Reliability Sistem Informasi Akuntansi (SIA); Faktor Penentu *Reliability* Sistem.

Ali Masjono Muchtar[1)], **Rahmanita Vidya Sari**[2)]**. Stefanus Heru Santoso** [3)]
[1,2]Jurusan Akuntansi.PNJ
ali.masjonouchtar@akuntansi.pnj.ac.id
[3)] KAP Stefanus Heru Santoso
sherusantoso@gmail.com

ABSTRACT

In producing an output, the accounting information system (AIS) will depend on Reliability of AIS System which supports the processes that occur in one or more of the applications used. These processes include computing, sorting, classifying, and summarizing. To guarantee that the process is accurate, precise, and error-free, a reliable accounting information system is needed. The aim of this research is to identify what factors or indicators that management needs to pay attention to ensure that AIS can produce accurate, precise, and trustworthy output. This research uses a literature study approach, meaning reviewing various literature related to System Reliability and identifying indicators to determine how to measure the reliability of a system. The results are indicators to identify whether the AIS is reliable or not to produce AIS's output.

Keywords : AIS, Reliability, System, output

ABSTRAK

Dalam menghasilkan suatu luaran, Sistem informasi akuntansi (SIA) akan bergantung kepada *System Reliability* SIA yang menopang proses yang terjadi di dalam salah satu aplikasi yang digunakan. Proses tersebut antara lain *computing, sorting, classifying, and summarizing*. Untuk menjamin bahwa proses tersebut akurat, tepat dan bebas kesalahan maka diperlukan suatu sistem informasi akuntansi yang reliabel. Tujuan dari penelitian ini adalah mengidentifikasi faktorlapa saja yang perlu diperhatikan oleh pihak manajemen agar SIA dapat menghasilkan luaran yang akurat, tepat dan dapat dipercaya. Penelitian ini menggunakan pendekatan studi literatur, artinya mereview berbagai literatur terkait *System Reliability* dan mengidentifkasi indikator apa yang perlu diperhatikan oleh manajemen untuk menentukan bagaimana cara mengurkur reliability suatu sistem. Hasil dari penelitian indikator digunakan untuk mengukur *system reliability*.

Kata Kunci: SIA, Reliabiltiym System, output.

PENDAHULUAN

Latar Belakang

Perkembangan sistem informasi dan komunikasi telah membawa suatu organisasi atau perusahaan kepada pada ketergantungan yang sangat tinggi terhadap keandalan sistem informasi tersebut. Seberapa besar organisasi bergantung tersebut yang didapatnya dari sistem informasi yang tersedia, jika sistem informasi tidak dapat menyediakan informasi yang dapat diandalkan dapat diartikan bahwa sistem tersebut tidak berguna atau pertanyaan sederhananya adalah mengapa menggunakan sistem informasi jika tidak dapat menyediakan informasi pada saat dibutuhkan. (Theintactone, 2019)

Efisiensi sistem informasi ditentukan oleh kemampuan informasi ketika dibutuhkan, Sistem informasi disuatu organisasi dioperasikan menggunakan *single system* atau *multipel System* untuk mendukung operasional organisasi, maka efisiensi sistem informasi tersebut dapat mendukung operasional setiap level organisasi. Selanjutnya, sistem informasi tersebut dapat membantu memenangkan

persaingan bisnis dimana organisasi menghadapi berbagai tantangan dari organisasi lain, sistem informasi dapat membantu untuk memenangkan persaingan dengan menyampaikan "*Competitive Report*" kepada para pesaing. (Theintactone, 2019)

Situasi terkini banyak organisasi beralih menggunakan *cloud computing*, paling tidak sebagian kecil dari proses yang terjadi di organisasi menggunakan *system cloud*. Disisi lain pihak manajemen ingin kepastian bahwa informasi yang dihasilkan oleh SIA dapat dipercaya dan reliability dari *system cloud* sangat baik dalammenopang SIA. Lebih jauh manajemen juga ingin kepastian bahwa organisasi patuh dengan perubahan peraturan dan persyaratan industri yang selalu terjadi, sehingga menimbulkan tingkat Kepercayaan yang baik terhadap SIA yang digunakan oleh organisasi.

Dalam beberapa katagori, sistem informasi dioperasikan hampir 100% oleh kemampuan peralatan, mesin dan berbagai aplikasi pendukung. Disini terlihat bahwa ketergantung kepada peralatan tersebut sangat tinggi. Secara kasat mata pengguna sistem tersebut dapat melihat, merasakan, menghitung ulang pekerjaan mesin tersebut. Namun disisi lain ada beberapa faktor yang tingkat *reliability* menurun karena usia peralatan dan membutuhkan perawatan, adanya proses yang menggantung (hang), disini campur tangan manusia masih diperlukan.

Disatu sisi SIA yang digunakan oleh suatu organisasi mampu memenuhi tuntutan manajemen dan publik untuk menyajikan laporan keuangan secara akurat, tepat waktu dan dapat dipercaya. Semua proses persiapan laporan keuangan tersebut diserahkan kepada mesin atau sistem informasi yang handal diorganisasi tersebut. Disisi lain kehandalan system tersebut sangat bergantung kepada kemampuan staff IT dan peralatan yang digunakan untuk mengoperasikan sistem informasi dan memaintain peralatan yang ada.

Reliabilty system informasi bertumpu kepada hubungan antara faktor berikut ini; *Security, Confidentiality, Privacy, Processing Integrity, Availability*, kelima variable tersebut disebut *Five Trust Services Principles for System reliability* (Romney & Steinbart, 2017).

Permasalahan

Dalam operasional sehari hari, manajemen bergantung kepada SIA yang digunakan dan kemampuan staf teknologi informasi dalam meyakinkan bahwa SIA yang digunakan masuk dalam katagori reliabel dan mampu menghasilkan luaran yang akurat, valid dan bebas dari kesalahan. Untuk itu permasalahan yang ingin dicapai adalah indikator apa yang telah diterapkan di perusahaan dan apakah indikator tersebut telah terpenuhi oleh perusahaannya.

Tujuan

Mengindentifikasi dan menentukan derajad reliability masing masing indikator yang dihasilkan. Dengan menggunakan indikator tersebut maka pihak manajemen bisa yakin bahwa SIA yang digunakan masuk dalam katagori reliable dalam menghasilkan luaran.

TINJAUAN PUSTAKA

Perkembangan yang terus menerus dibidang teknologi telah meningkatkan kebutuhan akan metodologi dan alat untuk menilai kinerja sistem informasi dalam hal *reliability, Conformance*, dan *Quality of service.* (Petrov, 2022) menjelaskan bahwa dari sudut metodologi memperlakukan data atau informasi yang dipandang dari sudut propabilitas terhadap komponen sistem informasi untuk memberikan jasanya. Pertama dipandang dari konsep ***entropi-***– untuk mengukur secara langsung keanekaragaman, persaingan, ketidakpastian; kedua, ***konsentrasi (hierarki)*** – untuk mengukur keteraturan, dominasi, dan kepastian secara langsung. (Petrov, 2022).

Lebih jauh dijelaskan bahwa *reliability system* adalah property sistem informasi yang terukur, berguna dan terkontrol. Berguna bagi manajemen untuk mendukung proses pengambilan keputusan. Manajemen perlu mengidentifikasi potensi masalah yang secara langsung terkait dengan efisiensi sistem semua komponen pendukung sistem informasi. *Reliability system* informasi dapat dikembangkan berdasarkan teori Delone dan Mcclean, Model Lyytinen dan Technology Acceptance model. (Tworek, 2022).

Reliability suatu sistem dapat diartikan sebagai sistem yang digunakan oleh suatu organisasi berfungsi sesuai dengan kebutuhan pengguna, misalnya manajemen dan pelanggan, stakeholder lainnya. Jika pelanggan senang dengan *Relibility system* yang digunakan oleh organisasi akan membawa kebaikan bagi organisasi. Organisasi dapat

menetapkan bahwa *system reliability* adalah sesuatu yang penting dalam rangka menyenangkan pelanggan. (Sevim & Hall, 2014). Untuk menentukan system reliability, menurut Romney dan Steinbert (Romney & Steinbart, 2017) dapat menggunakan konsep *Five Trust Services Principles for System reliability.*

Reliabilty system informasi bertumpu kepada hubungan antara variable/faktor berikut ini; *Security, Confidentiality, Privacy, Processing Integrity, Availability*, kelima variable tersebut disebut *Five Trust Services Principles for System reliability* (Romney & Steinbart, 2017).

Untuk meyakinkan bahwa suatu sistem *reliable* atau tidak maka dalam perspektif manajemen perlu mengetahui apakah sistem *security* yang ada hanya dapat di akses oleh orang yang berhak (*Controlled and restricted to legitimate user).* Manajemen di satu sisi hanya tahu bahwa ada sistem kendali yang ketat dan apakah semua pegawai sudah menyadari hal ini dan melakukan tindakan pencegahan terhadap upaya-upaya aksen oleh yang berhak (*unauthorize access*). *Confidentiality, privacy, processing integrity* dan *availability* semua dapat dikatorikan kedalam security.

Security dalam hal ini memastikan bahwa SIA yang digunakan tetap aman dan berguna. *Security* pada dasarnya memastikan akses ke SIA (data, informasi, asset informasi, saluran komunikasi) baik secara pisik (*physical access*) ketempat penyimpanan asset infromasi, secara non pisik (*logical access*) ke tempat pemyimpanan data, baik disimpan di local maupun disimpan di sistem *cloud* melalui berbagai aplikasi yang digunakan. (Ousley, 2013).

Data dan informasi perusahaan adalah asset yang paling berharga diantara asset-aset sistem informasi lainnya. Untuk menjamin adanya *system reliability* data tersebut, organisasi wajib mengelola, mengamankan dan memberikan otorisasi hanya kepada orang orang yang berhak saja (*authorize person only*).

Confindetility menjaga agar informasi sensitip milik perusahaan harus dijaga dari akses penggunan yang tidak berhak. (*Unauthorize disclosure*). Ini berarti bahwa semua informasi mengenai pegawai, pelanggan, keuangan, produk, merek dagang hanya dapat di akses oleh orang orang yang diberihak. Hal ini berarti perlu diterapkannya peraturan dan prosedur agar *confidentiality* terjaga.

Privacy dalam kontek ini organisasi wajib menjaga informasi pelangan, pegawai, rekanan yang telah dikumpulkan, digunakan, diekpos dan di maintenan hanya untuk kepentingan organisasi sesuai dengan kebijakan internal organisasi tersebut.

Data yang di gunakan organisasi perlu memastikan bahwa *Processing Integrity* sesuai dengan kebijakan perusahaan. Data hendaknya diproses secara akurat, lengkap, tersedia setiap waktu dan diolah oleh hanya orang yang diberi hak.

Ketersediaan (*availability*) informasi yang dihasilkan oleh sistem informasi sesuai dengan kebutuhan operasional dan kewajiban-kewajiban sesuai dengan peraturan yang berlaku.

Mengukur *System Reliability* adalah sesuatu yang penting (Klos & Ryszard, 2015) karena akan mempengaruhi pengambilan keputusan. Setiap kuputusan yang diambil selalu berdasarkan data terkini (*updated*). Organisasi bergantung kepada sistem informasi yang digunakan agar data selalu *up-to-date.* Agar yakin *reliability system* yang digunakan disaran untuk melakukan sendiri proses pengukuran (Klos & Ryszard, 2015)

Pengkuran menggunakan konsep *security maturity model* (Al-Matari, Helal, Mazen,, & Elhennawy, 2021). Model ini membagi organisasi menjadi lima level *security maturity model*. Level 0 adalan *nonexistence* dimana pada level ini dapat dikatakan pengendaliannya tidak ada (*lack of control*). Level 1 *adhoc* pengendaliannya dapat dikatakan sangat lemah atau buruk. Level 2 *repeatable* yang menandakan adanya kepedulian terhadap pengendalian. Level 3 *defined* yang ditandai dengan memulai pengendalian otomatis. Level 4 *managed* yang ditandai adanya atau organisasi telah memulai pengembangan bentuk dan jenis pengendalian dan level 5 *optimized*, organisasi telah menerapkan pengendalian yang otomatis.

Pengukuran *system reliability* dapat juga menggunakan metode Gage R&R (Kios, 2015). Metode ini menggunakan *Stochastic Method* dimana dalam mencari berbagai variasi masalah *reliability* dilakukan secara random untuk menentukan distribusi atau pattern yang mungkin mengindikasikan adanya kelemahan pada suatu sistem yang secara statistik diukur

dan dianalisis, Hasil bisa saja akurat atau tidak akurat.

Confidentiality artinya memprotek informasi agar orang orang tertentu dan yang diotorisasi saja yang dapat mengakes informasi tersebut. Informasi perusahaan memiliki nilai yang sangat tinggi hal ini didukung oleh ketentuan dan peraturan yang disahkan oleh manejemen dan dipatuhi oleh staff yang mengelola informasi. Seiring kemajuan teknologi seperti sekarang ini, informasi mengenai rekening bank nasabah, nomor kartu kredit, rahasia dagang, dokumen rahasia pemerintah perlu diprotek agar tidak jatuh ketangan orang orang yang tidak bertanggungg jawab. (Chia, 2016). Melindungi kerahasiaan bergantung pada penetapan dan penerapan tingkat akses yang sesuai untuk informasi. Dalam penerapannya sering kali melibatkan pemisahan informasi ke dalam kumpulan terpisah yang diatur oleh siapa yang seharusnya memiliki akses ke informasi tersebut dan seberapa sensitifnya (apotheon, 2008) Dalam kontek penelitian ini, manajemen perlu tahu sejauh mana informasi tersebut terlindung dan dapat dijaga dengan baik. Salah satu metode yang banyak digunakan antara lain menggunakan menerapkan metode enkripsi terhadap data yang disimpan.

Privacy artinya informasi sensitip mengenai seseorang perlu dijaga dan tidak boleh diekpos ke public. Untuk menjaga hal ini perusahaan perlu menetapkan prosedur dan aturan yang ketat dan dipatuhi oleh semua yang berkaitan dengan informasi sensitip. Dalam penelitian ini instrument yang hendak dibuat dapat mengetahui bahwa masalah *privacy* telah diimplementasikan sesuai dengan ketentuan perusahaan.

Dalam kontek *processing Integrity*, organisasi harus memiliki tingkat keyakinan bahwa data diproses secara akurat, lengkap dan dapat tersedia setiap saat untuk pengguna yang telah di otorisasi (Romney & Steinbart, 2017). Kata kunci dalam masalah *processing integrity* adalah melindungi data dari modifikasi atau penghapusan oleh pihak yang tidak berwenang, dan memastikan bahwa ketika orang yang berwenang membuat perubahan yang seharusnya tidak dilakukan, kerusakan dapat dibatalkan. (apotheon, 2008)

Untuk itu organisasi yakin bahwa data yang terdistribusi dapat diintegrasikan menjadi satu kesatuan yang utuh dan dapat memberikan informasi yang akurat. Implementasi *processing integrity* ini menjadi sangat krusial karena data suatu organisasi yang datanya terdistribusi, menghendaki suatu proses yang cepat (*Communication*), data tersimpan di database yang memiliki relasi yang ketat (*relationship*). Menggunakan sistem enkrisp dalam penyimpanan dan dalam transportasi, memilik hak *access* yang sesuai dengan level kewajiban. (Weber, 1999)

Dalam kontek *Availability*, organisasi harus memiliki tingkat keyakinan tinggi bahwa sistem yang digunakan tersedia setiap saat dan sesuai dengan kebutuhan operasional. Untuk jenis organisasi tertentu *availability* harus menerapkan skema 24/7, artinya system harus dapat diakses oleh pelanggan 24 jam dan 7 hari dalam satu minggu. Contohnya Bank, Toko online dan lain lain. Untuk meyakinkan hal ini *Information System Management* (IMS) harus yakin bahwa ketersediaan data, operasional sistem, saluran akses, serta mekanisme otentikasi, semuanya harus berfungsi dengan baik agar informasi yang mereka berikan dan lindungi tersedia saat dibutuhkan.

Konsep CIA triad menjelaskan bahwa tiga serangkai; *Confidentiality, Integrity dan Availablity*. Konsep ini menjelaskan model keamanan sistem informasi yang dikembangkan untuk membantu Information System Management (IMS) dalam membuat kebijakan keamanan sistem informasi guna mengidentifikasi area bermasalah dan mencari solusi yang diperlukan. (apotheon, 2008)

Nilai informasi adalah *Slippery Concept*, karena informasi tidak memiliki nilai universal, sangat bergantung kepada siapa yang menggunakan, kapan dan untuk apa. Setiap evaluasi terhadap informasi berhubungan dengan nilai yang diberikan ketika pengambilan keputusan. (Thakur, 2023).

Beberapa riset melihat nilai informasi dari berbagai sudut pandang. Riset yang menggunakan berbagai variabel untuk menentukan sukses (reliable) atau tidaknya suatu sistem informasi menggunakan variabel *System Quality, Information Quality, Use, User Satisfaction* serta efeknya kepada individu dan dampaknya kepad perusahaan. (Petter, DeLone, & McLean, 2008). Lebih dijelaskan oleh (Petter, DeLone, & McLean, 2008) bahwa SERVQUAL yang banyak digunakan dalam penelitian marketing juga digunakan untuk mengukur. SERVQUAL digunakan untuk mengukur *Quality IT Department* dengan mengukur dan membandingkan ekspektasi

pengguna dan persepsi terhadap *Quality IT Department.*

METODOLOGI

Penelitian ini menggunakan metode kualitatip yang mendeskriskan dan memahami fenomena tentang apa yang dialami oleh objek penelitian misalnya perilaku, persepsi, motivasi, tindakan, secara holistik dan tetap didukung oleh metode ilmiah. Dalam kontek penelitian ini, mendeskripsikan dan memahami adanya kebutuhan pihak manajemen suatu organisasi akan *system reliability.*

Berdasarkan paragraph diatas maka objek penelitian ini adalah *Information System Management* yang digunakan oleh suatu organisasi. Sub-objek yang dijadikan sasaran pengukuran reliabilitas adalah sudut *Security*, *Confidentiality*, *Privacy*, *Processing Integrity*, *Availability* (Romney & Steinbart, 2017). Indikator masing variabel akan ditentukan dalam penelitian yang kemudian dijadikan sebagai penentuan *reliability system*.

Untuk itu dalam melaksanakan penelitian ini digunakan *Focus Group Discussion* (FGD), dengan fokus pembahasan *Reliability system*. Metode wawancara digunakan untuk mendapatkan realitas implementasi sistem informasi di perusahaan yang menjadi rekanan mitra dan terhadap kasus dan atau study pustaka yang berkaitan dengan *reliability System*. FGD dilakukan untuk memperdalam berbagai kasus dan pustaka yang ada diantara tim penelitian dan mitra. Observasi dilakukan dengan melakukan pengamatan mendalam terhadap suatu organisasi yang telah dianggap mapan dalam *reliability system*. Survei dilakukan kepada beberapa perusahaan yang menjadi mitra dengan menggunakan alat atau instrument yang telah dikembangkan

Hasil FGD berupa indikator, kemudian indikator ini dijadikan penentukan *reliability system*. Hasilnya berupa katagorisasi sistem reliabilitas sistem informasi yang digunakan oleh organisasi dan memberikan solusi atau tindakan lanjutan yang diperlukan agar sistem informasinya masuk dalam katagori reliabel.

Tabel 1 Tahapan Penelitian

Tahap	Kegiatan	Hasil
1	Perancangan kerangka utama faktor faktor penentu system reliability; FGD dan Study Literatur Review	Faktor faktor penentu sistem reliability
2	Penyempurnaan faktor penentu dan pengelompkan kedalam *Five Trust Services Principles for System reliability* (Romney & Steinbart, 2017)	Hasil pengelompokan
3	FGD, survei, wawancara dengan mitra, dalam hal ini KAP Stefanus Heru Santoso	Perstujuan bentuk umum instrument
4	Pengkategorian faktor	Draf
5	Diskusi pengunaan instrument dengan Mitra	Masukan mitra
6	Finalisasi	publikasi

Sumber: OlahanTim Peneliti 2023

HASIL DAN PEMBAHASAN

Pembahasan ini bertumpu kepada konsep *Five Trust Services Principles for System reliability* (Romney & Steinbart, 2017). Dari konsep ini kemudian dijabarkan berbagai indikator yang mengindikasikan bahwa disuatau organisasi telah menerapkan prinsip tersebut.

Meningkatnya ancaman SIA terjadi karena sistem client/server mendistribusikan data ke banyak pengguna, itulah sebabnya sistem ini lebih sulit dikendalikan dibandingkan sistem komputer utama yang terpusat dan informasi tersedia bagi pekerja yang kurang baik.

Untuk mengamankan sistem dan informasi, setiap perusahaan atau organisasi harus menganalisis jenis ancaman yang akan dihadapi dan bagaimana pengaruh ancaman tersebut terhadap keamanan sistem informasi. Ancaman utama adalah *unauthorize access*, baik *physical access* atau *logical access*.

Untuk mengendalikan akses secara ilegal maka organisasi memiliki kendali terhadap hal ini berikut indikator bahwa *unauthorize access* telah ada bentuk pengendalian.

Security

Security adalah pengendalian dasar yang harus ada di SIA. Masalah *security* terkait dengan kemampuan bisnis yang kritis dan perlu diselaraskan dengan harapan dan budaya perusahaan. Dalam hal ini adalah memberikan kepemimpinan dan wawasan untuk mengidentifikasi risiko dan menerapkan kontrol yang efektif dan menyelaraskan kebutuhan keamanan informasi dengan tujuan bisnis harus menjadi prioritas utama.

Security adalah proteksi, dengan kemajuan teknologi informasi seperta saat ini, *security* menjadi pondasi dalam membangun, mengembangkan dan menggunakan SIA karena *security* sebagai perlindungan informasi dan elemen pentingnya, termasuk sistem dan perangkat keras yang menggunakan, menyimpan, dan mengirimkan informasi.

Akses oleh pengguna yang tidak berhak adalah pengendalian utama untuk SIA, dengan pemberian hak akses kepada orang orang tepat maka SIA akan aman dan berguna.

Dari tabel berikut terindikasi indikator yang perlu dipenuhi agar masalah *security* pada SIA dapat memenuhi sebuah sistem yang *reliable.*

Tabel 2 Pengendalian dan Pembatasan Akses Ke Aplikasi, Data dan Sumber Daya Lainnya.

No	Indikator
1	Memiliki kebijakan dan prosedur mengenai akses ke SIA dan didokumentasikan dengan baik
2	Menerapkan kombinasi Password yang rumit dan tersistem
3	Menerapkan sistem dua media atau lebih untuk authentikasi setiap perubahan hak akses atau setiap adanya pengguna baru.
4	Menerapkan sistem seleksi user yang tersistem/penentuan user
5	Menggunakan *User Matrix Control* untuk mengendalikan akses
6	Menerapkan sistem enksrip saat akses ke sistem perangkat keras dan ke aplikasi
7	Menerapkan sistem enkripsi pada media penyimpanan, baik di server perusahaan atau di media backup.
8	Menerapkan jenjang supervisi jika terjadi perubahan otorisasi (setiap perubahan harus diketahui oleh atasan langsung secara berjenjang)
9	Menerapkan cara pembatasan acess ke komputer dengan ketat dan konsisten.
10	Menerapkan kombinasi password yang kuat untuk memasuki acess ke sistem informasi.
11	Menerapkan perubahan password dilakukan secara berkala.

Sumber: Hasil olahan tim peneliti. 2023

Confidentiality

Satu organisasi atua perusahaan mengumpulkan, menyimpan dan menggunakan data para pelanggan, pegawai, rekanan dan data lainnya yang dapati di klasifikasikan sebagai data sensitif. Perusahaan wajib memberikan perlindungan terhadap data tersebut untuk menjadi bahwa data tersebut digunakan untuk keperluan lain.

Tabel 3 menjelaskan indikator penerapan yang dilakukan oleh perusahaan dalam upaya menyediakan tingkat *confidentiality* yang tinggi.

Tabel 3 Pengendalian yang Dapat Digunakan Untuk Melindungi Kerahasiaan Informasi Organisasi

No	Indikator
1	Memiliki kebijakan dan prosedur mengenai perlindungan kerahasiaan informasi, kerahasiaan kekayaan intelektual dan informasi bisnis sensitif.
2	Menentukan lokasi penyimpanan informasi dan menentukan siapa yang berhak akses ke lokasi penyimpanan (semua data storage)
3	Pengelompokan informasi berdasarkan Nilai dari informasi tersebut, misalnya mana informasi yang boleh diakses publik dan mana yang tidak boleh.
4	Menerapkan sistem enkripsi dan membatasi akses terhadap semua informasi sensitip.
5	Menerapkan kontrol yang ketat menggunakan konsep Information Right Management) yang dapat membatasi hak akses, misalnya Read, Modify, copy, print, download, dll)
6	Menerapkan pencegahan kehilangan data (Data Loss Prevention). Yang dapat memblokir pesan keluar (email, pesan instan, dll.) yang berisi kata kunci atau frasa yang terkait dengan kekayaan

	intelektual atau data sensitif lainnya yang ingin dilindungi oleh organisasi.
7	Memasang watermark pada setiap informasi yang dikatagorikan sensitif.
8	Memberitahu pegawai tentang confidentiality melalui pelatihan. Dengan pelatihan yang tepat, karyawan dapat memainkan peran penting dalam melindungi kerahasiaan informasi organisasi dan meningkatkan efektivitas

Sumber: Hasil olahan tim peneliti. 2023

Privacy

Perusahaan mengendalikan privasi terhadap data atau data individu untuk menyembunyikan informasi, pemikiran, keyakinan, tindakan, dan data pribadi tertentu tentang dirinya dan urusannya dari orang lain.

Tabel 4 Pengendalian terhadap data yang dikumpulkan oleh perusahaan

No	Indikator
1	Memiliki kebijakan dan prosedur mengenai privacy semua data yang dikumpulkan, disimpan dan digunakan.
2	Memberi tahu pelanggan bahwa perusahaan akan mengumpulkan data pribadi dan menjelaskan alasan pengumpulan data tersebut.
3	Perusahaan memberikan pilihan bagaimana data mereka diperlakukan
4	Perusahaan hanya mengumpukan data yang dibtuhkan saja untuk memenuhi tujuan perusahaan.
5	Perusahaan harus menggunakan data pelanggan hanya untuk kepentingan perusahaan yang telah di tuliskan di privacy policy. Perusahaan menyimpan data tersebut sepanjang untuk kegiatan bisnis yang sah.
6	Perusahaan menyediakan akses untuk mereview hanya kepada yang diberikan otorisasi.
7	Perusahaan dapat membuka data pelanggan kepada pihak ketiga sesuai dengan ketetapan yang telah digariskan pada Privacy Policy
8	Perusahaan harus mengambil langkah untuk memproteksi dari kehilangan dan akses oleh orang yang tidak berhak
9	Perusahaan harus memaintain integritas data pelanggan untuk memastikan akurasi informasi pelanggan.
10	Perusahaan harus menunjuk seseorang atau lebih pegawai yang bertanggung jawab atas implementasi Privacy Policy.

Sumber; Hasil olahan tim penelitian. 2023

Processing Integrity

Integritas proses yang dilaksanakan menjadi perhatian utama dalam mendukung *system reliability*. Untuk itu perusahaan hendaknya memiliki dan menerapkan indikator agar informasi yang dihasilkan SIA valid, lengkap dan akurat.

Tabel 5 menjelaskan penerapan integritas proses yang menjelaskan bahwa indikator ini menjadi indikator terlaksananya processing integrity.

Tabel 5 Pengendalian pada semua aplikasi yang digunakan terkait integrasi input, proses dan ouput

No	Indikator
1	Memiliki kebijakan dan prosedur mengenai integritas proses yang ada di perusahaan dan didokumentasikan dengan baik
2	Memastikan bahwa setiap aplikasi yang digunakan dapat memproses data secara akurat, lengkap, tepat waktu, dan hanya dengan otorisasi yang sesuai.
3	Memastikan bahwa data yang diproses oleh setiap aplikasi adalah data yang valid, diotorisasi, lengkap dan akurat.
4	Memastikan setiap kesalahan yang terjadi sebelum data diproses sudah diperbaiki sebelum dilanjutkan.
5	Memastikan bahwa luaran setiap aplikasi telah direview dan direkonsiliasi, menerapkan sistem enkripsi untuk setiap luaran atau proteksi terhadap luaran.

Sumber: Olahan tim Peneliti. 2023

Availability

Availability menjadi salah satu tonggak untuk *system reliability*. Dengan menerapkan indikator ini maka perusahaan menjadi lebih yakin bahwa ketersediaan informasi sepanjang waktu menjadi lebih meyakinkan.

Tabel 7 menjelaskan indikator untuk *availability* yang dapat atau telah diimplementasikan oleh perusahaan untuk menjadi proses bisnis tetap beroperasi sepanjang waktu agar tidak menimbulkan kerugian finansial atau kerugian lainnya.

Tabel 6 indikator proses bisnis tetap beroperasi sepanjang waktu guna menjamin availably informasi.

No	Indikator
1	Memiliki kebijakan dan prosedur mengenai ketersediaan SIA untuk keberlanjutan aktivitas perusahaan.
2	Penerapan *system downtime* untuk meminimumkan gangguan operasional dengan cara preventif. Misal memiliki Uninterruptible Power Supply (UPS). System fault tolerance, Penggunaan software berlisensi dan Pelatihan pengguna,
3	Memiliki system backup dan recovery yang terdokumentasi dan terupdate secara reguler
4	Memiliki system disaster recovery planning yang terdokumentasi dan terupdate secara reguler
5	Memiliki business continuity plan yang terdokumentasi dan terupdate secara reguler

Sumber: Hasil olahan tim peneliti 2023

System reliability menjadi instrumen bagi manajemen untuk mengetahui apakah SIA yang digunakan dalam proses bisnis telah dapat memberikan hasil yang optimal.

Pondasi dari *system reliability* ini ada *security*, dengan kuatnya sistem keamanan; akses pisik dan akses non pisik menjadi landasan bagi *system reliability*. Jika terjadi kelamahan pada system akses maka SIA akan menjadi sasaran empuk bagi para *hacker* untuk menyusup ke SIA. Jika indikator yang ada di tabel 2 diterapkan oleh perusahaan maka dapat dikatakan bahwa *security* SIA, minimum SIA sudah memenuhi kriteria aman dan berguna.

Tonggak pertama dari system reliability adalah *confidentiality*. Indikator yang terindentifkasi pada penelitian ini menjadi kriteria apakah perusahaan sudah memiliki sistem *confidentiality* yang kuat untuk menjamin telah terjadi penjaminan kerahasiaan data dan informasi.

Tonggak kedua adalah *privacy*. Perusahaan yang menggunakan SIA dapat memberikan jaminan bahwa data yang dikumpulkan, digunakan dan disimpan hanya untuk kepentingan perusahaan. Tabel 3 memberikan kriteria apakah perusahaan telah memenuhi kriteria penrapan *system privacy* dengan baik.

Tonggak ketiga adalah processing integrity. Untuk menjamin bahwa SIA menginput, memproses dan menghasilkan luaran maka kriteria yang tertera pada tabel 4.

Tonggak keempat adalah untuk menjamin *system reliability* ada di tabel 6. Indikator yang ada di tabel 6 penerapannya akan menjadi kriteria bahwa keberlanjutan layanan SIA akan tetap terjaga dengan bai.

KESIMPULAN

System reliability memiliki satu pondasi yaitu *security* dan dan empat tonggak pendukung yaitu *Confidentiality, Privacy, Processing Integrity* dan *Availabity*. Kombinasi dari semua faktor ini menjadi faktor utama dalam menyediakan SIA yang dapat dipercaya, tetap aman dan berguna.

Indikator-indikator yang ada di tabel 2 sampai tabel 6 dapat diterapkan oleh perusahaan dengan memberikan bobot kepada masing-masing indikator. Bobot berupa angka, dimana angkat 5 mencerminkan situasi yang paling ideal dan SIA dalam kondisi yang sangat reliable.

KETERBATASAN

Banyak studi mengenai *system reliability* yang telah dilakukan. Pengguna dapat menambah kekurangan yang ada pada penelitian ini dari peneliti lain untuk memperkuat hasil penelitian ini, misalnya ada tonggak *system reliability* yang tidak teridentifikasi pada penelitian dapat dikombinasi untuk memperkuat *system reliability.*

REFERENCES

Al-Matari, O. M., Helal, I. M., M. S., & Elhennawy, S. (2021). Adopting security maturity model to the organizations' capability model. *Egyptian Informatics Journal, 22*, 193-199. Retrieved from www.sciencedirect.com

apotheon. (2008, June 30). *The CIA Triad*. (TechRepublic) Retrieved April 6, 2022, from TechRepublic: https://www.techrepublic.com/article/the-cia-triad/

Chia, T. (2016, Februari). *IT Security Community Block*. (IT Security Community Block) Retrieved Februari 4, 2022, from https://security.blogoverflow.com/

Kios, R. (2015). MEASUREMENT SYSTEM RELIABILITY ASSESSMENT. *Journal of Polish Hyperbaric Medicine and Technology Society, 51*(2), 31-46. doi: 10.1515/phr.2015-009

Klos, & Ryszard. (2015, May). Measurement System Reliability Assessment. *Polish Hyperbaric Research 51(2), 52*(2). doi:10.1515/phr-2015-0009

Ousley, M. R. (2013). *Information Security; The Complete Reference* (Second Editon ed.). NewYork: The McGraw-Hill Companies.

Petrov, I. (2022). Information Systems Reliability in Traditional Entropy and Novel Hierarchy. *Cybernetics and Information Technologies,22(3) 3-17.*, *22*(3), 3-17. doi:https://doi.org/10.2478/cait-2022-0024

Petter, S., DeLone, W., & McLean, E. (2008). Measuring information systems success: models, dimensions, measures, and interrelationships. *European Journal of Information Systems*, 236-263. doi:https://doi.org/10.1057/ejis.2008.15

Romney, M. B., & Steinbart, P. J. (2017). *Accounting Information System.* Pearson.

Sevim, N., & Hall, E. E. (2014). Consumer Trust Impat on Online Shoping. *Internet Application and Management, 5*(2). doi:DOI: 10.5505/iuyd.2014.41636

Thakur, D. (2023). *Value of Information in Management Information System.* Computer Ntes. Retrieved from https://ecomputernotes.com/mis/what-is-mis/value-of-information#google_vignette

Theintactone. (2019, 9 3). *Evaluation of information system*. Retrieved from Theintactone: https://theintactone.com/2022/03/06/evaluation-of-information-systems/

Tworek, K. (2022). Reliability of information systems in organization in the context of banking sector: Empirical study from Poland. *European Journal of International Management, 2*(3). doi:https://doi.org/10.1080/23311975.2018.1522752

Weber, R. (1999). *Information.* NJ 07458: Prentice Hall.