, pelatihan yang berkesinambungan akan memperkuat kesadaran karyawan terhadap risiko dan meningkatkan kemampuan mereka dalam mengidentifikasi potensi ancaman terhadap keamanan informasi.

Sebuah model ISC yang komprehensif harus mencakup dimensi yang memandu perilaku karyawan untuk mematuhi kebijakan keamanan informasi (Nasir et al., 2020). Kebijakan tersebut harus jelas, mudah diakses, dan diperbarui secara berkala untuk mencerminkan perubahan dalam lanskap keamanan yang terus
asir et al., 2022). ISC juga dipengaruhi oleh budaya sosial dan
ebih luas, serta perkembangan ekonomi dan teknologi di negara
& Vuletić, 2022). Oleh karena itu, norma sosial dan nilai-nilai
dimanfaatkan untuk memperkuat ISC dan mempromosikan perilaku
i pada keamanan (Mikuletič et al., 2024).
trinsik memainkan peran penting dalam membentuk budaya
masi di suatu organisasi. Budaya keamanan informasi dapat

dipahami sebagai sikap dan perilaku kolektif yang mendukung praktik keamanan dalam pengelolaan informasi. Penelitian menunjukkan bahwa motivasi intrinsik, seperti keinginan untuk berprestasi dan tanggung jawab, dapat mendorong individu untuk lebih memperhatikan keamanan informasi (Triono et al., 2021). Dalam konteks ini, individu yang memiliki motivasi intrinsik yang kuat cenderung lebih proaktif dalam menjaga dan melindungi data, yang pada gilirannya memperkuat budaya keamanan informasi di organisasi tersebut (Ghiffari & Purba, 2021).

Faktor ekstrinsik juga memiliki pengaruh yang signifikan terhadap budaya keamanan informasi dalam suatu organisasi. Faktor-faktor ini mencakup elemen-elemen eksternal yang dapat memengaruhi perilaku dan sikap individu terhadap keamanan informasi, seperti kebijakan organisasi, pelatihan, insentif, dan lingkungan kerja. Penelitian menunjukkan bahwa kebijakan keamanan informasi yang jelas dan tegas dapat menciptakan budaya yang mendukung kepatuhan terhadap praktik keamanan (Maya Safitri et al., 2020; Triono et al., 2021). Ketika organisasi menetapkan kebijakan yang kuat dan memberikan dukungan yang memadai, karyawan cenderung lebih memahami pentingnya menjaga keamanan informasi dan berperilaku sesuai dengan kebijakan tersebut.

Selain faktor intrinsik dan ekstrinsik, pengembangan budaya keamanan informasi yang efektif juga melibatkan faktor-faktor penting seperti kesadaran, pengaruh budaya, budaya organisasi, serta program pendidikan dan pelatihan. Faktor-faktor ini membentuk bagaimana karyawan berinteraksi dengan kebijakan dan praktik keamanan informasi. Salah satu faktor tersebut adalah pengaruh budaya, di mana budaya nasional dan organisasi mempengaruhi keputusan individu dalam keamanan siber. Menyesuaikan pelatihan dengan konteks budaya dapat mengurangi risiko serangan rekayasa sosial (Collier et al., 2023). Budaya organisasi yang menekankan nilai etis dan moral dapat meningkatkan kepatuhan terhadap kebijakan keamanan (Ejigu et al., 2024), serta memperkuat niat karyawan untuk mematuhi kebijakan keamanan informasi (Handri et al., 2024).

Selain itu, program pendidikan, pelatihan, dan kesadaran juga memainkan peran kunci dalam membentuk budaya keamanan siber. Program SETA (*Security Education, Training, and Awareness*) yang efektif harus disesuaikan dengan kebutuhan industri serta konteks budaya organisasi agar dapat berjalan dengan optimal (Heyasat et al., 2023). Pendekatan yang komprehensif terhadap pendidikan dan pelatihan dapat membantu organisasi menghadapi ancaman siber dengan lebih baik (Handri et al., 2024).

Selain faktor budaya, integrasi teknologi juga berperan penting dalam pengembangan budaya keamanan informasi. Meskipun teknologi mempermudah operasional organisasi, teknologi juga meningkatkan kerentanannya terhadap [illegible] karena itu, budaya keamanan informasi yang kuat harus mencakup keamanan yang efektif serta pelatihan yang memastikan karyawan mengimplementasikan protokol yang ada. Teknologi tidak hanya [illegible]ijakan keamanan, tetapi juga memfasilitasi pemantauan dan [illegible]dap standar keamanan (Prasetyo & Setiawan, 2022).

[illegible] ini berfokus pada faktor intrinsik dan ekstrinsik dalam membentuk [illegible]an informasi karena kedua faktor ini sangat relevan dalam konteks

manajemen dan administrasi rumah sakit. Dalam manajemen rumah sakit, keberhasilan implementasi kebijakan keamanan informasi sangat bergantung pada sikap dan perilaku karyawan, yang dipengaruhi oleh faktor intrinsik dan ekstrinsik dalam menciptakan lingkungan yang mendukung kepatuhan terhadap protokol keamanan. Meskipun faktor-faktor lainnya juga penting, namun banyaknya serangan siber di rumah sakit yang disebabkan oleh kelalaian manusia, seperti penggunaan kata sandi yang lemah atau kurangnya pelatihan, menunjukkan bahwa dalam konteks manajemen dan administrasi rumah sakit, faktor manusia, baik intrinsik maupun ekstrinsik, merupakan elemen utama dalam membangun budaya keamanan informasi yang efektif. Keberhasilan dalam mengelola risiko keamanan informasi di rumah sakit memerlukan integrasi antara kepemimpinan yang mendukung, kebijakan yang jelas, dan pelatihan berkelanjutan bagi karyawan untuk memastikan perlindungan data yang optimal.

Selanjutnya, budaya keamanan informasi memiliki pengaruh yang signifikan terhadap kesadaran keamanan informasi (*Information Security Awareness*, ISA) di dalam organisasi. Budaya ini mencakup nilai-nilai, norma, dan praktik yang mendukung perilaku yang aman dalam pengelolaan informasi. Penelitian menunjukkan bahwa individu yang berada dalam lingkungan dengan budaya keamanan informasi yang kuat cenderung memiliki tingkat kesadaran yang lebih tinggi terhadap pentingnya keamanan informasi (Prasetyo et al., 2023a). Hal ini disebabkan oleh pengaruh positif dari pengetahuan dan kepatuhan terhadap kebijakan keamanan yang ada, yang pada gilirannya meningkatkan perilaku individu dalam menjaga keamanan informasi (Md Azmi et al., 2021).

Information Security Awareness (ISA) adalah konsep yang sangat penting dalam menjaga keamanan informasi di sektor kesehatan, terutama di rumah sakit. ISA mencakup pemahaman dan kesadaran individu terhadap risiko yang terkait dengan keamanan informasi serta praktik terbaik untuk melindungi data sensitif, termasuk data pasien. Dalam konteks rumah sakit, di mana data kesehatan sangat berharga dan sering menjadi target serangan siber, penerapan ISA sangat penting untuk mencegah pelanggaran data dan menjaga kepercayaan pasien (Nifakos et al., 2021; Priestman et al., 2019).

Pentingnya ISA tidak dapat dianggap sepele, terutama mengingat meningkatnya ancaman siber yang dihadapi oleh institusi kesehatan. Rumah sakit sering kali menjadi sasaran serangan karena mereka menyimpan informasi pribadi yang sensitif, termasuk riwayat medis dan data keuangan pasien. Penelitian menunjukkan bahwa serangan siber terhadap rumah sakit dapat mengakibatkan kerugian finansial yang signifikan, serta dampak reputasi yang merugikan (Landolt et al., 2012; Mocydlarz-Adamcewicz et al., 2023). Dengan meningkatkan kesadaran
masi di kalangan staf, rumah sakit dapat mengurangi risiko
sia, yang merupakan salah satu penyebab utama pelanggaran data
).
erperan dalam memastikan bahwa semua anggota staf memahami
rosedur keamanan yang ada. Hal ini termasuk pelatihan tentang
ta sandi yang kuat, pengenalan terhadap *phishing*, dan cara
den keamanan. Dengan pengetahuan yang memadai, staf dapat

lebih siap untuk mengenali dan merespons potensi ancaman, sehingga mengurangi kemungkinan terjadinya pelanggaran data (Yuan & Li, 2019). Selain itu, ISA dapat membantu menciptakan budaya keamanan di dalam organisasi, di mana setiap individu merasa bertanggung jawab untuk melindungi informasi yang mereka kelola (Collier et al., 2023). Implementasi ISA yang efektif juga dapat mendukung kepatuhan terhadap regulasi perlindungan data, seperti *General Data Protection Regulation* (GDPR) di Eropa, yang mengharuskan institusi kesehatan untuk melindungi data pribadi pasien dengan ketat (Yuan & Li, 2019)).

Menurut Viega dan Martins (2017) faktor-faktor yang mempengaruhi budaya kesadaran keamanan informasi ini dibagi menjadi dua kategori utama: faktor intrinsik dan ekstrinsik. Faktor intrinsik mencakup elemen yang berasal dari dalam individu, seperti perilaku keamanan, kepatuhan terhadap kebijakan, dan norma sosial yang mempengaruhi cara karyawan berinteraksi dengan kebijakan keamanan informasi. Di sisi lain, faktor ekstrinsik meliputi elemen yang berasal dari lingkungan luar individu, seperti manajemen, kebijakan keamanan informasi, kemampuan tempat kerja, serta budaya nasional dan organisasi. Manajemen berperan penting dalam membentuk budaya keamanan dengan menetapkan visi dan strategi, sementara kebijakan yang jelas dan pelatihan yang efektif dapat meningkatkan kesadaran dan kepatuhan karyawan terhadap praktik keamanan. Kedua faktor ini saling berinteraksi dan berkontribusi pada pembentukan budaya keamanan informasi yang kuat dalam organisasi (Veiga & Martins, 2017).

Berdasarkan pengumpulan data primer terhadap 30 responden pengguna sistem informasi manajemen rumah sakit di RS Stella Maris Makassar, diketahui bahwa masalah utama yang dihadapi adalah rendahnya *Information Security Awareness* (ISA) di kalangan karyawan. Hal ini terlihat dari tingginya persentase responden yang belum pernah mengikuti pelatihan atau seminar terkait ancaman siber. Sebanyak 93,3% responden tidak pernah mengikuti pelatihan atau seminar tentang rekayasa sosial, dan 80% tidak pernah mengikuti pelatihan keamanan siber, padahal keduanya merupakan aspek penting dalam perlindungan sistem informasi rumah sakit. Selain itu, 66,7% responden tidak pernah mengganti kata sandi akun profesional, dan 36,7% tidak pernah melaporkan insiden keamanan yang mencurigakan, yang menunjukkan lemahnya kesadaran serta tindakan pencegahan terhadap potensi ancaman digital. Kondisi ini diperparah oleh minimnya pemahaman terhadap kebijakan keamanan serta risiko penggunaan perangkat pribadi yang tidak aman dalam lingkungan kerja. Rendahnya tingkat kesadaran dan kewaspadaan ini berpotensi menimbulkan risiko besar terhadap keamanan data pasien serta integritas sistem informasi di RS Stella Maris.

endahnya kesadaran terhadap keamanan informasi (*Information* *ness* atau ISA) di RS Stella Maris Makassar menjadi perhatian saat ini ketergantungan terhadap sistem digital meningkat. Salah alah insiden serangan *malware* yang terjadi pada sistem INACBGs adian ini menunjukkan bahwa sistem informasi belum sepenuhnya

terlindungi, dan kemungkinan besar disebabkan oleh kurangnya kesadaran serta pemahaman staf terhadap keamanan siber.

Berdasarkan data primer tahun 2024, sebagian besar responden belum pernah mendapatkan pelatihan atau seminar terkait ancaman rekayasa sosial, yakni sebanyak 93,3%, padahal jenis serangan ini termasuk yang paling sering terjadi di sektor kesehatan. Selain itu, 80% responden juga belum pernah mengikuti pelatihan keamanan siber, yang seharusnya menjadi bekal penting untuk menghadapi berbagai ancaman digital. Perilaku berisiko lainnya juga cukup menonjol, seperti 66,7% responden yang mengaku tidak pernah mengganti kata sandi akun profesional, sehingga membuka peluang bagi pihak tidak bertanggung jawab untuk mengakses sistem. Lebih lanjut, 36,7% responden tidak pernah melaporkan saat ada kejadian atau insiden keamanan siber yang mencurigakan, padahal pelaporan dini dapat membantu mencegah kerugian yang lebih besar.

Rendahnya kesadaran ini tidak lepas dari beberapa faktor yang memengaruhi, salah satunya adalah faktor organisasi. Dalam konteks organisasi, budaya keamanan informasi berperan penting dalam membentuk perilaku staf terhadap keamanan data. Budaya ini terbagi menjadi faktor intrinsik, yang berasal dari kesadaran individu, dan faktor ekstrinsik, yang terkait dengan aturan dan kebijakan organisasi (Sari et al., 2021). Selain itu, gaya kepemimpinan juga turut memengaruhi tingkat kepatuhan staf terhadap prosedur keamanan informasi (Ali et al., 2021). Kepemimpinan yang mendukung budaya keamanan akan mampu mendorong staf untuk lebih peduli terhadap keamanan data. Faktor lain yang tak kalah penting adalah norma subjektif, yaitu persepsi individu mengenai ekspektasi sosial terhadap keamanan informasi, serta penerapan sistem penghargaan dan hukuman yang efektif untuk meningkatkan motivasi staf (Khando et al., 2021; Chaudhary, 2024; Riahi & Islam, 2024).

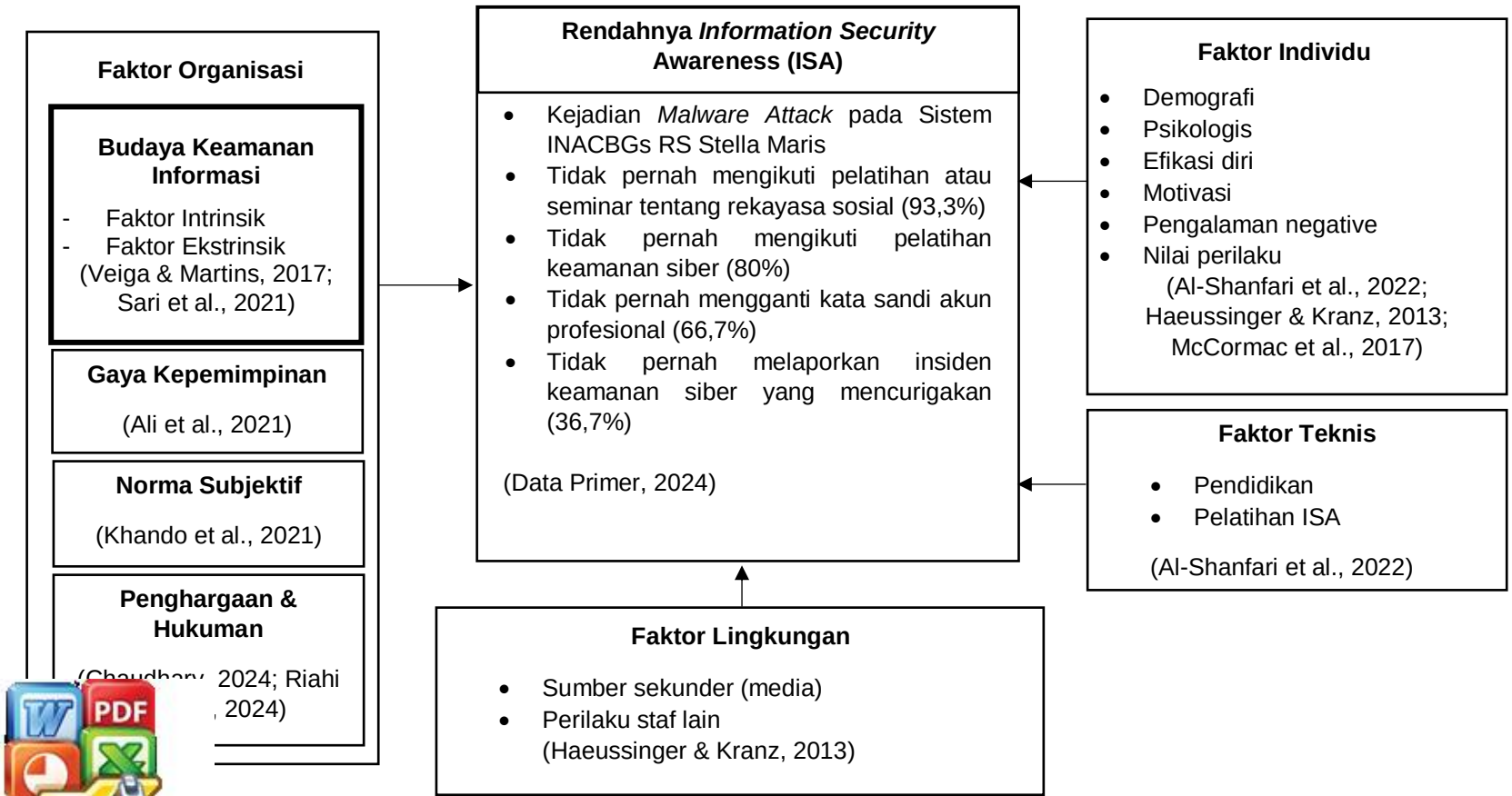
Selain faktor organisasi, faktor individu juga memiliki pengaruh signifikan terhadap ISA. Faktor demografi, seperti usia, tingkat pendidikan, dan pengalaman kerja, dapat memengaruhi kesadaran seseorang terhadap pentingnya keamanan informasi. Di samping itu, aspek psikologis, termasuk efikasi diri, motivasi, dan pengalaman negatif terhadap insiden keamanan sebelumnya, turut membentuk sikap staf dalam menjaga keamanan data (Al-Shanfari et al., 2022; Haeussinger & Kranz, 2013). Nilai perilaku yang dimiliki individu juga menentukan sejauh mana mereka mematuhi aturan yang ada (McCormac et al., 2017)

Faktor lain yang perlu diperhatikan adalah faktor lingkungan, yang mencakup sumber informasi dari media dan perilaku rekan kerja. Media memainkan peran penting dalam memberikan informasi terkini mengenai ancaman keamanan siber, sementara perilaku staf lain dapat memengaruhi tingkat kesadaran individu dalam [illegible]sedur keamanan informasi (Haeussinger & Kranz, 2013).

[illegible]aktor teknis seperti pendidikan dan pelatihan keamanan informasi [illegible]an untuk meningkatkan kesadaran dan keterampilan staf. Pelatihan [illegible]dapat memberikan pemahaman yang lebih baik mengenai prosedur [illegible]ukan ketika menghadapi ancaman keamanan data (Al-Shanfari et [illegible] karena itu, pendekatan yang komprehensif dari berbagai faktor ini [illegible]k meningkatkan *Information Security Awareness* di rumah sakit.

Dengan memperkuat budaya organisasi, memberikan pelatihan yang memadai, serta menanamkan nilai-nilai perilaku positif, diharapkan risiko terhadap keamanan informasi dapat diminimalkan.

Adapun kajian masalah dalam penelitian ini dapat digambarkan sebagai berikut:



gan Kajian Masalah
Primer, 2024

1.3 Rumusan Masalah

Berdasarkan latar belakang dan kajian masalah yang telah diuraikan, rumusan masalah yang muncul adalah:

1. Bagaimana besar pengaruh faktor intrinsik (Pengetahuan, Kepatuhan terhadap Aturan Keamanan, Perilaku Keamanan, Isu Lunak yang Berkaitan dengan Tempat Kerja) terhadap budaya keamanan informasi di Rumah Sakit Stella Maris Makassar?
2. Bagaimana besar pengaruh faktor ekstrinsik (Pelatihan dan Kesadaran, Manajemen Operasional, Budaya Organisasi, Dukungan Manajemen Puncak, Kemampuan di Tempat Kerja, Faktor Risiko dan Tindakan, Manajemen Perubahan, serta Kebijakan Keamanan Informasi) terhadap budaya keamanan informasi di Rumah Sakit Stella Maris Makassar?
3. Bagaimana besar pengaruh budaya keamanan informasi terhadap *Information Security Awareness* (ISA) di Rumah Sakit Stella Maris Makassar?
4. Faktor apakah yang paling berpengaruh terhadap budaya keamanan informasi di Rumah Sakit Stella Maris Makassar?

1.4 Tujuan Penelitian

1.4.1 Tujuan Umum

Untuk menganalisis pengaruh faktor intrinsik dan ekstrinsik terhadap *Information Security Awareness* (ISA) pada staf di Rumah Sakit Stella Maris Makassar.

1.4.2 Tujuan Khusus

1. Menganalisis besar pengaruh antara faktor intrinsik (Pengetahuan, Kepatuhan terhadap Aturan Keamanan, Perilaku Keamanan, Isu Lunak yang Berkaitan dengan Tempat Kerja) terhadap budaya keamanan informasi di Rumah Sakit Stella Maris Makassar.
2. Menganalisis besar pengaruh antara faktor ekstrinsik (Pelatihan dan Kesadaran, Manajemen Operasional, Budaya Organisasi, Dukungan Manajemen Puncak, Kemampuan di Tempat Kerja, Faktor Risiko dan Tindakan, Manajemen Perubahan, serta Kebijakan Keamanan Informasi) terhadap budaya keamanan informasi di Rumah Sakit Stella Maris Makassar.
3. Menganalisis besar pengaruh antara faktor budaya keamanan informasi terhadap *Information Security Awareness* (ISA) di Rumah Sakit Stella Maris Makassar.
4. Menganalisis faktor yang paling berpengaruh terhadap budaya keamanan informasi di Rumah Sakit Stella Maris Makassar.

ian

Ilmiah

mberikan kontribusi terhadap pengembangan teori budaya manan informasi (ISC*)* dan penerapan model *Knowledge–Attitude–avior* (KAB) dalam konteks rumah sakit.

2. Menambah wawasan empiris tentang perilaku tenaga kesehatan terhadap keamanan informasi dan integrasinya dalam sistem manajemen informasi rumah sakit.

1.5.2 Manfaat Praktis

1. Menyediakan rekomendasi praktis bagi Rumah Sakit Stella Maris Makassar untuk meningkatkan kepatuhan dan *Information Security Awareness*, sehingga mengurangi risiko serangan siber.
2. Memberikan dasar untuk merancang program pelatihan dan pendidikan yang efektif bagi staf kesehatan terkait ancaman dan praktik keamanan siber.
3. Mengidentifikasi dan mengurangi kelemahan dalam sistem *Information Security Awareness* yang disebabkan oleh faktor manusia, sehingga mengurangi risiko pelanggaran data dan serangan siber.

1.5.3 Manfaat Bagi Peneliti

1. Memberikan pengalaman berharga dalam melakukan penelitian empiris di lingkungan kesehatan, yang melibatkan analisis data dan pengembangan rekomendasi praktis.
2. Memberikan wawasan yang lebih mendalam tentang tantangan dan solusi dalam penerapan kebijakan keamanan informasi di rumah sakit, yang dapat digunakan untuk memperbaiki praktik keamanan di institusi kesehatan yang serupa.
3. Menyediakan peluang untuk mempublikasikan hasil penelitian di jurnal-jurnal ilmiah dan konferensi, sehingga berkontribusi pada komunitas akademik dan profesional.

BAB II
TINJAUAN PUSTAKA

2.1 Konsep Dasar ISA

2.1.1 Definisi *Information Security Awareness*

Information Security Awareness (ISA) adalah kesadaran dan pemahaman individu atau organisasi terhadap pentingnya keamanan informasi, serta risiko yang terkait dengan ancaman dan kerentanannya. Dalam konteks ini, ISA bertujuan untuk meningkatkan perhatian dan tindakan proaktif untuk melindungi informasi sensitif dari berbagai ancaman, seperti akses tidak sah, kebocoran data, dan serangan siber. ISA berfokus pada perubahan perilaku pengguna dalam mengikuti kebijakan keamanan dan protokol yang diterapkan untuk mengurangi risiko keamanan (Gioulekas et al., 2022).

2.1.2 Komponen utama ISA

ISA terdiri dari tiga komponen utama yang saling terkait, yaitu:

1. Pengetahuan

   Komponen pengetahuan dalam ISA mencakup pemahaman yang mendalam tentang kebijakan, prosedur, dan praktik terbaik dalam menjaga keamanan informasi. Pengetahuan ini mencakup pemahaman mengenai berbagai risiko keamanan, seperti serangan siber, *malware, phishing,* dan berbagai ancaman lainnya. Pemahaman yang baik akan kebijakan internal organisasi, termasuk klasifikasi informasi sensitif dan cara melindunginya, sangat penting. Selain itu, pengetahuan juga meliputi metode yang dapat digunakan untuk mencegah kebocoran data, seperti penggunaan enkripsi, autentikasi multi-faktor, dan pengelolaan kata sandi yang aman. Pengetahuan ini menjadi dasar dalam membentuk perilaku yang aman.

2. Sikap

   Sikap merujuk pada cara pandang individu terhadap keamanan informasi. Sikap yang positif terhadap kebijakan dan prosedur keamanan akan memengaruhi seseorang untuk lebih patuh dan termotivasi dalam menjaga keamanan data. Sikap ini juga terbentuk dari pemahaman terhadap risiko dan konsekuensi dari pelanggaran keamanan informasi. Individu yang memiliki sikap proaktif akan lebih cenderung memperhatikan praktik-praktik yang aman dan merasa bertanggung jawab dalam menjaga informasi sensitif. Sebaliknya, sikap yang acuh tak acuh dapat meningkatkan kerentanan terhadap ancaman keamanan. Oleh karena itu, organisasi perlu memastikan bahwa sikap positif terhadap keamanan informasi terbangun melalui kampanye kesadaran dan edukasi yang berkelanjutan.

u

u merupakan manifestasi nyata dari pengetahuan dan sikap u terhadap keamanan informasi. Perilaku yang diharapkan meliputi

tindakan-tindakan konkret seperti menggunakan kata sandi yang kuat dan unik, tidak membagikan informasi sensitif kepada pihak yang tidak berwenang, serta selalu memperbarui perangkat lunak keamanan secara berkala. Selain itu, perilaku proaktif juga mencakup tindakan untuk segera melaporkan insiden keamanan atau pelanggaran yang terdeteksi, sehingga dapat dilakukan mitigasi lebih awal. Perilaku yang baik dalam hal keamanan informasi akan secara langsung berkontribusi pada perlindungan data organisasi dan meminimalisir risiko terjadinya kebocoran informasi.

2.1.3 Tujuan dan Manfaat ISA di Lingkungan Rumah Sakit

ISA memiliki tujuan penting dalam meningkatkan keamanan informasi di lingkungan rumah sakit, yang sering menangani data pasien yang sangat sensitif. Beberapa tujuan dan manfaat dari penerapan ISA di rumah sakit meliputi:

1) Meningkatkan kepatuhan terhadap peraturan dan standar
   Rumah sakit harus mematuhi berbagai peraturan dan standar terkait keamanan informasi, seperti HIPAA (*Health Insurance Portability and Accountability Act*). ISA membantu memastikan bahwa semua karyawan memahami pentingnya peraturan ini dan bagaimana cara menerapkannya.
2) Melindungi data pasien
   Data pasien adalah informasi yang sangat sensitif dan perlu dijaga kerahasiaannya. Dengan ISA, karyawan lebih sadar akan pentingnya menjaga kerahasiaan dan integritas data pasien, serta mencegah kebocoran atau akses tidak sah.
3) Mengurangi risiko serangan siber
   Peningkatan kesadaran karyawan terhadap ancaman keamanan informasi dapat mengurangi risiko serangan siber, seperti serangan *ransomware* yang dapat mengganggu operasi rumah sakit dan mengancam keselamatan pasien.
4) Meningkatkan tanggapan terhadap insiden keamanan
   ISA juga memastikan bahwa staf memiliki pengetahuan dan keterampilan untuk merespons insiden keamanan dengan cepat dan efektif, meminimalkan dampak dari insiden tersebut terhadap operasi rumah sakit.

Dengan menerapkan program ISA yang kuat, rumah sakit dapat menjaga integritas, kerahasiaan, dan ketersediaan informasi penting yang diperlukan [illegible]nyediakan layanan kesehatan yang aman dan efektif (Blackley et

l Peningkatan ISA

peningkatan kesadaran keamanan informasi (*Information Security* A) menekankan perubahan perilaku yang berkaitan dengan

kesadaran terhadap isu-isu keamanan informasi di tingkat individu, organisasi, dan teknologi. Beberapa model yang digunakan untuk meningkatkan ISA antara lain:

2.3.1 Model KAB (*Knowledge-Attitude-Behaviour*)

Model pengukuran kesadaran keamanan informasi ini berfungsi dengan menghubungkan tiga komponen utama—pengetahuan, sikap, dan perilaku—untuk memberikan gambaran yang komprehensif tentang tingkat kesadaran individu atau organisasi terhadap keamanan informasi. Dalam konteks *Information Security Awareness* (ISA), ketiga elemen ini saling memengaruhi dan berkontribusi terhadap perilaku yang aman dalam mengelola dan melindungi informasi sensitif (Khando et al., 2021).

Pengetahuan mengenai kebijakan, prosedur, dan ancaman keamanan informasi adalah dasar dari model ini. Ketika seseorang memiliki pengetahuan yang cukup tentang risiko keamanan, seperti serangan siber, *phishing*, atau kebocoran data, individu tersebut lebih siap untuk mengenali dan menghadapi ancaman tersebut. Pengetahuan ini juga mencakup pemahaman mengenai regulasi dan standar yang harus diikuti dalam melindungi informasi, seperti yang tertuang dalam kebijakan keamanan informasi organisasi. Seiring meningkatnya pengetahuan, kesadaran individu terhadap pentingnya menjaga data juga meningkat, sehingga mendorong pembentukan sikap yang positif.

Sikap merupakan respon emosional dan mental terhadap pengetahuan yang dimiliki. Sikap yang positif terhadap kebijakan keamanan informasi akan memotivasi individu untuk lebih patuh dan proaktif dalam menerapkan langkah-langkah keamanan. Sebagai contoh, ketika seseorang menyadari betapa seriusnya dampak dari pelanggaran keamanan, mereka akan lebih bersedia mengikuti protokol yang ada. Sikap ini dapat mencakup kesediaan untuk melaporkan insiden keamanan atau menggunakan teknologi seperti enkripsi dan autentikasi multi-faktor sebagai bagian dari kebiasaan sehari-hari. Sikap positif memfasilitasi terciptanya lingkungan kerja yang lebih aman dan terkendali.

Perilaku, yang merupakan cerminan nyata dari pengetahuan dan sikap, menjadi indikator paling nyata dalam pengukuran kesadaran keamanan informasi. Perilaku yang baik dalam hal keamanan informasi meliputi tindakan seperti rutin memperbarui perangkat lunak keamanan, menggunakan kata sandi yang kompleks, serta menghindari klik pada tautan atau lampiran email yang mencurigakan. Perilaku ini merupakan wujud dari kesadaran yang terbentuk melalui pengetahuan dan sikap, dan dapat dilihat melalui kepatuhan individu terhadap kebijakan keamanan yang [illegible]an oleh organisasi.

[illegible]*etwork Theory* (ANT), *Structuration Theory*, dan *Contextualism*

[illegible]odel ini sering digunakan untuk menganalisis perubahan [illegible]an keamanan informasi di berbagai level, baik individu, organisasi, [illegible] teknologi. Model ini cocok diterapkan di organisasi besar dengan [illegible]pemangku kepentingan.

2.3.3 *Gamifikasi*

Metode ini melibatkan penggunaan permainan untuk meningkatkan keterlibatan dan pemahaman karyawan terhadap ancaman keamanan informasi. *Gamifikasi* membantu menyesuaikan konten pelatihan agar lebih relevan dengan kebutuhan pengguna (Schroeder, 2020).

2.3.4 Pendekatan *Konstruktivis*

Dalam pendekatan ini, karyawan berpartisipasi secara aktif dalam membangun kampanye kesadaran keamanan informasi, sehingga mereka lebih terlibat dan peduli terhadap isu keamanan (Schroeder, 2020).

2.3.5 *Plan-Do-Check-Act* (PDCA)

Model siklus manajemen ini digunakan untuk merencanakan, melaksanakan, mengevaluasi, dan memperbaiki program kesadaran keamanan informasi secara berkelanjutan.

2.3.6 Pendeteksian Pelanggaran (*Violation Detection*)

Metode ini melibatkan deteksi pelanggaran terhadap kebijakan keamanan informasi yang kemudian digunakan sebagai bahan untuk kampanye kesadaran.

Secara keseluruhan, teori dan model ini berfungsi untuk menciptakan konten dan program ISA yang efektif guna mengubah perilaku karyawan agar sesuai dengan kepatuhan terhadap kebijakan keamanan informasi.

2.3 Faktor-Faktor yang Mempengaruhi ISA

Information Security Awareness (ISA) adalah pemahaman dan kesadaran individu terhadap risiko dan tindakan yang harus dilakukan untuk melindungi informasi sensitif. Faktor-faktor yang memengaruhi ISA dapat dikelompokkan menjadi dua kategori utama yakni faktor intrinsik dan ekstrinsik (Influence et al., 2024).

2.3.1 Faktor Intrinsik

Faktor intrinsik berkaitan dengan karakteristik individu yang memengaruhi tingkat kesadaran keamanan informasi, termasuk pengetahuan, kepatuhan, perilaku, dan isu psikologis.

1) Pengetahuan (*Knowledge*)

Faktor intrinsik berupa pengetahuan memiliki peran sentral dalam membentuk *Information Security Awareness* (ISA) di dalam organisasi. Pengetahuan, yang didefinisikan sebagai pemahaman dan informasi yang dimiliki individu terkait praktik keamanan informasi, secara langsung memengaruhi tingkat kesadaran dan kepatuhan mereka terhadap kebijakan keamanan. Penelitian menunjukkan bahwa program kesadaran keamanan informasi yang efektif dirancang untuk meningkatkan pengetahuan, keterampilan, dan panduan bagi karyawan, sangat penting dalam melindungi aset informasi (Yunita & Deden Nurdeni, 2023). Program semacam ini tidak hanya bertujuan untuk lidik karyawan tentang ancaman keamanan, tetapi juga untuk namkan budaya kepatuhan terhadap keamanan dalam organisasi ningsih et al., 2019).

Hubungan antara pengetahuan dan ISA juga diperkuat oleh temuan Almindeel dan Martins, yang mengungkapkan bahwa pengetahuan dan aspek perilaku karyawan meningkat secara signifikan setelah mengikuti program *e-learning* tentang keamanan informasi. Namun, mereka juga mencatat bahwa retensi pengetahuan ini menurun seiring waktu, menyoroti perlunya inisiatif pelatihan yang berkelanjutan untuk menjaga tingkat kesadaran (AlMindeel & Martins, 2021). Hal ini sejalan dengan pengamatan Prasetyo, yang menegaskan bahwa tingkat pengetahuan yang tinggi tentang keamanan informasi berkorelasi dengan kepatuhan dan perilaku yang lebih kuat di antara individu (Prasetyo et al., 2023b). Sifat siklus dari akuisisi pengetahuan dan dampaknya terhadap ISA menunjukkan bahwa organisasi harus memprioritaskan pendidikan dan pelatihan berkelanjutan untuk mempertahankan tenaga kerja yang berpengetahuan.

Selain itu, pentingnya mengintegrasikan pendidikan keamanan informasi ke dalam kurikulum yang lebih luas ditegaskan oleh Avcı dan Oruç, yang berpendapat bahwa meningkatnya ancaman siber mengharuskan institusi pendidikan untuk memperluas fokus pada keamanan informasi di luar mata pelajaran TI tradisional (Avcı & Oruç, 2020). Pendekatan proaktif terhadap pendidikan ini dapat secara signifikan meningkatkan kesadaran dan kesiapan siswa terhadap ancaman siber potensial. Shillair et al. juga menekankan bahwa inisiatif pelatihan berbasis bukti di tingkat nasional sangat penting untuk meningkatkan kesadaran dan pengetahuan di kalangan karyawan, yang pada akhirnya akan menghasilkan praktik keamanan yang lebih baik (Shillair, 2022).

Dalam konteks sektor tertentu, Nasir et al. menyajikan model budaya keamanan informasi berbasis dimensi yang menggambarkan bagaimana pengetahuan memengaruhi perilaku keamanan karyawan di institusi pendidikan tinggi (Nasir et al., 2019). Model ini memperkuat gagasan bahwa tenaga kerja yang memiliki informasi yang baik lebih mungkin untuk terlibat dalam perilaku yang sesuai dengan kebijakan keamanan informasi. Selain itu, temuan dari Limna et al. menunjukkan bahwa terdapat hubungan signifikan antara pengetahuan keamanan siber, kesadaran, dan pilihan perilaku pengguna, yang menunjukkan bahwa peningkatan pengetahuan secara langsung memengaruhi perilaku protektif individu (Limna et al., 2023)

2) Kepatuhan terhadap Aturan Keamanan (*Security Compliance*)

Kepatuhan terhadap keamanan adalah faktor intrinsik yang signifikan memengaruhi *Information Security Awareness* (ISA) di dalam organisasi. Kepatuhan keamanan merujuk pada kesesuaian perilaku karyawan terhadap kebijakan dan praktik keamanan informasi yang ditetapkan, yang sangat penting untuk menjaga integritas dan kerahasiaan informasi sensitif. Penelitian menunjukkan bahwa budaya kepatuhan yang kuat merupakan elemen esensial untuk menciptakan

lingkungan yang mendukung kesadaran keamanan informasi (Alotaibi et al., 2019). Perilaku kepatuhan ini dibentuk oleh berbagai faktor, termasuk budaya organisasi, sikap individu, dan persepsi terhadap pentingnya kebijakan keamanan (Alassaf & Alkhalifah, 2021).

Menurut Kang et al., pendidikan memainkan peran penting dalam memperkuat kepatuhan terhadap kebijakan keamanan informasi. Mereka menyatakan bahwa keamanan informasi organisasi merupakan tantangan multidimensi yang membutuhkan tidak hanya kesadaran tetapi juga komitmen terhadap kepatuhan dari seluruh karyawan (Kang et al., 2022). Hal ini sejalan dengan pandangan Alotaibi et al., yang menekankan bahwa pemahaman terhadap tanggung jawab yang tercantum dalam kebijakan keamanan adalah dasar dari kepatuhan. Kepatuhan tidak hanya berarti mengikuti aturan, tetapi juga memahami implikasi dari praktik keamanan terhadap keselamatan organisasi secara keseluruhan (Alotaibi et al., 2019).

Angraini et al. menunjukkan bahwa perilaku dan kebiasaan masa lalu memiliki pengaruh signifikan terhadap kepatuhan terhadap kebijakan keamanan informasi. Kebiasaan yang sudah terbentuk dapat meningkatkan kepatuhan, meskipun sering kali kurang efektif dibandingkan dengan pendekatan proaktif lainnya (Angraini et al., 2021). Oleh karena itu, organisasi perlu berfokus pada pembentukan kebiasaan keamanan yang positif melalui pelatihan berkelanjutan dan penguatan kebijakan keamanan.

Dalam tinjauan sistematis oleh Alassaf dan Alkhalifah, ditemukan bahwa faktor langsung dan tidak langsung, seperti budaya organisasi dan motivasi individu, memainkan peran penting dalam memengaruhi perilaku kepatuhan (Alassaf & Alkhalifah, 2021). Temuan ini menggarisbawahi pentingnya pendekatan yang komprehensif untuk mendukung kepatuhan, termasuk penguatan budaya dan motivasi individu.

Prasetyo menegaskan bahwa perspektif individu terhadap keamanan informasi dipengaruhi oleh kesadaran, pengetahuan, dan perilaku kepatuhan mereka (Prasetyo, 2023). Keterkaitan ini menunjukkan bahwa peningkatan kepatuhan dapat meningkatkan kesadaran, dan sebaliknya. Budiningsih et al. juga mendukung pandangan ini dengan menyatakan bahwa penetapan prosedur dan prinsip keamanan yang jelas sangat penting untuk mendorong kepatuhan di kalangan karyawan, yang pada gilirannya meningkatkan kesadaran mereka terhadap isu-isu keamanan (Budiningsih et al., 2019).

Budaya organisasi memiliki dampak yang signifikan dalam mendorong kepatuhan. Karlsson et al. menemukan bahwa persepsi karyawan terhadap budaya organisasi secara langsung memengaruhi kepatuhan mereka terhadap kebijakan keamanan informasi (Karlsson et al., 2021). Budaya yang mendukung dan memprioritaskan kepatuhan

keamanan dapat memotivasi karyawan untuk mematuhi kebijakan, sehingga meningkatkan ISA secara keseluruhan.

Amankwa et al. juga menyoroti efek gabungan antara faktor organisasi dan perilaku terhadap budaya kepatuhan, menyarankan bahwa pendekatan menyeluruh diperlukan untuk mencapai kepatuhan keamanan yang efektif (Amankwa et al., 2022). Hal ini menunjukkan bahwa organisasi perlu menciptakan lingkungan yang mendukung kepatuhan melalui kebijakan yang jelas, pelatihan yang konsisten, dan penguatan budaya keamanan yang kuat.

3) Perilaku Keamanan (*Security Behaviour*)

Hubungan antara perilaku keamanan dan *Information Security Awareness* (ISA) merupakan bidang kajian penting dalam keamanan informasi. Perilaku keamanan mengacu pada tindakan dan praktik yang diadopsi individu untuk melindungi aset informasi, sedangkan ISA mencakup pengetahuan dan pemahaman individu tentang kebijakan dan ancaman keamanan informasi. Penelitian menunjukkan bahwa kedua elemen ini saling bergantung, di mana peningkatan kesadaran berdampak pada perilaku keamanan yang lebih baik di kalangan karyawan.

Almindeel dan Martins menyoroti bahwa sikap dan niat perilaku karyawan adalah prediktor signifikan dari kepatuhan aktual terhadap kebijakan keamanan informasi. Penelitian mereka menunjukkan pentingnya mendorong sikap positif terhadap praktik keamanan untuk meningkatkan kepatuhan, terutama dalam sektor pemerintahan (AlMindeel & Martins, 2020). Hal ini didukung oleh Yunita, yang mencatat bahwa upaya berkelanjutan untuk meningkatkan kesadaran pengguna sangat penting dalam manajemen keamanan informasi. Program kesadaran dirancang untuk memberikan pengetahuan, keterampilan, dan panduan yang menjadi dasar untuk meningkatkan perilaku keamanan (Yunita, 2023).

Model *Knowledge-Attitude-Behavior* (KAB) sering digunakan dalam literatur untuk memahami hubungan antara pengetahuan, sikap, dan perilaku dalam konteks keamanan informasi. Farah et al. menjelaskan bahwa pengabaian atau kegagalan dalam mematuhi kebijakan keamanan informasi sering kali disebabkan oleh kurangnya pengetahuan atau kesadaran, yang menekankan perlunya intervensi ISA yang terarah (Farah et al., 2022). Model ini menunjukkan bahwa peningkatan pengetahuan individu dapat memperbaiki sikap mereka terhadap keamanan.

Penelitian oleh Prasetyo menunjukkan bahwa perspektif individu dap keamanan informasi dipengaruhi oleh kesadaran, etahuan, kepatuhan, dan perilaku mereka. Kesadaran yang lebih terhadap isu-isu keamanan berhubungan dengan kepatuhan yang baik dan perilaku keamanan yang proaktif (Prasetyo, 2023). Malik slam juga menemukan bahwa kesadaran keamanan informasi

berdampak positif pada kinerja organisasi, menunjukkan bahwa peningkatan kesadaran menghasilkan praktik keamanan yang lebih baik (Malik & Islam, 2019).

Program pelatihan memiliki peran penting dalam membentuk ISA dan perilaku keamanan. Ernita et al. menyatakan bahwa program kesadaran keamanan informasi yang dilakukan secara teratur penting untuk meningkatkan pengetahuan karyawan tentang kebijakan dan prosedur keamanan, yang pada akhirnya memperbaiki perilaku keamanan mereka (Ernita et al., 2022). Alkhazi et al. juga menekankan bahwa metode pelatihan harus tidak hanya meningkatkan pengetahuan tetapi juga memotivasi karyawan untuk mengadopsi kebiasaan keamanan yang positif (Alkhazi et al., 2022). Temuan ini selaras dengan laporan Azmi et al., yang menunjukkan bahwa program pendidikan dan kesadaran keamanan memiliki dampak signifikan terhadap budaya keamanan informasi dalam organisasi (Azmi et al., 2021).

Budaya organisasi memainkan peran penting dalam memengaruhi perilaku keamanan. Koohang et al. menyarankan bahwa membangun budaya kepercayaan dan kolaborasi dapat meningkatkan keterlibatan karyawan dalam praktik keamanan, sehingga memperbaiki kepatuhan dan kesadaran mereka (Koohang et al., 2019). Kovačević et al. juga menyoroti hubungan kuat antara pengetahuan, sikap, dan perilaku dalam membentuk praktik keamanan siber (Kovačević et al., 2020).

4) Isu Lunak yang Bergantung pada Tempat Kerja (*Soft Issues - Workplace Independent*)

Workplace independence, atau kemandirian di tempat kerja, adalah faktor penting yang memengaruhi *Information Security Awareness* (ISA). Konsep ini mencakup otonomi yang dimiliki karyawan dalam menjalankan tugasnya, yang dapat memengaruhi kesadaran dan kepatuhan terhadap praktik keamanan informasi. Hubungan ini bersifat multidimensi, mencakup keterlibatan karyawan, budaya organisasi, serta pengaruh psikologis terhadap perilaku keamanan.

Penelitian menunjukkan bahwa keterikatan karyawan yang aman di tempat kerja dapat meningkatkan kenyamanan dan keterlibatan mereka, yang pada akhirnya memperkuat ISA. Mura et al. (2023) mengungkapkan bahwa keterikatan yang aman di tempat kerja membantu meningkatkan keterlibatan kerja di kalangan staf kesehatan. Ketika karyawan merasa nyaman dan aman di lingkungan kerja mereka, [illegible]ka lebih cenderung berpartisipasi aktif dalam inisiatif kesadaran [illegible]anan informasi.

Kenyamanan ini menciptakan budaya kepatuhan, di mana [illegible]wan lebih termotivasi untuk terlibat dalam program-program ISA [illegible]nematuhi protokol keamanan. Hal ini menunjukkan bahwa otonomi [illegible]wan yang didukung oleh lingkungan kerja yang mendukung dapat [illegible]orong kesadaran dan perilaku keamanan yang lebih baik.

Budaya organisasi memainkan peran penting dalam membentuk ISA. Farshadkhah dan Stafford (2019) menekankan pentingnya dinamika sosial dalam memotivasi perilaku pro-keamanan. Karyawan dipengaruhi oleh rekan kerja dan lingkungan organisasi mereka. Ketika budaya organisasi mendukung prioritas keamanan informasi, karyawan lebih cenderung terlibat dalam perilaku keamanan yang proaktif.

Budaya yang mendukung juga memperkuat rasa tanggung jawab individu terhadap keamanan informasi. Hal ini mendorong karyawan untuk memanfaatkan kemandirian mereka dalam peran masing-masing untuk mendukung tujuan keamanan organisasi.

Aspek psikologis dari kemandirian di tempat kerja juga berkontribusi pada ISA. Rebillon et al. (2023) menunjukkan bahwa kenyamanan yang dirasakan di tempat kerja berhubungan dengan gaya keterikatan, yang memengaruhi perilaku positif seperti kepatuhan terhadap kebijakan keamanan. Lingkungan kerja yang mendukung tidak hanya mengurangi tingkat stres tetapi juga meningkatkan keterlibatan karyawan, faktor penting dalam mempertahankan tingkat ISA yang tinggi.

Selain itu, otonomi dapat memberikan karyawan rasa kepemilikan terhadap tanggung jawab keamanan mereka. Hal ini memungkinkan mereka untuk mengambil keputusan yang lebih sadar terkait perlindungan aset informasi.

Implementasi program ISA yang efektif sangat penting dalam menciptakan budaya keamanan di dalam organisasi. Legárd (2020) menyoroti pentingnya program ISA yang disesuaikan dengan karakteristik unik organisasi, termasuk strategi komunikasi dan keterlibatan. Program seperti ini dapat memanfaatkan otonomi karyawan untuk mendorong mereka mengambil peran aktif dalam praktik keamanan, sekaligus memperkuat pengetahuan dan perilaku mereka.

Program pelatihan yang dirancang untuk meningkatkan pengetahuan karyawan juga harus mendorong adopsi kebiasaan keamanan yang positif. Dengan demikian, otonomi di tempat kerja dapat menjadi aset penting dalam membangun budaya keamanan yang lebih kuat.

2.3.2 Faktor Ekstrinsik (Sari et al., 2021)

1) Pelatihan dan Kesadaran (*Training and Awareness*)

Pelatihan keamanan informasi membantu individu memahami ancaman
anggung jawab mereka. Pelatihan yang interaktif dan relevan lebih
f dalam meningkatkan kesadaran.

jemen Operasional (*Operational Management*)

jemen operasional berperan dalam memastikan sistem keamanan
konsisten diterapkan di seluruh organisasi. Tata kelola keamanan
baik membantu meningkatkan kepatuhan dan kesadaran di tingkat
asional.

3) Budaya Organisasi (*Organizational Culture*)
   Budaya organisasi yang mendukung keamanan informasi memainkan peran penting dalam mendorong perilaku yang diinginkan. Organisasi dengan budaya keamanan yang kuat cenderung memiliki tingkat pelanggaran yang lebih rendah.
4) Dukungan Manajemen Puncak (*Top Management Support*)
   Dukungan dari manajemen puncak, seperti penyediaan sumber daya dan promosi kebijakan keamanan, mendorong kepatuhan individu. Keterlibatan manajemen sangat penting untuk menciptakan lingkungan yang kondusif bagi keamanan.
5) Kemampuan di Tempat Kerja (*Workplace Capabilities*)
   Kemampuan teknis dan fasilitas kerja yang memadai memungkinkan karyawan untuk melaksanakan praktik keamanan dengan lebih mudah. Alat dan infrastruktur yang mendukung keamanan sangat penting untuk menunjang praktik keamanan.
6) Faktor Risiko dan Tindakan (*Risk and Response Factors*)
   Kesadaran akan risiko dan respons terhadap ancaman keamanan menjadi motivasi eksternal bagi individu untuk mengambil langkah pencegahan. Persepsi risiko meningkatkan kepatuhan terhadap kebijakan keamanan.
7) Manajemen Perubahan (*Change Management*)
   Perubahan dalam kebijakan atau teknologi keamanan membutuhkan pendekatan manajemen perubahan yang baik. Komunikasi yang jelas dan pelibatan karyawan membantu mengurangi resistensi terhadap perubahan.
8) Kebijakan Keamanan Informasi (*Information Security Policies*)
   Kebijakan keamanan yang jelas dan mudah dipahami menjadi panduan utama bagi karyawan. Kebijakan yang relevan dan terukur membantu menciptakan kesadaran yang lebih baik.

2.4 *Information Security Culture* (Budaya Keamanan Informasi)

Budaya kesadaran informasi dapat didefinisikan sebagai sikap dan perilaku kolektif dalam sebuah organisasi yang mendukung praktik keamanan informasi. Penelitian menunjukkan bahwa kesadaran informasi berfungsi sebagai pendorong utama dalam membentuk budaya keamanan informasi yang kuat. Dalam konteks lembaga jasa keuangan, misalnya, kesadaran informasi dan norma subjektif terbukti menjadi prediktor signifikan bagi budaya keamanan informasi (Mupokosera et al., 2023)

Studi sebelumnya menunjukkan hubungan antara budaya organisasi dan
nasi. Penelitian ini menunjukkan bahwa budaya organisasi yang
ningkatkan kesadaran informasi di kalangan karyawan, yang pada
urangi risiko pelanggaran keamanan (Wiley et al., 2020). Oleh
nting bagi manajemen untuk menciptakan lingkungan yang
belajaran dan komunikasi terkait keamanan informasi.

Dalam konteks organisasi kemanusiaan, model kesadaran informasi yang ditingkatkan telah diusulkan untuk memenuhi kebutuhan spesifik mereka. Model ini mencakup area tambahan seperti pengamanan perangkat dan pemahaman kebijakan, yang terbukti meningkatkan kesadaran keamanan informasi di dalam organisasi tersebut (Al-Nassiri & Al-Balatah, 2024). Hal ini menunjukkan bahwa penyesuaian model kesadaran informasi sesuai dengan konteks organisasi dapat meningkatkan efektivitas program pelatihan dan kesadaran.

Studi sistematis tentang evolusi maturitas kesadaran informasi mengidentifikasi dimensi standar seperti manajemen risiko, budaya organisasi, program pelatihan, kepatuhan terhadap kebijakan, dan langkah-langkah teknis. Penelitian ini menekankan perlunya pendekatan komprehensif dalam pengembangan kerangka kerja maturitas ISA untuk menghadapi ancaman siber yang terus berkembang (Ahmad et al., 2024). Dengan demikian, organisasi perlu mengintegrasikan kontrol teknis dengan penilaian perilaku untuk mencapai tingkat maturitas yang lebih tinggi.

Pengukuran tingkat kesadaran informasi di kalangan karyawan menjadi krusial untuk memperkuat budaya keamanan. Beberapa pendekatan telah digunakan untuk mengevaluasi tingkat kesadaran ini, termasuk paradigma Pengetahuan, Sikap, dan Perilaku (KAB). Penelitian menunjukkan bahwa mengukur ketiga aspek ini dapat memberikan wawasan penting tentang efektivitas program pelatihan keamanan informasi (Perkasa & Setiawan, 2024).

2.5 Rumah Sakit

2.5.1 Definisi Rumah Sakit

Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan menjelaskan bahwa Rumah Sakit merupakan fasilitas pelayanan kesehatan yang menyelenggarakan pelayanan kesehatan perseorangan secara paripurna melalui pelayanan kesehatan promotif, preventif, kuratif, rehabilitatif, dan/atau paliatif dengan menyediakan pelayanan rawat inap, rawat jalan, dan gawat darurat. Dalam pelaksanaannya secara perseorangan dalam bentuk spesialistik dan/atau spesialistik, pelayanan kesehatan dasar, penyelenggaraan fungsi pendidikan dan penelitian di bidang kesehatan (DPR RI, 2023).

Pada peraturan Pemerintah Nomor 47 tahun 2021 menjelaskan bahwa Rumah Sakit adalah institusi pelayanan kesehatan kesehatan yang menyelenggarakan pelayanan kesehatan perorangan secara paripurna yang menyediakan pelayanan terdiri dari rawat inap, rawat jalan, dan gawat darurat. Akreditasi rumah sakit merupakan pengakuan terhadap mutu
an rumah sakit setelah dilakukan beberapa tahap penilaian bahwa
akit telah memenuhi standar akreditasi (PP No. 47, 2021).
ari definisi rumah sakit yang dipaparkan, rumah sakit adalah untuk
i pasien yang terisolasi dari keluarga dan masyarakat sekitar dan
menawarkan layanan kesehatan yang komprehensif kepada
kat, baik preventif maupun kuratif. Selain menjadi rumah bagi
fasilitas kesehatan ini juga berfungsi sebagai tempat penelitian

biososial dan rumah sakit pendidikan bagi para profesional medis. (Dewan Perwakilan Rakyat RI, 2023).

2.5.2 Tujuan dan Fungsi Rumah Sakit

Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan menjalankan fungsi pelayanan kesehatan perseorangan dalam bentuk spesialistik dan/atau sub-spesialistik, pelayanan kesehatan dasar, dan sebagai penyelenggara fungsi pendidikan dan penelitian di bidang kesehatan, serta menyelenggarakan tata kelola rumah sakit dan tata kelola klinis yang baik (DPR RI., 2023).

2.5.3 Klasifikasi Rumah Sakit

Berdasarkan jenis pelayanan yang tersedia, rumah sakit dikategorikan dalam Rumah Sakit Umum dan Rumah Sakit Khusus yang ditetapkan klasifikasinya oleh pemerintah berdasarkan kapabilitas pelayanan fasilitas kesehatan, sarana penunjang dan sumber daya manusia (PP No. 47 Tahun 2021), klasifikasi tersebut yaitu:

Klasifikasi Rumah Sakit umum terdiri atas:

a. Rumah Sakit umum kelas A;
b. Rumah Sakit umum kelas B;
c. Rumah Sakit umum kelas C; dan
d. Rumah Sakit umum kelas D.

Klasifikasi Rumah Sakit khusus terdiri atas:

a. Rumah Sakit khusus kelas A;
b. Rumah Sakit khusus kelas B; dan
c. Rumah Sakit khusus kelas C.

2.5.4 Kewajiban Rumah Sakit

Setiap rumah sakit memiliki kewajiban terdiri atas (UU Kesehatan Nomor 17 Tahun 2023):

a. Memberikan informasi yang benar tentang pelayanan Rumah Sakit kepada masyarakat;
b. Memberikan pelayanan kesehatan yang aman, bermutu, antidiskriminatif, dan efektif dengan mengutamakan kepentingan pasien sesuai dengan standar pelayanan Rumah Sakit;
c. Memberikan pelayanan gawat darurat kepada pasien sesuai dengan kemampuan pelayanannya;
d. Berperan aktif dalam memberikan pelayanan kesehatan pada bencana
ıai dengan kemampuan pelayanannya;
yediakan sarana dan pelayanan bagi masyarakat tidak mampu
miskin;
ıksanakan fungsi sosial antara lain dengan memberikan fasilitas
yanan bagi pasien tidak mampu atau miskin, pelayanan gawat
ırat tanpa uang muka, ambulans gratis, pelayanan bagi korban

bencana dan kejadian luar biasa (KLB), atau bakti sosial bagi misi kemanusiaan;

g. Membuat, melaksanakan, dan menjaga standar mutu pelayanan kesehatan di Rumah Sakit sebagai acuan dalam melayani pasien;
h. Menyelenggarakan rekam medis;
i. Menyediakan sarana dan prasarana umum yang layak, antara lain sarana ibadah, tempat parkir, ruang tunggu, sarana untuk penyandang disabilitas, wanita menyusui, anak-anak, dan lanjut usia;
j. Melaksanakan sistem rujukan;
k. Menolak keinginan pasien yang bertentangan dengan standar profesi dan etika serta ketentuan peraturan perundang-undangan;
l. Memberikan informasi yang benar, jelas, dan jujur mengenai hak dan kewajiban pasien;
m. Menghormati dan melindungi hak-hak pasien;
n. Melaksanakan etika Rumah Sakit;
o. Memiliki sistem pencegahan kecelakaan dan penanggulangan bencana;
p. Melaksanakan program pemerintah di bidang kesehatan, baik secara regional maupun nasional;
q. Membuat daftar tenaga medis yang melakukan praktik kedokteran atau kedokteran gigi dan tenaga kesehatan lainnya;
r. Menyusun dan melaksanakan peraturan internal Rumah Sakit;
s. Melindungi dan memberikan bantuan hukum bagi semua petugas Rumah Sakit dalam melaksanakan tugas; dan
t. Memberlakukan seluruh lingkungan Rumah Sakit sebagai kawasan tanpa rokok.

2.5.5 Hak Rumah Sakit

Rumah sakit memiliki hak berupa (UU Kesehatan No, 17 Tahun 2023):

a. Menentukan jumlah, jenis, dan kualifikasi sumber daya manusia sesuai dengan klasifikasi Rumah Sakit;
b. Menerima imbalan jasa pelayanan serta menentukan remunerasi, insentif, dan penghargaan sesuai dengan ketentuan peraturan perundang-undangan;
c. Melakukan kerja sama dengan pihak lain dalam mengembangkan pelayanan;
d. Menerima bantuan dari pihak lain sesuai dengan ketentuan peraturan perundang-undangan;
e. Menggugat pihak yang mengakibatkan kerugian;
f. dapatkan pelindungan hukum dalam melaksanakan pelayanan hatan; dan
g. promosikan layanan kesehatan yang ada di Rumah Sakit sesuai an ketentuan peraturan perundang-undangan.

2.6 Sistem Informasi Manajemen Rumah Sakit (SIMRS)

2.6.1 Definisi SIMRS

Sistem Informasi Manajemen Rumah Sakit (SIMRS) adalah sistem terintegrasi yang dirancang untuk mengelola seluruh aspek operasional dan manajerial di rumah sakit. SIMRS mencakup berbagai modul fungsional yang mendukung kegiatan administratif, klinis, dan finansial rumah sakit, seperti pendaftaran pasien, manajemen rekam medis, pelayanan farmasi, manajemen laboratorium, serta pengelolaan keuangan dan inventaris. Tujuan utama dari SIMRS adalah untuk meningkatkan efisiensi dan efektivitas pelayanan kesehatan dengan meminimalkan waktu dan biaya yang dibutuhkan untuk menangani proses manual, serta memperbaiki kualitas informasi yang digunakan untuk pengambilan keputusan.

2.6.2 Komponen SIMRS

SIMRS terdiri dari beberapa komponen utama, antara lain:

a. Pendaftaran dan Administrasi Pasien
   Modul ini digunakan untuk mengelola data pasien sejak pertama kali masuk rumah sakit, termasuk proses pendaftaran, pengelolaan identitas pasien, penjadwalan rawat inap, dan rawat jalan.
b. Rekam Medis Elektronik (*Electronic Medical Record*/ EMR)
   Rekam medis pasien yang didigitalkan dan terintegrasi, sehingga tenaga kesehatan dapat mengakses data pasien secara *real-time* untuk mempercepat diagnosis dan pengobatan.
c. Sistem Informasi Keuangan
   Mengelola seluruh aspek finansial di rumah sakit, termasuk *billing*, klaim asuransi, serta laporan keuangan.
d. Manajemen Laboratorium dan Radiologi
   SIMRS memungkinkan manajemen hasil laboratorium dan radiologi secara elektronik, mengurangi kesalahan manusia dalam pencatatan dan pengiriman hasil.
e. Manajemen Farmasi
   Mengelola persediaan obat dan alat kesehatan, termasuk proses pengadaan, distribusi, serta kontrol penggunaan obat yang lebih efisien dan terpantau.

2.6.3 Peran dan Manfaat SIMRS

SIMRS berperan penting dalam meningkatkan efisiensi operasional rumah sakit. Manfaat utama dari implementasi SIMRS antara lain:

- Meningkatkan Kualitas Pelayanan Kesehatan
  ...an sistem yang terintegrasi, informasi medis pasien dapat diakses ...a cepat dan akurat oleh tenaga kesehatan, sehingga proses ...osis dan pengobatan bisa dilakukan dengan lebih baik.
- ...ngkatkan Efisiensi Administratif

SIMRS mengurangi proses manual yang memerlukan banyak waktu dan sumber daya manusia, sehingga operasional rumah sakit berjalan lebih efisien.

c. Pengambilan Keputusan yang Lebih Baik
Data yang dikumpulkan oleh SIMRS dapat digunakan oleh manajemen rumah sakit untuk analisis dan pengambilan keputusan strategis berdasarkan informasi yang lebih akurat.

d. Transparansi dan Akuntabilitas Keuangan
Modul keuangan SIMRS membantu meningkatkan transparansi dalam pengelolaan biaya layanan kesehatan, pembayaran, serta klaim asuransi, sehingga meminimalisir kesalahan atau *fraud*.

e. Meningkatkan Keamanan Data Pasien
Dengan implementasi SIMRS, data pasien lebih terlindungi karena menggunakan sistem keamanan berbasis digital, dibandingkan dengan metode manual yang rentan terhadap pencurian atau kerusakan data.

2.6.4 Regulasi Terkait SIMRS

Pemerintah Indonesia telah menetapkan regulasi terkait pengembangan dan implementasi SIMRS melalui Peraturan Menteri Kesehatan (Permenkes) Nomor 82 Tahun 2013 tentang Sistem Informasi Manajemen Rumah Sakit. Permenkes ini yang mengatur kewajiban penerapan SIMRS di semua rumah sakit. SIMRS diharapkan mampu meningkatkan efisiensi dan efektivitas layanan kesehatan dengan memfasilitasi akses data yang lebih cepat, mengintegrasikan layanan seperti BPJS, dan memudahkan pelaporan ke Kementerian Kesehatan. Rumah sakit diharuskan menggunakan aplikasi SIMRS yang sesuai standar, baik dengan menggunakan aplikasi *open source* yang disediakan pemerintah atau mengembangkan sendiri dengan memenuhi persyaratan minimal yang ditetapkan.

Selain itu, PMK Nomor 24 Tahun 2022 memperkenalkan kewajiban penerapan Rekam Medis Elektronik (RME), yang merupakan komponen penting dalam integrasi SIMRS. Rumah sakit harus memastikan bahwa rekam medis mereka terhubung dengan platform SatuSehat dari Kemenkes untuk menciptakan *big data* kesehatan yang lebih efisien. Kewajiban ini harus sudah dipenuhi hingga akhir 2023. Pelanggaran terhadap kewajiban ini dapat menyebabkan sanksi administrasi, pembekuan atau pencabutan izin operasional, hingga pembatasan kerja sama dengan BPJS.

2.7 Review Penelitian Terkait

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

Tabel 1. Review Penelitian Terkait

No	Peneliti	Judul	Variabel Dependen	Variabel Independen	Populasi dan Sampel	Metode	Hasil Penelitian	Persamaan dan Perbedaan
1	Warusia Yassin Al-Shanfari, Nasser Tabook, Roesnita Ismail, and Anuar Ismail	*Determinants of Information Security Awareness and Behaviour Strategies in Public Sector Organizations among Employees.*	Variabel dependen dalam penelitian ini adalah niat perilaku ISA dan perilaku aktual adopsi keamanan informasi (InfoSec) di kalangan karyawan sektor publik.	Faktor-faktor yang memengaruhi, termasuk faktor prediksi kontrol, faktor penangkalan, faktor motivasi, faktor terkait teknis, dan faktor kondisi pendukung, memiliki peran penting dalam analisis perilaku dan pengambilan keputusan.	Populasi dalam penelitian ini terdiri dari karyawan di sektor publik Kesultanan Oman, yang mempekerjakan sekitar 170.104 individu. Ukuran sampel minimum yang diperlukan adalah 384 peserta.	Metodologi penelitian ini menggunakan pendekatan kuantitatif dengan memanfaatkan kuesioner untuk mengumpulkan data dari karyawan sektor publik di Kesultanan Oman, dengan fokus pada faktor-faktor yang memengaruhi kesadaran (ISA) dan perilaku terkait keamanan informasi.	Penelitian ini mengungkapkan bahwa berbagai faktor secara positif memengaruhi niat karyawan sektor publik untuk mengadopsi perilaku keamanan informasi, kecuali untuk kepastian sanksi yang dirasakan.	Persamaan: Meneliti mengenai faktor yang mempengaruhi ISA. Perbedaan: faktor-faktor yang diamati sangat banyak dan tidak dikelompokkan ke dalam intrinsik dan ekstrinsik.
2	Ag M Ta	s	Variabel dependen dalam	Variabel independen yang dianalisis dalam	Populasi penelitian terdiri dari pekerja di	Penelitian ini menggunakan metodologi survei	Penelitian ini mengungkapkan bahwa sifat-sifat	Persamaan: Sama-sama

No	Peneliti	Judul	Variabel Dependen	Variabel Independen	Populasi dan Sampel	Metode	Hasil Penelitian	Persamaan dan Perbedaan
	Zwaans, Kathryn Parsons, Dragana Calic, Marcus Butavicius, and Malcolm Pattinson.	*Information Security Awareness.*	penelitian ini adalah Kesadaran Keamanan Informasi (*Information Security Awareness*/ ISA), yang didefinisikan sebagai pengetahuan, sikap, dan perilaku individu terhadap kebijakan serta prosedur keamanan informasi.	penelitian ini meliputi usia, jenis kelamin, sifat kepribadian (kesungguhan, keramahan, stabilitas emosional, keterbukaan), dan kecenderungan untuk mengambil risiko.	Australia, khususnya individu berusia di atas 18 tahun yang saat ini bekerja dan menghabiskan sebagian waktu kerja mereka menggunakan komputer. Sebanyak 505 individu berpartisipasi dalam survei ini, yang mengumpulkan data demografis, termasuk usia dan jenis kelamin.	untuk menganalisis hubungan antara perbedaan individu dan Kesadaran Keamanan Informasi (*Information Security Awareness*/ ISA) di antara 505 pekerja di Australia. Partisipan diwajibkan berusia di atas 18 tahun, saat ini bekerja, dan berada di Australia, dengan fokus pada mereka yang menggunakan komputer di organisasi yang memiliki kebijakan	seperti kesungguhan (*conscientiousness*), keramahan (*agreeableness*), stabilitas emosional, dan kecenderungan mengambil risiko secara signifikan memengaruhi Kesadaran Keamanan Informasi (*Information Security Awareness*/ ISA). Usia juga berperan, di mana individu yang lebih tua menunjukkan skor ISA yang lebih tinggi. Penelitian ini memvalidasi model Pengetahuan,	meneliti mengenai ISA. Perbedaan: Faktor yang diamati berfokus pada faktor internal pekerja.

No	Peneliti	Judul	Variabel Dependen	Variabel Independen	Populasi dan Sampel	Metode	Hasil Penelitian	Persamaan dan Perbedaan
						keamanan informasi (InfoSec) formal maupun informal. Untuk mengukur ISA, digunakan *Human Aspects of Information Security Questionnaire* (HAIS-Q), yang menilai pengetahuan, sikap, dan perilaku individu terkait kebijakan dan prosedur keamanan informasi.	Sikap, dan Perilaku (*Knowledge, Attitude, and Behavior*/ KAB) untuk mengukur ISA, dengan menekankan pentingnya pengetahuan dan sikap dalam memprediksi perilaku keamanan informasi. Temuan ini menunjukkan perlunya pelatihan keamanan informasi yang disesuaikan berdasarkan perbedaan individu.	

No	Peneliti	Judul	Variabel Dependen	Variabel Independen	Populasi dan Sampel	Metode	Hasil Penelitian	Persamaan dan Perbedaan
3	Adéle Da Veiga and Nico Martins.	*Defining and identifying dominant information security cultures and subcultures.*	Budaya keamanan informasi.	Intervensi keamanan informasi, faktor geografis, faktor divisi kerja, faktor demografis.	Populasi penelitian terdiri dari karyawan dari berbagai unit bisnis dan negara dalam organisasi, dengan jumlah total karyawan didokumentasikan untuk setiap survei yang dilakukan. Sampel yang representatif diambil dengan memastikan jumlah respons yang cukup untuk memenuhi tingkat kepercayaan 95% dalam analisis data. Metode survei memungkinkan diagnosis budaya keamanan informasi	Penelitian ini menggunakan metode survei kuantitatif untuk mengukur budaya keamanan informasi dalam organisasi. Instrumen yang digunakan adalah kuesioner untuk mengumpulkan data tentang sikap dan persepsi karyawan, yang memungkinkan analisis statistik untuk mengidentifikasi subkultur. Metodologi ini memastikan keandalan dan validitas instrumen diagnostik, yang	Hasil menunjukkan peningkatan budaya keamanan informasi (IS) secara keseluruhan, dengan perubahan positif terbesar pada 2013 saat skor rata-rata melebihi 4,0. Penurunan skor IS pada 2010 terjadi akibat restrukturisasi bisnis. Intervensi spesifik dilakukan berdasarkan hasil survei, menargetkan subkultur IS tertentu, terutama di Sydney dan Johannesburg. Persentase	Persamaan: Sama-sama meneliti mengenai budaya keamanan informasi. Perbedaan: faktor yang diteliti tidak dikelompokkan ke dalam intrinsik dan ekstrinsik, variabel dependennya juga tidak difokuskan pada ISA tetapi pada budaya keamanan informasi.

No	Peneliti	Judul	Variabel Dependen	Variabel Independen	Populasi dan Sampel	Metode	Hasil Penelitian	Persamaan dan Perbedaan
					organisasi dan identifikasi subkultur potensial. Pertanyaan biografis dalam survei membantu segmentasi data dan perbandingan respons di antara kelompok demografis yang berbeda.	sangat penting untuk memperoleh hasil yang akurat dalam konteks studi budaya organisasi.	kesepakatan pada pernyataan utama tentang komitmen terhadap keamanan informasi meningkat dari 2006 hingga 2013, mencerminkan peningkatan kesadaran dan keterlibatan.	
4	Ernest Godson, Deus Ngaruko, and George Oreku.	*Influence of Information Security Awareness on Security of Electronic*	Variabel utama yang diteliti adalah keamanan rekam medis elektronik (EHR) di rumah sakit umum Tanzania, dipengaruhi oleh kesadaran	Variabel independen dalam studi ini meliputi kesadaran tentang kebijakan keamanan, *phishing* dan rekayasa sosial, langkah keamanan teknis, serta respons insiden. Semua	Populasi penelitian terdiri dari 1200 pengguna utama EHR di enam rumah sakit umum di Tanzania, termasuk dokter, petugas IT, perawat, apoteker, teknolog	Penelitian menggunakan desain survei hipotesis eksplanatori dengan pendekatan kuantitatif untuk menilai pengaruh kesadaran keamanan informasi terhadap	Penelitian menunjukkan pengaruh positif yang signifikan secara statistik antara kesadaran keamanan informasi (ISA) dan keamanan rekam medis elektronik (EHR) di rumah sakit umum Tanzania	Persamaan: Sama-sama menyertakan variabel kesadaran keamanan informasi. Perbedaan: ISA pada penelitian ini berperan sebagai faktor independen. Penelitian ini

No	Peneliti	Judul	Variabel Dependen	Variabel Independen	Populasi dan Sampel	Metode	Hasil Penelitian	Persamaan dan Perbedaan
			keamanan informasi. Keamanan EHR juga dipengaruhi oleh kontrol keamanan, seperti kebijakan keamanan, *phishing*, teknik sosial, langkah teknis, dan respons insiden. Temuan menunjukkan bahwa kesadaran akan faktor-faktor ini secara signifikan memengaruhi keamanan EHR, menegaskan	variabel ini secara signifikan memengaruhi keamanan rekam medis elektronik (EHR) di rumah sakit umum Tanzania. Peningkatan kesadaran di area ini berdampak positif pada keamanan EHR, dengan koefisien yang menunjukkan tingkat pengaruh masing-masing. Hal ini menekankan pentingnya pelatihan kesadaran keamanan informasi yang komprehensif	laboratorium, petugas pencatatan, dan staf administratif. Teknik *purposive sampling* digunakan untuk memilih 300 responden dengan tingkat presisi 5% (e = 0,05). Ukuran sampel ini dianggap cukup untuk menganalisis pengaruh kesadaran keamanan informasi terhadap keamanan EHR.	keamanan rekam medis elektronik (EHR) di rumah sakit umum Tanzania. Sampel 300 responden, termasuk pengguna utama EHR seperti dokter, petugas IT, dan perawat, dipilih dari enam rumah sakit umum di berbagai zona di Tanzania menggunakan teknik *purposive sampling*. Data dikumpulkan melalui kuesioner survei daring dan dianalisis menggunakan statistik deskriptif serta regresi linier berganda untuk	($p < 0,01$). Analisis regresi menunjukkan variabel independen menjelaskan 39,6% variansi dalam keamanan EHR, sementara 60,4% dipengaruhi faktor lain. Temuan ini mendukung pentingnya pelatihan dan program kesadaran rutin untuk meningkatkan keamanan EHR di rumah sakit tersebut.	berfokus pada bagaimana ISA mempengaruhi keamanan informasi.

No	Peneliti	Judul	Variabel Dependen	Variabel Independen	Populasi dan Sampel	Metode	Hasil Penelitian	Persamaan dan Perbedaan
			pentingnya kesadaran keamanan informasi di sektor kesehatan.	bagi karyawan sektor kesehatan.		menguji hipotesis penelitian.		
5	Felix Haeussinger and Johann Kranz.	*Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior.*	Variabel dependen utama dalam penelitian ini adalah "Niat untuk mematuhi" Kebijakan Keamanan Informasi (ISPs), yang mencerminkan kesediaan karyawan untuk mengikuti protokol keamanan organisasi. Model penelitian	Variabel independen dalam penelitian ini meliputi Penyediaan Kebijakan Keamanan Informasi (ISP Provision), Program Pendidikan, Pelatihan, dan Kesadaran Keamanan (SETA), Pengetahuan Sistem Informasi (IS *Knowledge*), Pengaruh Sumber Sekunder, dan Perilaku Rekan.	Populasi penelitian terdiri dari karyawan dari berbagai organisasi yang memiliki Kebijakan Keamanan Informasi (ISPs). Sebanyak 1.120 pengunjung awal direkrut melalui berbagai saluran distribusi, termasuk email dan jaringan bisnis. Dari jumlah tersebut, 661 peserta menyelesaikan kuesioner, namun	Penelitian ini menggunakan pendekatan pemodelan persamaan struktural untuk memvalidasi model yang diusulkan, dengan metode *partial least square* (PLS) berbasis komponen menggunakan SmartPLS versi 2.0. Survei daring dilakukan, di mana 1.120 pengunjung awal direkrut, menghasilkan	Model penelitian divalidasi menggunakan pemodelan persamaan struktural, yang menjelaskan sebagian besar variansi dalam Kesadaran Keamanan Informasi (ISA) dan niat untuk mematuhi kebijakan keamanan, dengan nilai R^2 masing-masing sebesar .50 dan .41. ISA ditemukan	Persamaan: sama-sama menyertakan ISA. Perbedaan: ISA pada penelitian ini berperan sebagai variabel mediasi.

No	Peneliti	Judul	Variabel Dependen	Variabel Independen	Populasi dan Sampel	Metode	Hasil Penelitian	Persamaan dan Perbedaan
			menunjukkan bahwa niat untuk mematuhi dipengaruhi oleh berbagai faktor awal, dengan Kesadaran Keamanan Informasi (ISA) sebagai mediator. Studi ini juga mengkaji dampak subdimensi ISA, yaitu Kesadaran Umum (GISA) dan Kesadaran ISP (ISPA), terhadap niat untuk mematuhi.	Semua variabel ini memengaruhi variabel dependen, yaitu Niat untuk mematuhi kebijakan keamanan informasi (ISPs). Model penelitian menunjukkan bahwa variabel-variabel tersebut berkontribusi pada pengembangan Kesadaran Keamanan Informasi (ISA), yang memediasi pengaruhnya terhadap niat untuk mematuhi.	setelah mengecualikan respons yang tidak dapat dipercaya dan mereka yang bekerja sendiri atau berasal dari organisasi tanpa ISP, ukuran sampel akhir adalah 475 responden. Demografi sampel menunjukkan mayoritas berjenis kelamin laki-laki (68%) dengan rentang usia yang beragam, di mana kelompok terbesar adalah usia 26-35 tahun (52,2%).	ukuran sampel akhir 475 responden setelah mengecualikan respons yang tidak dapat dipercaya dan tidak relevan. Studi ini menilai properti psikometrik dari model pengukuran dan menguji hipotesis menggunakan model struktural, memastikan reliabilitas dan validitas konstruk yang terlibat.	memediasi sepenuhnya hubungan antara niat untuk mematuhi dan Penyediaan Kebijakan Keamanan Informasi (ISP Provision) serta Program SETA, sementara memediasi sebagian pengaruh Pengetahuan Sistem Informasi (IS *Knowledge*), Pengaruh Sumber Sekunder, dan Perilaku Rekan terhadap niat untuk mematuhi. Penelitian ini mengonfirmasi bahwa promosi dan penyediaan	

No	Peneliti	Judul	Variabel Dependen	Variabel Independen	Populasi dan Sampel	Metode	Hasil Penelitian	Persamaan dan Perbedaan
							ISP adalah faktor awal yang paling signifikan untuk ISA.	
6	Norshima Humaidi and Vimala Balakrishnan .	*Leadership Styles and Information Security Compliance Behavior: The Mediator Effect of Information Security Awareness*	Variabel dependen dalam penelitian ini adalah perilaku kepatuhan pengguna terhadap kebijakan keamanan informasi.	Variabel independen dalam penelitian ini adalah gaya kepemimpinan, khususnya kepemimpinan transformasional dan kepemimpinan transaksional.	Populasi penelitian terdiri dari karyawan di tiga rumah sakit lokal di Malaysia: Rumah Sakit Serdang, Rumah Sakit Selayang, dan Rumah Sakit Sungai Buloh. Sebanyak 900 kuesioner dibagikan kepada tenaga kesehatan, termasuk dokter, staf pendukung, dan administrator kesehatan, yang merupakan pengguna akhir dari Sistem Informasi	Penelitian ini menggunakan metode penelitian kuantitatif dengan kuesioner yang dikembangkan berdasarkan studi tentang gaya kepemimpinan dan *Health Belief Model* (HBM) terkait keamanan informasi.	Penelitian ini menemukan bahwa gaya kepemimpinan transformasional dan transaksional secara signifikan memengaruhi kesadaran karyawan terhadap keamanan informasi, dengan gaya kepemimpinan transaksional memiliki efek langsung dan tidak langsung terhadap perilaku kepatuhan melalui kesadaran akan keparahan dan	Persamaan: sama-sama meneliti mengenai perilaku keamanan informasi. Perbedaan: Penelitian ini berfokus pada gaya kepemimpinan dan perilaku keamanan informasi.

No	Peneliti	Judul	Variabel Dependen	Variabel Independen	Populasi dan Sampel	Metode	Hasil Penelitian	Persamaan dan Perbedaan
					Kesehatan (HIS). Dari kuesioner yang dibagikan, 454 dikembalikan dan divalidasi, 421 tidak memberikan respons, dan 25 ditolak karena memiliki banyak nilai yang hilang. Mayoritas responden adalah perempuan (78,6%), berusia antara 20-40 tahun (86,7%), dan memiliki pengalaman kerja dengan HIS kurang dari 10 tahun (80%).		manfaat. Model penelitian menunjukkan validitas diskriminan yang memadai, yang mengindikasikan tidak adanya tumpang tindih antar konstruk dalam pengukuran. Analisis menunjukkan bahwa 46,7% variansi dalam perilaku kepatuhan dijelaskan oleh konstruk kesadaran, sementara kesadaran akan kerentanan tidak memiliki pengaruh signifikan terhadap perilaku	

No	Peneliti	Judul	Variabel Dependen	Variabel Independen	Populasi dan Sampel	Metode	Hasil Penelitian	Persamaan dan Perbedaan
							kepatuhan. Temuan ini menggarisbawahi bahwa peningkatan kesadaran keamanan informasi dapat meningkatkan perilaku kepatuhan terhadap kebijakan keamanan informasi di kalangan profesional kesehatan.	
7	Adéle Da Veiga.	*An approach to information* *y* *ange* *ng* *and* *A* *aire*	Variabel dependen dalam penelitian ini terkait dengan persepsi dan perilaku karyawan terhadap	Variabel independen dalam penelitian ini berkaitan dengan integrasi pendekatan manajemen perubahan dan penilaian budaya	Populasi penelitian mencakup seluruh karyawan organisasi yang berpartisipasi, dengan sekitar 7.000 karyawan pada survei	Penelitian ini menggunakan pendekatan *Information Security Culture Change Management* (ISCCM) yang mengintegrasikan	Penelitian ini menunjukkan bahwa pendekatan ISCCM bersama instrumen diagnostik ISCA efektif dalam mendefinisikan	Persamaan: sama-sama meneliti mengenai ISCA. Perbedaan: Variabel dependen yang diamati pada peneltiian ini

No	Peneliti	Judul	Variabel Dependen	Variabel Independen	Populasi dan Sampel	Metode	Hasil Penelitian	Persamaan dan Perbedaan
		transition to the desired culture	budaya keamanan informasi. Variabel-variabel ini mencakup penerimaan karyawan terhadap perubahan praktik kerja untuk memastikan keamanan informasi, kepatuhan terhadap kebijakan keamanan informasi, dan persepsi tentang pentingnya meluangkan waktu untuk inisiatif	keamanan informasi. Secara khusus, penelitian ini menggunakan model ADKAR dari Prosci dan instrumen diagnostik *Information Security Culture Assessment* (ISCA) sebagai kerangka kerja untuk mengukur efektivitas intervensi yang bertujuan mengubah perilaku karyawan terkait keamanan informasi.	pertama dan sekitar 8.000 karyawan pada survei lanjutan. Sampel terdiri dari 2.320 karyawan yang merespons survei pertama dan 2.159 karyawan yang berpartisipasi dalam survei lanjutan. Survei dilakukan secara sukarela, dan metode Krejcie dan Morgan digunakan untuk menentukan jumlah minimum respons yang diperlukan untuk tingkat kepercayaan 95%, yaitu 364 untuk survei pertama dan 367	model ADKAR dan instrumen diagnostik *Information Security Culture Assessment* (ISCA) untuk menangani perilaku karyawan yang memengaruhi keamanan informasi. Data dari studi empiris digunakan untuk menunjukkan efektivitas pendekatan ISCCM, dengan fokus pada pendefinisian intervensi manajemen perubahan berdasarkan hasil survei ISCA. Metodologi	intervensi perubahan keamanan informasi. Survei lanjutan menunjukkan peningkatan signifikan dalam persepsi dan penerimaan karyawan terhadap perubahan. Manajemen berkelanjutan terhadap budaya keamanan informasi diperlukan untuk memastikan kepatuhan karyawan, yang memperkuat budaya keamanan organisasi. Data ISCA membantu	adalah persepsi individu mengenai ISCA yang dipengaruhi oleh integrasi pendekaan manajemen.

No	Peneliti	Judul	Variabel Dependen	Variabel Independen	Populasi dan Sampel	Metode	Hasil Penelitian	Persamaan dan Perbedaan
			keamanan informasi.		untuk survei lanjutan.	penelitian mencakup metode sampel sensus untuk mengumpulkan respons dari karyawan di berbagai tingkat pekerjaan dan lokasi, guna memberikan pemahaman menyeluruh tentang budaya keamanan informasi organisasi.	memahami budaya keamanan dan kebutuhan pelatihan serta kesadaran.	

2.8 Mapping Teori

Berdasarkan hasil kajian peneliti, berikut adalah gambaran mapping teori penelitian:

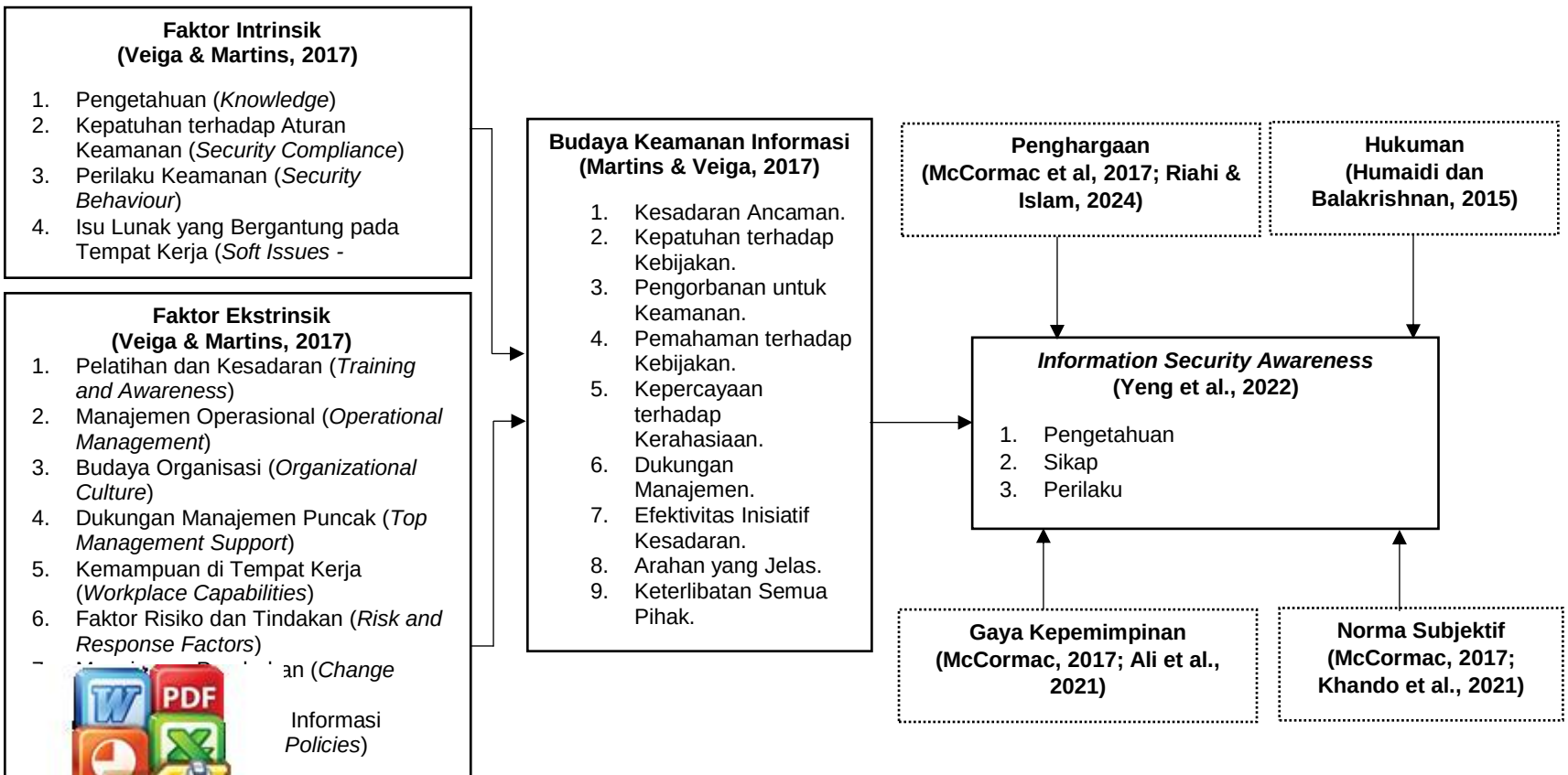
***Information Security Awareness* (ISA)**	***Information Security Culture* (ISC)**	**Faktor Intrinsik**	**Faktor Ekstrinsik**
(Alhuwail et al., 2021) 1. Target Pelatihan Keamanan Siber. 2. Prioritas Pelatihan untuk Dokter. 3. Identifikasi Individu Rentan.	(Georgiadou et al., 2022) 1. Organisasional (asset, keberlanjutan, akses dan kepercayaan, operasi, perlindungan, tata kelola keamanan). 2. Individual (sikap, kesadaran, perilaku, kompetensi).	**(Veiga & Martins, 2017)** **1. Pengetahuan (*Knowledge*).** **2. Kepatuhan terhadap Aturan Keamanan (*Security Compliance*).** **3. Perilaku Keamanan (*Security Behaviour*).** **4. Isu Lunak yang Bergantung pada Tempat Kerja (*Soft Issues - Workplace Independent*).**	**(Veiga & Martins, 2017)** **1. Pelatihan dan Kesadaran (*Training and Awareness*).** **2. Manajemen Operasional (*Operational Management*).** **3. Budaya Organisasi (*Organizational Culture*).** **4. Dukungan Manajemen Puncak (*Top Management Support*).** **5. Kemampuan di Tempat Kerja (*Workplace Capabilities*).** **6. Faktor Risiko dan Tindakan (*Risk and Response Factors*).** **7. Manajemen Perubahan (*Change Management*).** **8. Kebijakan Keamanan Informasi (*Information Security Policies*).**

***Information Security Awareness* (ISA)**	***Information Security Culture* (ISC)**	**Faktor Intrinsik**	**Faktor Ekstrinsik**
(Kő et al., 2023) 1. Manajemen Risiko dan Struktur Organisasi. 2. Level Maturitas ISA .	**(Veiga & Martins, 2017)** **1. Kesadaran Ancaman.** **2. Kepatuhan terhadap Kebijakan.** **3. Pengorbanan untuk Keamanan.** **4. Pemahaman terhadap Kebijakan.** **5. Kepercayaan terhadap Kerahasiaan.** **6. Dukungan Manajemen.** **7. Efektivitas Inisiatif Kesadaran.** **8. Arahan yang Jelas.** **9. Keterlibatan Semua Pihak.**	(Almuqrin et al., 2024) 1. *Threat susceptibility* 2. *Threat severity* 3. *Response cost* 4. *Self-efficacy*	
Information Security Awareness **(Yeng et al., 2022)** **1. Pengetahuan.**	(Mikuletič et al., 2024) 1. *Privacy oriented* 2. *Security oriented*		

***Information Security Awareness* (ISA)**	***Information Security Culture* (ISC)**	**Faktor Intrinsik**	**Faktor Ekstrinsik**
(Djotaroeno & Beulen, 2024) 1. Penyederhanaan Topik Keamanan Informasi. 2. Integrasi Penyederhanaan dalam SETA (*Security Education, Training, and Awareness*).			

Gambar 2. Mapping Teori

2.9 Kerangka Teori Penelitian



angka Teori

t al., 2021; Chaudhary, 2024; Khando et al., 2021; Riahi & Islam, 2024; Sari et al., 2021; Veiga & Martins, 2017;

et al., 2022)

2.10 Kerangka Konsep Penelitian

Dalam era digital yang semakin kompleks, keamanan informasi menjadi isu yang krusial terutama di sektor kesehatan. Rumah sakit, sebagai institusi yang mengelola data pasien yang sangat sensitif, memiliki tanggung jawab besar dalam menjaga kerahasiaan, integritas, dan ketersediaan data tersebut. Salah satu kunci dalam menjaga keamanan informasi adalah dengan meningkatkan *Information Security Awareness* (ISA) di kalangan seluruh karyawan.

Penelitian ini bertujuan untuk mengkaji pengaruh faktor intrinsik dan ekstrinsik terhadap *Information Security Awareness* (ISA) di Rumah Sakit Stella Maris Makassar melalui peran budaya keamanan informasi sebagai variabel mediasi. Kerangka konsep penelitian dirancang untuk memberikan pemahaman yang komprehensif mengenai bagaimana elemen-elemen internal dan eksternal individu dalam organisasi berkontribusi pada pembentukan kesadaran keamanan informasi.

Faktor intrinsik mengacu pada karakteristik internal individu yang memengaruhi perilaku mereka terhadap keamanan informasi. Faktor-faktor ini meliputi tingkat pengetahuan seseorang mengenai keamanan informasi, sikap terhadap pentingnya menjaga kerahasiaan data, serta kesadaran diri dalam menjalankan kebijakan keamanan yang berlaku di tempat kerja. Individu yang memiliki faktor intrinsik yang kuat akan lebih cenderung menunjukkan perilaku yang mendukung keamanan informasi.

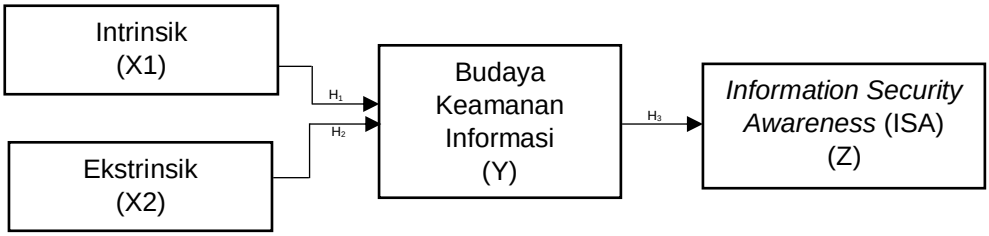
Selain faktor intrinsik, faktor ekstrinsik juga memainkan peran penting dalam membentuk perilaku individu terkait keamanan informasi. Faktor ekstrinsik mencakup pengaruh dari lingkungan eksternal, seperti dukungan manajemen, kebijakan organisasi yang tegas terkait keamanan informasi, serta pelatihan dan edukasi yang diterima oleh karyawan. Dukungan dari organisasi ini bertujuan untuk menciptakan lingkungan kerja yang kondusif dalam membangun kesadaran terhadap pentingnya menjaga keamanan data.

Interaksi antara faktor intrinsik dan ekstrinsik menghasilkan budaya keamanan informasi di dalam organisasi. Budaya keamanan informasi merupakan cerminan sejauh mana kesadaran terhadap keamanan informasi telah melekat dalam perilaku, nilai, dan kebiasaan seluruh anggota organisasi. Dengan adanya budaya keamanan informasi yang kuat, organisasi akan mampu menciptakan lingkungan yang secara konsisten mendukung dan memperkuat praktik-praktik keamanan informasi.

Hasil akhir yang diharapkan dari penelitian ini adalah peningkatan *Information Security Awareness* (ISA) di Rumah Sakit Stella Maris Makassar. ISA menggambarkan tingkat kesadaran individu terhadap ancaman keamanan informasi dan kemampuan mereka dalam mengambil langkah-langkah yang tepat

i data dan informasi organisasi. Dengan adanya budaya keamanan
uat sebagai perantara, faktor intrinsik dan ekstrinsik diyakini akan
h signifikan terhadap peningkatan ISA di lingkungan rumah sakit.

Gambar 4. Kerangka Konsep Penelitian.



2.11 Hipotesis Penelitian

A. Hipotesis Nul/ Awal (H0)

1. Tidak terdapat pengaruh faktor intrinsik terhadap budaya keamanan informasi di Rumah Sakit Stella Maris Makassar.
2. Tidak terdapat pengaruh faktor ekstrinsik terhadap budaya keamanan informasi di Rumah Sakit Stella Maris Makassar.
3. Tidak terdapat pengaruh budaya keamanan informasi terhadap *Information Security Awareness* (ISA) di Rumah Sakit Stella Maris Makassar.

B. Hipotesis Alternatif (Ha)

1. Terdapat pengaruh faktor intrinsik terhadap budaya keamanan informasi di Rumah Sakit Stella Maris Makassar.
2. Terdapat pengaruh faktor ekstrinsik terhadap budaya keamanan informasi di Rumah Sakit Stella Maris Makassar.
3. Terdapat pengaruh budaya keamanan informasi terhadap *Information Security Awareness* (ISA) di Rumah Sakit Stella Maris Makassar.

2.12 Definisi Operasional dan Kriteria Objektif

No	Variabel	Definisi Teori	Definisi Operasional	Alat dan Cara Pengukuran	Kriteria Objektif	Skala
1	Intrinsik	Faktor intrinsik merujuk pada elemen atau karakteristik yang berasal dari dalam suatu sistem atau individu itu sendiri, yang mempengaruhi kinerja, motivasi, atau hasil tertentu (Arshad et al., 2019). 1. Pengetahuan (*Knowledge*): Pengetahuan dalam keamanan informasi merujuk pada pemahaman dan keterampilan yang diperlukan untuk melindungi informasi dari ancaman dan kerentanan (Fenz & Ekelhart, 2009). 2. Kepatuhan terhadap Aturan Keamanan (*Security Compliance*): Kepatuhan terhadap aturan keamanan (*security compliance*) adalah proses di mana	Faktor intrinsik diukur melalui tingkat pengetahuan, motivasi pribadi, serta sikap karyawan terhadap pentingnya keamanan informasi di Rumah Sakit Stella Maris. Indikator faktor intrinsik yang diantaranya adalah sebagai berikut 1. Pengetahuan (*Knowledge*): Tingkat pemahaman individu mengenai pentingnya perlindungan informasi pribadi, sensitif, dan rahasia serta risiko yang terkait dengan masalah keamanan informasi. Pengetahuan ini	Kuesioner sebanyak 12 pertanyaan dengan pilihan jawaban: 4 = Sangat Setuju 3 = Setuju 2 = Tidak Setuju 1 = Sangat Tidak Setuju	Baik jika skor > mean. Kurang jika skor ≤ mean.	Likert

No	Variabel	Definisi Teori	Definisi Operasional	Alat dan Cara Pengukuran	Kriteria Objektif	Skala
		organisasi mematuhi standar hukum, regulasi, dan industri yang mengatur perlindungan data, privasi, dan langkah-langkah keamanan. Ini mencakup penerapan kerangka kerja keamanan yang bertujuan untuk mengelola risiko, melindungi data sensitif, dan memastikan kerahasiaan, integritas, serta ketersediaan informasi (Folorunso et al., 2024). 3. Perilaku Keamanan (*Security Behaviour*): Perilaku keamanan merujuk pada tindakan dan kebiasaan pengguna yang mempengaruhi keamanan informasi	mencakup pemahaman tentang siapa yang bertanggung jawab atas keamanan informasi dalam organisasi. 2. Kepatuhan terhadap Aturan Keamanan (*Security Compliance*): Kesadaran dan kepatuhan individu terhadap aturan dan prosedur yang ditetapkan oleh organisasi terkait keamanan informasi. Termasuk kesadaran akan kewajiban untuk mematuhi kebijakan			

No	Variabel	Definisi Teori	Definisi Operasional	Alat dan Cara Pengukuran	Kriteria Objektif	Skala
		dalam organisasi (Safa et al., 2015). 4. Isu Lunak yang Bergantung pada Tempat Kerja (*Soft Issues - Workplace Independent*): Isu lunak dalam keamanan informasi mencakup elemen-elemen seperti manusia, organisasi, budaya, etika, kebijakan, dan hukum. Elemen-elemen ini sering kali diabaikan dalam definisi tradisional keamanan informasi yang lebih berfokus pada aspek teknis (Lundgren & Möller, 2017).	meskipun tidak selalu dapat mematuhinya sepenuhnya. 3. Perilaku Keamanan (*Security Behaviour*): Tindakan nyata yang diambil oleh individu untuk melindungi informasi yang mereka kelola, yang meliputi upaya untuk mencegah kebocoran data dan menghindari potensi ancaman. 4. Isu Lunak yang Bergantung pada Tempat Kerja (*Soft Issues - Workplace Independent*): Kesadaran			

No	Variabel	Definisi Teori	Definisi Operasional	Alat dan Cara Pengukuran	Kriteria Objektif	Skala
			individu tentang dampak yang dapat ditimbulkan oleh masalah keamanan informasi dan langkah-langkah yang dapat diambil untuk melindunginya. Kesadaran ini juga mencakup kesadaran tentang ancaman eksternal yang dapat memengaruhi keputusan terkait keamanan.			
2	Ekstrinsik	Faktor-faktor yang berasal dari luar individu yang mempengaruhi kesadaran terhadap keamanan informasi, seperti dukungan manajemen, kebijakan keamanan, dan lingkungan kerja.	Faktor ekstrinsik diukur melalui dukungan manajemen, pelatihan, serta adanya kebijakan keamanan informasi di rumah sakit. Indikator faktor ekstrinsik meliputi:	Kuesioner sebanyak 24 pertanyaan dengan pilihan jawaban:	Baik jika skor > mean. Kurang jika skor ≤ mean.	Likert

No	Variabel	Definisi Teori	Definisi Operasional	Alat dan Cara Pengukuran	Kriteria Objektif	Skala
		1. Pelatihan dan Kesadaran (*Training and Awareness*): Pelatihan dan kesadaran keamanan informasi melibatkan program yang dirancang untuk meningkatkan pengetahuan, sikap, dan perilaku karyawan terhadap praktik keamanan informasi yang baik. Program ini bertujuan untuk mengubah perilaku karyawan agar lebih waspada dan proaktif dalam menjaga keamanan data organisasi (Alkhazi et al., 2022; Stefaniuk, 2020) 2. Manajemen Operasional (*Operational Management*): Aktivitas	1. Pelatihan dan Kesadaran (*Training and Awareness*): Pelatihan dan Kesadaran merujuk pada upaya yang dilakukan oleh organisasi untuk mendidik dan memberi pemahaman kepada karyawan mengenai pentingnya keamanan informasi. Ini mencakup program-program pelatihan yang dirancang untuk meningkatkan kemampuan karyawan dalam mengidentifikasi potensi ancaman	4 = Sangat Setuju 3 = Setuju 2 = Tidak Setuju 1 = Sangat Tidak Setuju		

No	Variabel	Definisi Teori	Definisi Operasional	Alat dan Cara Pengukuran	Kriteria Objektif	Skala
		organisisasi untuk memastikan bahwa seluruh lingkungan komputasi dalam organisasi terlindungi dengan baik. Ini mencakup pengawasan dan pemeliharaan kebijakan keamanan informasi yang telah ditetapkan (White, 2009). 3. Budaya Organisasi (*Organizational Culture*): Budaya organisasi adalah sistem makna bersama yang dipegang oleh anggota organisasi yang membedakan satu organisasi dari yang lain. Ini mencakup asumsi dasar tentang dunia dan nilai-nilai yang membimbing kehidupan	terhadap keamanan informasi, serta kegiatan kampanye yang bertujuan untuk meningkatkan kesadaran tentang pentingnya menjaga informasi dengan cara yang aman dan sesuai dengan kebijakan perusahaan. 2. Manajemen Operasional (*Operational Management*): Meliputi tinjauan rutin terhadap sistem informasi, pelaksanaan audit (internal dan eksternal), serta peran kontrak			

No	Variabel	Definisi Teori	Definisi Operasional	Alat dan Cara Pengukuran	Kriteria Objektif	Skala
		dalam organisasi (Schneider et al., 2009). 4. Dukungan Manajemen Puncak (*Top Management Support*): Dukungan Manajemen Puncak melibatkan tindakan seperti penyediaan sumber daya, manajemen perubahan, dan berbagi visi untuk memastikan bahwa semua pihak dalam organisasi memiliki pemahaman yang sama tentang tujuan dan ideal dari sistem baru yang diimplementasikan (Dong et al., 2009) 5. Kemampuan di Tempat Kerja (*Workplace Capabilities*): Merupakan kemampuan yang dimiliki pekerja yang dipengaruhi oleh faktor	pihak ketiga dalam menjamin keamanan informasi. 3. Budaya Organisasi (*Organizational Culture*): Menilai sejauh mana karyawan memahami pentingnya keamanan informasi dan kemauan mereka untuk melindungi data sensitif. 4. Dukungan Manajemen Puncak (*Top Management Support*): Tingkat keterlibatan dan komunikasi pimpinan organisasi mengenai			

No	Variabel	Definisi Teori	Definisi Operasional	Alat dan Cara Pengukuran	Kriteria Objektif	Skala
		eksternal seperti kebijakan organisasi, hubungan sosial, dan lingkungan kerja yang mendukung atau menghambat pencapaian nilai-nilai kerja yang diinginkan (Abma et al., 2016) 6. Faktor Risiko dan Tindakan (*Risk and Response Factors*): Faktor Risiko dan Tindakan (*Risk and Response Factors*) dalam sistem keamanan informasi merujuk pada elemen-elemen yang dapat menyebabkan ancaman terhadap keamanan informasi dan langkah-langkah yang diambil untuk mengatasi ancaman tersebut. Faktor risiko mencakup berbagai aspek yang	pentingnya keamanan informasi, termasuk petunjuk yang jelas mengenai tindakan yang harus diambil oleh karyawan. 5. Kemampuan di Tempat Kerja (*Workplace Capabilities*): Adanya perjanjian yang mewajibkan kerahasiaan dalam kontrak kerja, hukum yang mewajibkan karyawan untuk mengikuti standar keamanan, dan pemeriksaan rutin terhadap sistem keamanan informasi untuk			

No	Variabel	Definisi Teori	Definisi Operasional	Alat dan Cara Pengukuran	Kriteria Objektif	Skala
		dapat mempengaruhi keamanan sistem informasi, sementara tindakan merujuk pada strategi yang diterapkan untuk mengurangi atau mengelola risiko tersebut (Feng et al., 2014). 7. Manajemen Perubahan (*Change Management*): Manajemen perubahan adalah proses membantu individu dan organisasi dalam transisi dari cara lama ke cara baru dalam melakukan sesuatu, termasuk dalam konteks sistem keamanan informasi (Lorenzi & Riley, 2003). 8. Kebijakan Keamanan Informasi (*Information Security Policies*): Kebijakan keamanan informasi adalah	mencegah kebocoran data. 6. Faktor Risiko dan Tindakan (*Risk and Response Factors*): Langkah-langkah yang diambil untuk menilai risiko sebelum mengambil keputusan, mengurangi ancaman, dan memberikan informasi kepada karyawan tentang aturan keamanan informasi serta sanksi untuk ketidakpatuhan. 7. Manajemen Perubahan (*Change Management*): Menyebutkan upaya organisasi			

No	Variabel	Definisi Teori	Definisi Operasional	Alat dan Cara Pengukuran	Kriteria Objektif	Skala
		dokumen yang mendefinisikan batasan dan pedoman untuk memastikan keamanan informasi dalam organisasi (Höne & Eloff, 2002)	untuk menyesuaikan sistem atau praktik yang ada untuk meningkatkan keamanan, termasuk edukasi kepada karyawan mengenai perubahan tersebut. 8. Kebijakan Keamanan Informasi (*Information Security Policies*): Kejelasan, penerapan, dan kemudahan implementasi kebijakan keamanan informasi di dalam pekerjaan sehari-hari.			

No	Variabel	Definisi Teori	Definisi Operasional	Alat dan Cara Pengukuran	Kriteria Objektif	Skala
3	Budaya Keamanan Informasi/ *Information Security Culture*	Budaya Keamanan Informasi (*Information Safety Culture*) adalah sub-kultur dalam organisasi yang berfokus pada perlindungan aset informasi melalui perilaku manusia yang terkoordinasi. Ini melibatkan norma, keyakinan, peran, dan praktik yang berkaitan dengan penanganan risiko dan bahaya informasi (Niekerk & Solms, 2010)	*Information Security Culture* diukur melalui tingkat kepatuhan karyawan terhadap kebijakan keamanan informasi, kesadaran akan ancaman, dan kepercayaan terhadap sistem keamanan informasi di rumah sakit. Indikator budaya keamanan informasi meliputi: 1. Kesadaran Ancaman. 2. Kepatuhan terhadap Kebijakan. 3. Pengorbanan untuk Keamanan. 4. Pemahaman terhadap Kebijakan. 5. Kepercayaan terhadap Kerahasiaan.	Kuesioner sebanyak 10 pertanyaan dengan pilihan jawaban: 4 = Sangat Setuju 3 = Setuju 2 = Tidak Setuju 1 = Sangat Tidak Setuju	Baik jika skor > mean. Kurang jika skor ≤ mean.	Likert

No	Variabel	Definisi Teori	Definisi Operasional	Alat dan Cara Pengukuran	Kriteria Objektif	Skala
			6. Dukungan Manajemen. 7. Efektivitas Inisiatif Kesadaran. 8. Arahan yang Jelas. 9. Keterlibatan Semua Pihak.			
4	*Information Security Awareness* (ISA)	*Information Security Awareness* adalah Kesadaran Keamanan Informasi (*Information Security Awareness* atau ISA) merujuk pada pemahaman individu tentang kebijakan dan prosedur keamanan informasi, sikap mereka terhadap pentingnya mematuhi kebijakan tersebut, dan perilaku aktual mereka dalam menerapkannya (McCormac et al., 2017)	*Information Security Awareness* diukur melalui tiga dimensi utama: pengetahuan, sikap, dan perilaku karyawan dalam menjaga keamanan informasi di rumah sakit.	Kuesioner sebanyak 9 pertanyaan dengan pilihan jawaban: 4 = Sangat Setuju 3 = Setuju 2 = Tidak Setuju 1 = Sangat Tidak Setuju	Baik jika skor > mean. Kurang jika skor ≤ mean.	Likert