KEMENTERIAN AGAMA R.I
UNIVERSITAS ISLAM NEGERI AR-RANIRY BANDA ACEH
LEMBAGA PENELITIAN DAN PENGABDIAN KEPADA MASYARAKAT
Jl. Syeikh Abdur Rauf, No. 1 Gedung Museum Lt. 1, Kopelma Darussalam Banda Aceh, 23111
Telp.: 0651-7552921, Fax. 0651-7551857
Email: lp2m@ar-raniry.ac.id; Situs: http://lp2m.uin.ar-raniry.ac.id

SURAT KETERANGAN

Nomor : 29/Un.08/LP2M.1/TL.0.1/02/2024

Kepala Pusat Penelitian dan Penerbitan (Puslitpen), Lembaga Penelitian dan Pengabdian kepada Masyarakat (LP2M) UIN Ar-Raniry Banda Aceh dengan ini menerangkan bahwa identitas di bawah ini:

Nama	: Rika Yuliana
Pekerjaan	: Dosen Tetap UIN Ar-Raniry Banda Aceh
NIP/ NIDN	: 198407132014032001/ 2013078403
Fakultas/ Program Studi	: Sains dan Teknologi/ Teknologi Informasi

Benar telah melakukan penelitian mandiri di tahun 2023 dengan judul ***Best Practice framework for Information Technology Security Governance in Indonesian Government***.

Demikian Surat Keterangan ini dibuat untuk dipergunakan sebagaimana mestinya.

Banda Aceh, 15 Februari 2024
a.n. Ketua LP2M
Kepala Pusat Penelitian dan Penerbitan

Anton Widyanto

No. Reg:

LAPORAN PENELITIAN

Best Practice Framework For Information Technology Security Governance In Indonesian Government

Ketua Peneliti

Rika Yuliana, M.T
NIDN: 2013078403
NIPN: -

Anggota:
-

Klaster	**-**
Bidang Ilmu Kajian	**Sains dan Teknologi**
Sumber Dana	**Mandiri**

PUSAT PENELITIAN DAN PENERBITAN
LEMBAGA PENELITIAN DAN PENGABDIAN KEPADA MASYARAKAT
UNIVERSITAS ISLAM NEGERI AR-RANIRY BANDA ACEH
JANUARI 2024

LEMBARAN IDENTITAS DAN PENGESAHAN LAPORAN PENELITIAN
PUSAT PENELITIAN DAN PENERBITAN LP2M UIN AR-RANIRY BANDA ACEH
TAHUN 2024

1. a. Judul : Best Practice Framework for IT Security Governance in Indonesian overnment
   b. Klaster :
   c. No. Registrasi :
   d. Bidang Ilmu yang diteliti : Teknologi Informasi

2. Peneliti/Ketua Pelaksana
   a. Nama Lengkap : Rika Yuliana
   b. Jenis Kelamin : p
   c. NIP *(Kosongkan bagi Non PNS)* : 198407132014032001
   d. NIDN : 2013078403
   e. NIPN (ID Peneliti) :
   f. Pangkat/Gol. : Penata/ IIIc
   g. Jabatan Fungsional : Lektor
   h. Fakultas/Prodi : Fakultas Sains dan Teknologi/ Teknologi Informasi

   i. Anggota Peneliti 1
      Nama Lengkap : -
      Jenis Kelamin :
      Fakultas/Prodi :

   j. Anggota Peneliti 2 *(Jika Ada)*
      Nama Lengkap : -
      Jenis Kelamin :
      Fakultas/Prodi :

(Jika anggota peneliti lebih dari 2, silakan ditambahkan dengan mengikuti format anggota peneliti di atas)

3. Lokasi Kegiatan : Indonesia
4. Jangka Waktu Pelaksanaan : 12 (dua belas) Bulan
5. Tahun Pelaksanaan : 2023
6. Jumlah Anggaran Biaya : Rp.
7. Sumber Dana : Mandiri
8. *Output* dan *Outcome* : a. Laporan Penelitian; b. Publikasi Ilmiah; c. HKI

Mengetahui,
Kepala Pusat Penelitian dan Penerbitan
LP2M UIN Ar-Raniry Banda Aceh,

Dr. Anton Widyanto, M. Ag.
NIP. 197610092002121002

Banda Aceh, 15 Januari 2024
Pelaksana,

Rika Yuliana
NIDN. 2013078403.

Menyetujui:
Rektor UIN Ar-Raniry Banda Aceh,

Prof. Dr. H. Mujiburrahman, M.Ag.
NIP. 197109082001121001

BEST PRACTICE FRAMEWORK FOR INFORMATION TECHNOLOGY SECURITY GOVERNANCE IN INDONESIAN GOVERNMENT

Ketua Peneliti:
Rika Yuliana

Anggota Peneliti:
-

Abstrak

Information technology security is crucial for a digital government system to have so that the continuity of business processes can run smoothly. However, the current best practice of information security governance in the Indonesian national government is still inadequate according to various related studies still siloed and scattered and leading to vulnerabilities in the various digital services provided. Therefore, this study aims to develop a best practice framework for managing information security that is aligned with the needs of Indonesia's digital government. This research started by looking for the main framework of information security governance. Then the main components that resulted from that were benchmarked with other Information Security Governance (ISG) best practices from different countries. Finally, it ended up complementing them with information security parameters, other related components, and recommendations, particularly in the Indonesian context, so that the main components and their respective constituent sub-components can be obtained according to the needs of the Indonesian e-government. The cause-and-effect analysis concept analyses the data linkages between the six central components and their respective sub-components. This study concludes that each of main components and sub-components supports each other so that all these things must be carried out in a balanced and continuous manner.

Kata Kunci: *Best practice, Digital government,Framework,Indonesia,Security governance*

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

Syukur Alhamdulillah kepada Allah SWT, karena dengan rahmat dan hidayah-Nya penulis telah dapat menyelesaikan laporan penelitian dengan judul **"Best Practice Framework For Information Technology Security Governance In Indonesian Government"**. Salawat beriring salam penulis persembahkan kepada Nabi Muhammad SAW, beserta keluarga dan para sahabatnya.

Dalam proses penelitian dan penulisan laporan ini tentu banyak pihak yang ikut memberikan motivasi, bimbingan dan arahan. Oleh karena itu penulis tidak lupa menyampaikan ucapan terima kasih kepada yang terhormat:

1. Rektor Universitas Islam Negeri Ar-Raniry Banda Aceh;
2. Ketua LP2M UIN Ar-Raniry Banda Aceh;
3. Sekretaris LP2M UIN Ar-Raniry Banda Aceh;
4. Kepala Pusat Penelitian dan Penerbitan UIN Ar-Raniry Banda Aceh;
5. Dekan Fakultas Sains dan teknologi beserta jajarannya;
6. Kolega yang tidak bisa disebutkan satu per satu;

Akhirnya hanya Allah SWT yang dapat membalas amalan mereka, semoga menjadikannya sebagai amal yang baik.

Harapan penulis, semoga hasil penelitian ini bermanfaat dan menjadi salah satu amalan penulis yang diperhitungkan sebagai ilmu yang bermanfaat di dunia dan akhirat. *Amin ya Rabbal 'Alamin.*

Banda Aceh, 15 Januari 2024

Ketua Peneliti,

Rika Yuliana

DAFTAR ISI

BAB I PENDAHULUAN

Ketika peretas semakin pintar, kebutuhan untuk melindungi aset digital dan perangkat jaringan Anda semakin besar. Ancaman terhadap keamanan TI dapat muncul dalam berbagai bentuk. Ancaman yang umum adalah malware, atau perangkat lunak berbahaya, yang dapat hadir dalam berbagai variasi untuk menginfeksi perangkat jaringan, termasuk: ransomware, spyware, virus. Ancaman-ancaman ini menjadikan penerapan praktik keamanan yang andal menjadi semakin penting. Keamanan TI mencegah ancaman berbahaya dan potensi pelanggaran keamanan yang dapat berdampak besar pada organisasi Anda. Saat Anda memasuki jaringan internal perusahaan, keamanan TI membantu memastikan hanya pengguna resmi yang dapat mengakses dan membuat perubahan pada informasi sensitif yang ada di sana. Keamanan TI berfungsi untuk memastikan kerahasiaan data organisasi Anda. Meskipun penyediaan keamanan TI membutuhkan biaya yang mahal, pelanggaran yang signifikan akan menimbulkan kerugian yang jauh lebih besar bagi organisasi. Pelanggaran besar dapat membahayakan kesehatan usaha kecil. Selama atau setelah insiden, tim keamanan TI dapat mengikuti rencana respons insiden sebagai alat manajemen risiko untuk mengendalikan situasi. Meskipun keamanan TI dan keamanan informasi terdengar serupa, keduanya mengacu pada jenis keamanan yang berbeda. Keamanan informasi mengacu pada proses dan alat yang dirancang untuk melindungi informasi bisnis sensitif dari invasi, sedangkan keamanan TI mengacu pada pengamanan data digital, melalui keamanan jaringan komputer.

Keamanan TI (kependekan dari keamanan teknologi informasi), adalah praktik melindungi aset TI organisasi—sistem komputer, jaringan, perangkat digital, data—dari akses tidak sah, pelanggaran data, serangan siber, dan aktivitas berbahaya lainnya. Cakupan keamanan TI sangat luas dan sering kali melibatkan perpaduan teknologi dan solusi keamanan yang bekerja sama untuk mengatasi kerentanan pada perangkat digital, jaringan komputer, server, database, dan aplikasi perangkat lunak. Contoh keamanan TI yang paling sering dikutip mencakup disiplin keamanan digital seperti keamanan titik akhir, keamanan cloud, keamanan jaringan, dan keamanan aplikasi. Namun keamanan TI juga mencakup langkah-langkah keamanan fisik—misalnya, kunci, kartu identitas, kamera pengintai—yang diperlukan untuk melindungi gedung dan perangkat yang menyimpan data dan aset TI.

Keamanan TI sering disalahartikan dengan keamanan siber, suatu disiplin ilmu yang lebih sempit yang secara teknis merupakan bagian dari keamanan TI. Keamanan siber berfokus terutama pada perlindungan organisasi dari serangan digital, seperti ransomware, malware, dan penipuan phishing, sedangkan keamanan TI melayani seluruh infrastruktur teknis organisasi, termasuk sistem perangkat keras, aplikasi perangkat lunak, dan titik akhir, seperti laptop dan perangkat seluler, serta perusahaan. jaringan dan berbagai komponennya, seperti pusat data fisik dan berbasis cloud.

Serangan siber dan insiden keamanan dapat menimbulkan dampak besar berupa hilangnya bisnis, rusaknya reputasi, denda peraturan, dan, dalam beberapa kasus, pemerasan dan pencurian aset. Misalnya, laporan IBM Cost of a Data Breach 2023 mempelajari lebih dari 550 perusahaan yang mengalami pelanggaran data antara bulan Maret 2022 dan Maret 2022. Rata-rata kerugian akibat pelanggaran data yang dialami perusahaan-perusahaan tersebut adalah

USD 4,45 juta—naik 2,3 persen dari temuan serupa. belajar setahun sebelumnya, dan naik 15,3 persen dibandingkan studi tahun 2020. Faktor-faktor yang berkontribusi terhadap biaya ini mencakup segala hal mulai dari memberi tahu pelanggan, eksekutif, dan regulator hingga denda peraturan, hilangnya pendapatan selama waktu henti, dan pelanggan hilang secara permanen.

Beberapa insiden keamanan memerlukan biaya yang lebih besar dibandingkan insiden lainnya. Serangan Ransomware mengenkripsi data organisasi, membuat sistem tidak dapat digunakan, dan menuntut pembayaran uang tebusan yang mahal untuk kunci dekripsi guna membuka kunci data; semakin banyak mereka yang menuntut uang tebusan kedua untuk mencegah pembagian data sensitif kepada publik atau penjahat dunia maya lainnya. Menurut IBM Security Definitive Guide to Ransomware 2023, permintaan tebusan telah meningkat hingga mencapai jumlah 7 dan 8 digit, dan dalam kasus ekstrim telah mencapai angka USD 80 juta.

Dapat diprediksi, investasi pada keamanan TI akan terus meningkat. Analis industri Gartner memperkirakan bahwa pada tahun 2023 organisasi akan menghabiskan USD 188,3 miliar untuk sumber daya dan layanan keamanan informasi dan manajemen risiko, dengan pasar yang terus membengkak di tahun-tahun mendatang, menghasilkan hampir USD 262 miliar pada tahun 2026, mengikuti tingkat pertumbuhan tahunan gabungan sebesar 11 persen dari tahun 2021.

Setiap organisasi rentan terhadap ancaman siber dari dalam dan luar organisasinya. Ancaman ini bisa disengaja, seperti yang dilakukan penjahat dunia maya, atau tidak disengaja, seperti yang dilakukan karyawan atau kontraktor yang secara tidak sengaja mengeklik tautan berbahaya atau mengunduh malware. Keamanan TI bertujuan untuk mengatasi berbagai risiko keamanan dan

memperhitungkan semua jenis pelaku ancaman serta berbagai motivasi, taktik, dan tingkat keterampilan mereka.

A. perangkat lunak perusak

Malware adalah perangkat lunak berbahaya yang dapat membuat sistem yang terinfeksi tidak dapat dioperasikan, menghancurkan data, mencuri informasi, dan bahkan menghapus file penting bagi sistem operasi. Jenis malware yang terkenal meliputi:

- Ransomware adalah malware yang mengunci data atau perangkat korban dan mengancam akan tetap menguncinya—atau lebih buruk lagi—kecuali korban membayar uang tebusan kepada penyerang. Menurut IBM Security X-Force Threat Intelligence Index 2023, serangan ransomware mewakili 17 persen dari seluruh serangan siber pada tahun 2022.
- Kuda Troya adalah malware yang menipu orang agar mengunduhnya dengan menyamar sebagai program berguna atau bersembunyi di dalam perangkat lunak yang sah. Trojan akses jarak jauh (RAT) menciptakan pintu belakang rahasia pada perangkat korban, sementara Trojan penetes memasang malware tambahan setelah perangkat tersebut memiliki pijakan.
- **Perangkat mata-mata**diam-diam mengumpulkan informasi sensitif, seperti nama pengguna, kata sandi, nomor kartu kredit, dan data pribadi lainnya, dan mengirimkannya kembali ke peretas.
- Worm adalah malware yang mereplikasi dirinya sendiri dan dapat menyebar secara otomatis antar aplikasi dan perangkat.

- **Perangkat lunak iklan** adalah perangkat lunak periklanan yang dapat digunakan untuk menyebarkan malware.
- **Botnet** adalah jaringan komputer yang terinfeksi malware yang digunakan penjahat dunia maya untuk melakukan tugas secara online tanpa izin pengguna.
- **Perangkat mata-mata**: Sebuah program yang diam-diam mencatat apa yang dilakukan pengguna, sehingga penjahat dunia maya dapat memanfaatkan informasi ini. Misalnya, spyware dapat menangkap rincian kartu kredit.
- **Virus**: Program yang mereplikasi dirinya sendiri untuk membersihkan file dan menyebar ke seluruh sistem komputer, menginfeksi file dengan kode berbahaya.
- **Penipuan Romantis**.

  Pada bulan Februari 2020, FBI memperingatkan warga AS untuk mewaspadai penipuan kepercayaan yang dilakukan penjahat dunia maya menggunakan situs kencan, ruang obrolan, dan aplikasi. Pelaku memanfaatkan orang-orang yang mencari pasangan baru, menipu korban agar memberikan data pribadi. FBI melaporkan bahwa ancaman dunia maya percintaan berdampak pada 114 korban di New Mexico pada tahun 2019, dengan kerugian finansial sebesar $1,6 juta.

B. Serangan Rekayasa Sosial

Sering disebut sebagai "peretasan manusia", rekayasa sosial memanipulasi korban untuk mengambil tindakan yang mengungkap

informasi sensitif, membahayakan keamanan organisasi, atau mengancam kesejahteraan finansial organisasi.

Phishing adalah jenis serangan rekayasa sosial yang paling terkenal dan paling luas. Serangan phishing menggunakan email palsu, pesan teks, atau panggilan telepon untuk mengelabui orang agar membagikan data pribadi atau kredensial akses, mengunduh malware, mengirim uang ke penjahat dunia maya, atau mengambil tindakan lain yang dapat membuat mereka terkena kejahatan dunia maya. Jenis phishing khusus meliputi:

- Spear phishing—serangan phishing bertarget tinggi yang memanipulasi individu tertentu, sering kali menggunakan detail dari profil media sosial publik korban untuk membuat tipu muslihatnya lebih meyakinkan.
- Whale phishing—spear phishing yang menargetkan eksekutif perusahaan atau individu kaya.
- Kompromi email bisnis (BEC)—penipuan di mana penjahat dunia maya menyamar sebagai eksekutif, vendor, atau rekan bisnis tepercaya untuk mengelabui korban agar mengirim uang atau membagikan data sensitif.

Taktik rekayasa sosial lainnya, tailgaiting, kurang teknis namun juga merupakan ancaman bagi keamanan TI: taktik ini melibatkan mengikuti (atau 'mengekor') seseorang yang memiliki akses fisik ke pusat data (misalnya, seseorang dengan kartu identitas) dan secara harfiah menyelinap masuk di belakang mereka sebelum pintu ditutup.

C. Serangan penolakan layanan (DoS).

Serangan DoS membanjiri situs web, aplikasi, atau sistem dengan volume lalu lintas palsu, menjadikannya terlalu lambat untuk digunakan atau sama sekali tidak tersedia bagi pengguna yang sah. Serangan penolakan layanan terdistribusi (DDoS) menggunakan jaringan perangkat yang terhubung ke internet dan terinfeksi malware—disebut botnet—untuk melumpuhkan atau membuat crash aplikasi atau sistem target.

D. Eksploitasi zero-day

Sebuah eksploitasi zero-day yang memanfaatkan kelemahan keamanan yang tidak diketahui atau belum terselesaikan pada perangkat lunak, perangkat keras, atau firmware komputer. 'Zero day' mengacu pada fakta bahwa vendor perangkat lunak atau perangkat tidak punya waktu, atau waktu, untuk memperbaiki kelemahan tersebut, karena pelaku kejahatan sudah dapat menggunakannya untuk mendapatkan akses ke sistem yang rentan.

E. Ancaman dari dalam

Ancaman orang dalam berasal dari karyawan, mitra, dan pengguna lain yang memiliki akses resmi ke jaringan. Baik yang tidak disengaja (misalnya, vendor pihak ketiga yang tertipu untuk meluncurkan malware) atau jahat (misalnya, karyawan yang tidak puas dan bertekad membalas dendam), ancaman dari dalam sangat berpengaruh. Laporan terbaru dari Verizon (tautan ada di luar ibm.com) mengungkapkan bahwa meskipun rata-rata ancaman eksternal mencakup sekitar 200 juta data, ancaman

yang melibatkan pelaku ancaman dari dalam telah mengungkap sebanyak 1 miliar data.

F. Serangan Man-in-the-middle (MIM).

Dalam serangan MITM, penjahat dunia maya menguping koneksi jaringan dan menyadap serta menyampaikan pesan antara dua pihak untuk mencuri data. Jaringan Wi-Fi yang tidak aman adalah tempat berburu bagi peretas yang melancarkan serangan MITM.

G. Injeksi SQL

Injeksi SQL (kueri bahasa terstruktur) adalah jenis serangan cyber yang digunakan untuk mengambil kendali dan mencuri data dari database. Penjahat dunia maya mengeksploitasi kerentanan dalam aplikasi berbasis data untuk memasukkan kode berbahaya ke dalam database melalui pernyataan SQL yang berbahaya. Ini memberi mereka akses ke informasi sensitif yang terdapat dalam database.

Perlindungan pengguna akhir atau keamanan titik akhir merupakan aspek penting dalam keamanan siber. Lagi pula, sering kali individu (pengguna akhir) yang secara tidak sengaja mengunggah malware atau bentuk ancaman dunia maya lainnya ke desktop, laptop, atau perangkat seluler mereka. Pertama, keamanan siber bergantung pada protokol kriptografi untuk mengenkripsi email, file, dan data penting lainnya. Hal ini tidak hanya melindungi informasi dalam perjalanan, tetapi juga melindungi dari kehilangan atau pencurian. Selain itu, perangkat lunak keamanan pengguna akhir memindai komputer untuk mencari potongan kode berbahaya, mengkarantina kode ini, dan kemudian menghapusnya

dari mesin. Program keamanan bahkan dapat mendeteksi dan menghapus kode berbahaya yang tersembunyi di catatan boot utama dan dirancang untuk mengenkripsi atau menghapus data dari hard drive komputer. Protokol keamanan elektronik juga fokus pada deteksi malware secara real-time. Banyak yang menggunakan analisis heuristik dan perilaku untuk memantau perilaku program dan kodenya untuk bertahan melawan virus atau Trojan yang berubah bentuk setiap kali dieksekusi (malware polimorfik dan metamorfik). Program keamanan dapat membatasi program yang berpotensi berbahaya ke dalam gelembung virtual yang terpisah dari jaringan pengguna untuk menganalisis perilakunya dan mempelajari cara mendeteksi infeksi baru dengan lebih baik. Program keamanan terus mengembangkan pertahanan baru seiring para profesional keamanan siber mengidentifikasi ancaman baru dan cara baru untuk memeranginya. Untuk memanfaatkan perangkat lunak keamanan pengguna akhir secara maksimal, karyawan perlu dididik tentang cara menggunakannya. Yang terpenting, menjaganya tetap berjalan dan memperbaruinya secara rutin akan memastikan bahwa aplikasi ini dapat melindungi pengguna dari ancaman dunia maya terbaru.

Keamanan informasi merupakan komponen penting dalam proses perencanaan teknologi informasi yang terintegrasi dalam organisasi, khususnya di pemerintahan Indonesia [1]. Hal ini disebabkan karena pemerintah sedang dalam proses mengembangkan sistem pemerintahan digital dan juga smart city secara keseluruhan, sehingga aspek keamanan menjadi salah satu perhatian utama pemerintah dalam memberikan pelayanan yang lebih baik kepada pemangku kepentingan. Karena kebutuhan untuk menjaga kualitas layanan yang diberikan oleh pemerintah Indonesia dalam hal kerahasiaan, integritas, dan ketersediaan sistem pemerintahan digital, pemerintah harus memenuhi kebutuhan pengguna hingga tingkat kematangan keamanan teknologi informasi tertinggi. Lebih lanjut,

aspek keamanan dikaitkan dengan kota pintar di mana sistem fisik siber tidak hanya digunakan oleh warga negara tetapi juga dapat dimodifikasi oleh peretas dan pencuri identitas [2]. Berdasarkan beberapa penelitian dari referensi [3], [4] dan fakta dari dunia nyata [5], namun Indonesia belum memiliki kerangka praktik terbaik yang komprehensif dalam mengelola keamanan informasi. Hal ini berdampak pada banyak layanan yang belum dimanfaatkan secara maksimal karena rentannya serangan malware, crash, dan masalah terkait lainnya.

BAB II LANDASAN TEORI

Perkembangan di bidang teknologi informasi terus mengalami perubahan setiap tahunnya. Adanya internet memudahkan setiap orang dalam mencari sesuatu melalui perangkat elektroniknya, terutama ponsel atau komputer sebagai medianya. Gadget saat ini seolah menjadi jendela dunia, dengan hadirnya internet maka apapun yang kita cari akan muncul dan bisa kita temukan di internet. Tak hanya itu, seiring berjalannya waktu, pembayaran, pemesanan makanan, pemesanan tiket transportasi bisa dilakukan melalui gadget. Hal ini membuat dunia yang jauh menjadi dekat. Semua pihak terus mengembangkan dan melakukan inovasi-inovasi terkini di bidang teknologi. Demi tercapainya pelayanan publik yang prima saat ini, pemerintah senantiasa memberikan inovasi sejalan dengan perkembangan masa kini, khususnya di bidang teknologi. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik menyatakan bahwa pelayanan publik adalah kegiatan atau rangkaian kegiatan dalam rangka memenuhi kebutuhan pelayanan sesuai dengan peraturan perundang-undangan bagi setiap warga negara dan penduduk mengenai barang, jasa atau pelayanan administrasi yang disediakan oleh penyelenggara pelayanan publik. Pelayanan publik di Indonesia terus melakukan berbagai inovasi baru di berbagai bidang, mulai dari barang, jasa, dan pelayanan administrasi. Hal ini memberikan dampak positif terhadap kemajuan pelayanan publik di Indonesia, dengan berbagai adaptasi yang dilakukan pemerintah dalam upaya mencapai pelayanan publik yang prima mengingat era Pelayanan Publik Baru. Pada era sekarang ini, tata kelola pemerintahan dituntut untuk memberikan pelayanan prima dalam melaksanakan pelayanan kepada masyarakat.

E-Government memberikan layanan pemerintah kepada masyarakat secara efektif dan efisien sehingga meningkatkan transparansi dan akuntabilitas, mengurangi korupsi dan meningkatkan pendapatan dan/atau mengurangi biaya (Ismail et al., 2020). Terdapat keterkaitan yang jelas antara e-Government untuk meningkatkan pelayanan publik dan mengurangi korupsi. Beberapa penelitian lain menunjukkan bahwa e-Government terbukti mampu mengurangi korupsi dan meningkatkan pelayanan publik (Afriana et al., 2020). Erkut (2020) mengatakan bahwa dalam perspektif baru, E-Government atau Digital Government merupakan bagian dari konsep Digital Governance dimana struktur praktik sektor publik atau kebijakan pemerintah dilakukan dengan menggunakan teknologi informasi dan komunikasi sehingga memungkinkan terjadinya interaksi dengan masing-masing pemangku kepentingan. dan pelaksanaannya, transparansi, pelayanan prima, efisiensi dan efektivitas.

Keamanan TI (kependekan dari keamanan teknologi informasi), adalah praktik melindungi aset TI organisasi—sistem komputer, jaringan, perangkat digital, data—dari akses tidak sah,pelanggaran data,serangan siber, dan aktivitas jahat lainnya. Cakupan keamanan TI sangat luas dan sering kali melibatkan perpaduan teknologi dan solusi keamanan yang bekerja sama untuk mengatasi kerentanan pada perangkat digital, jaringan komputer, server, database, dan aplikasi perangkat lunak. Contoh keamanan TI yang paling sering dikutip mencakup disiplin keamanan digital sepertikeamanan titik akhir,keamanan awan,keamanan jaringan, dan keamanan aplikasi. Namun keamanan TI juga mencakup langkah-langkah keamanan fisik—misalnya, kunci, kartu identitas,

kamera pengintai—yang diperlukan untuk melindungi gedung dan perangkat yang menyimpan data dan aset TI.

Jenis keamanan TI adalah sebagai berikut:

- Keamanan awan

  Keamanan cloud mengatasi ancaman siber eksternal dan internal terhadap infrastruktur, aplikasi, dan data berbasis cloud suatu organisasi. Keamanan cloud beroperasi pada model tanggung jawab bersama. Dengan kata lain, penyedia layanan cloud (CSP) bertanggung jawab untuk mengamankan infrastruktur yang digunakan untuk memberikan layanan cloud, dan pelanggan bertanggung jawab untuk mengamankan apa pun yang dijalankan pada infrastruktur tersebut. Detail tanggung jawab bersama tersebut berbeda-beda bergantung pada layanan cloud.Aplikasi, data, dan identitas dipindahkan ke cloud, artinya pengguna terhubung langsung ke Internet dan tidak dilindungi oleh sistem keamanan tradisional. Keamanan cloud dapat membantu mengamankan penggunaan aplikasi perangkat lunak sebagai layanan (SaaS) dan cloud publik. Broker keamanan akses cloud (CASB), gateway Internet aman (SIG), dan manajemen ancaman terpadu (UTM) berbasis cloud dapat digunakan untuk keamanan cloud.

- Keamanan titik akhir

  Keamanan titik akhir melindungi pengguna akhir dan perangkat titik akhir, seperti desktop, laptop, ponsel, dan server, dari serangan siber. Keamanan titik akhir juga melindungi jaringan dari penjahat dunia maya yang mencoba menggunakan perangkat titik akhir untuk melancarkan serangan siber terhadap data sensitif dan aset lainnya. Keamanan titik

akhir memberikan perlindungan di tingkat perangkat. Perangkat yang dapat diamankan dengan keamanan titik akhir mencakup ponsel, tablet, laptop, dan komputer desktop. Keamanan titik akhir akan mencegah perangkat Anda mengakses malwarejaringanyang mungkin menjadi ancaman bagi organisasi Anda. Perlindungan malware tingkat lanjut dan perangkat lunak manajemen perangkat adalah contoh keamanan titik akhir.

- Keamanan jaringan

  Keamanan jaringan memiliki tiga tujuan utama: untuk mencegah akses tidak sah ke sumber daya jaringan, untuk mendeteksi dan menghentikan serangan siber dan pelanggaran keamanan secara real-time, dan untuk memastikan bahwa pengguna yang berwenang memiliki akses aman ke sumber daya jaringan yang mereka perlukan saat dibutuhkan.Hal ini memastikan kegunaan, keandalan, dan integritas tanpa kompromi. Jenis keamanan ini diperlukan untuk mencegah peretas mengakses data di dalam jaringan. Hal ini juga mencegah mereka memberikan dampak negatif terhadap kemampuan pengguna Anda untuk mengakses atau menggunakan jaringan. Keamanan jaringan menjadi semakin menantang seiring dengan meningkatnya jumlah endpoint dan migrasi layanan ke cloud publik.

- Keamanan aplikasi

  Keamanan aplikasi mengacu pada tindakan yang diambil pengembang saat membuat aplikasi untuk mengatasi potensi kerentanan, dan melindungi data pelanggan serta kode mereka sendiri agar tidak dicuri, bocor, atau disusupi.Dengan keamanan aplikasi, aplikasi diberi kode khusus pada saat pembuatannya agar seaman mungkin, untuk membantu

memastikan aplikasi tidak rentan terhadap serangan. Lapisan keamanan tambahan ini melibatkan evaluasi kode aplikasi dan mengidentifikasi kerentanan yang mungkin ada dalam perangkat lunak.

- Keamanan internet

  Keamanan internet melindungi data dan informasi sensitif yang dikirimkan, disimpan, atau diproses oleh browser atau aplikasi. Keamanan internet melibatkan serangkaian praktik dan teknologi keamanan yang memantau lalu lintas internet masuk untuk mencari malware dan konten berbahaya lainnya. Teknologi di bidang ini mencakup mekanisme otentikasi, gateway web, protokol enkripsi dan, yang paling penting, firewall.Keamanan internet melibatkan perlindungan informasi yang dikirim dan diterima di browser, serta keamanan jaringan yang melibatkan aplikasi berbasis web. Perlindungan ini dirancang untuk memantau lalu lintas internet masuk dari malware serta lalu lintas yang tidak diinginkan. Perlindungan ini dapat berupa firewall, antimalware, dan antispyware.

- Keamanan IOT dan OT

  Keamanan Internet of Things (IoT) berfokus pada pencegahan sensor dan perangkat yang terhubung ke Internet—misalnya kamera bel pintu, peralatan pintar, mobil modern—dikendalikan oleh peretas atau digunakan oleh peretas untuk menyusup ke jaringan organisasi. Keamanan teknologi operasional (OT) berfokus lebih spesifik pada perangkat terhubung yang memantau atau mengendalikan proses dalam perusahaan—misalnya, sensor pada jalur perakitan otomatis.

Keamanan TI sering dikacaukan dengan keamanan cyber, disiplin yang lebih sempit yang secara teknis merupakan bagian dari keamanan TI. Keamanan

siber berfokus terutama pada perlindungan organisasi dari serangan digital, seperti ransomware, malware, dan penipuan phishing, sedangkan keamanan TI melayani seluruh infrastruktur teknis organisasi, termasuk sistem perangkat keras, aplikasi perangkat lunak, dan titik akhir, seperti laptop dan perangkat seluler, serta perusahaan. jaringan dan berbagai komponennya, seperti pusat data fisik dan berbasis cloud.

Mengingat adanya tumpang tindih yang signifikan, istilah 'keamanan TI', 'keamanan informasi', dan 'keamanan siber' sering (dan secara keliru) digunakan secara bergantian. Mereka berbeda terutama dalam cakupannya. Keamanan informasi adalah perlindungan file dan data digital suatu organisasi, dokumen kertas, media fisik dan bahkan ucapan manusia terhadap akses, pengungkapan, penggunaan atau perubahan yang tidak sah. Keamanan informasi memiliki cakupan paling luas di antara ketiganya: seperti keamanan TI, keamanan informasi berkaitan dengan perlindungan aset fisik TI dan pusat data, namun juga berkaitan dengan keamanan fisik fasilitas penyimpanan file kertas dan media lainnya. Keamanan siber berfokus pada perlindungan data dan aset digital dari ancaman siber—tindakan berbahaya dari pelaku ancaman eksternal dan internal, serta ancaman tidak disengaja yang ditimbulkan oleh orang dalam yang ceroboh. Meskipun merupakan upaya yang sangat besar, keamanan siber memiliki cakupan yang paling sempit karena tidak berkaitan dengan perlindungan data kertas atau analog.

Berbagai permasalahan dan permasalahan yang timbul akibat penggunaan teknologi e-Government di Indonesia semakin hari semakin meningkat, terutama yang berkaitan dengan keamanan informasi. Misalnya, rentannya suatu website pemerintah diretas oleh pihak yang tidak bertanggung jawab dapat

mengakibatkan terganggunya layanan yang dapat diberikan kepada masyarakat. Hal ini juga dapat menimbulkan stigma buruk di masyarakat. Meskipun pemerintah dan pemangku kepentingan terkait mempunyai kepedulian terhadap pentingnya keamanan informasi dalam layanan e-Government, yang terlihat dari integrasi aspek keamanan dalam implementasi pemerintahan digital Indonesia dan berbagai penelitian terkait, namun masih terdapat kesenjangan dalam penerapannya. tata kelola keamanan informasi. Hal ini bisa terjadi karena para peneliti yang terlibat hanya melihat keamanan informasi di Indonesia dari segi teknis. Sehingga menimbulkan berbagai dampak pula terhadap kehidupan anggota masyarakat Indonesia, seperti pencurian identitas. Selain itu, penelitian ini menunjukkan bahwa tantangan ini perlu diatasi dengan tiga cara: pengembangan kepraktisan tata kelola, kemampuan beradaptasi, dan keterukuran, dan kemudian penyelarasannya dengan organisasi [6]. Oleh karena itu, pemerintah Indonesia harus memiliki panduan komprehensif tentang cara mengatur keamanan informasi, khususnya dalam bentuk praktik terbaik yang berasal dari kerangka kerja dan tata kelola terkait untuk mencapai tingkat kematangan keamanan informasi tertinggi dalam penerapan pemerintahan digital di Indonesia seiring dengan perkembangan negara ini. dan berkembang.

Ketika ancaman keamanan siber terus meningkat dalam keganasan dan kompleksitas, organisasi menerapkan strategi keamanan TI yang menggabungkan berbagai sistem, program, dan teknologi keamanan. Diawasi oleh tim keamanan berpengalaman, praktik dan teknologi keamanan TI ini dapat membantu melindungi seluruh infrastruktur TI organisasi, dan menghindari atau memitigasi dampak ancaman siber yang diketahui dan tidak diketahui.

1. Pelatihan kesadaran keamanan

   Karena banyak serangan siber, seperti serangan phishing, mengeksploitasi kerentanan manusia, pelatihan karyawan telah menjadi garis pertahanan penting terhadap ancaman orang dalam. Pelatihan kesadaran keamanan mengajarkan karyawan untuk mengenali ancaman keamanan dan menggunakan kebiasaan kerja yang aman. Topik yang dibahas sering kali mencakup kesadaran phishing, keamanan kata sandi, pentingnya menjalankan pembaruan perangkat lunak secara berkala, dan masalah privasi, seperti cara melindungi data pelanggan dan informasi sensitif lainnya.

2. Otentikasi multi-faktor

   Otentikasi multi-faktor memerlukan satu atau lebih kredensial selain nama pengguna dan kata sandi. Menerapkan otentikasi multi-faktor dapat mencegah peretas mendapatkan akses ke aplikasi atau data di jaringan, meskipun peretas mampu mencuri atau mendapatkan nama pengguna dan kata sandi pengguna yang sah. Autentikasi multi-faktor sangat penting bagi organisasi yang menggunakan sistem masuk tunggal, yang memungkinkan pengguna masuk ke suatu sesi satu kali, dan mengakses beberapa aplikasi dan layanan terkait selama sesi tersebut tanpa perlu masuk lagi.

3. Respons insiden

   Respons insiden, terkadang disebut respons insiden keamanan siber, mengacu pada proses dan teknologi organisasi untuk mendeteksi dan merespons ancaman siber, pelanggaran keamanan, dan serangan siber. Tujuan dari respons insiden adalah untuk mencegah serangan siber

sebelum terjadi, dan untuk meminimalkan biaya dan gangguan bisnis akibat serangan siber yang terjadi.

Banyak organisasi membuat rencana respons insiden (IRP) formal yang mendefinisikan proses dan perangkat lunak keamanan (lihat di bawah) yang mereka gunakan untuk mengidentifikasi, membendung, dan menyelesaikan berbagai jenis serangan siber. Menurut laporan Biaya Pelanggaran Data tahun 2003, di organisasi yang membuat dan secara rutin menguji IRP formal, biaya pelanggaran data adalah sebesar USD 232.008 lebih rendah dari rata-rata (USD 4,45 juta).

4. Perangkat lunak keamanan

Tidak ada satu pun alat keamanan yang dapat mencegah serangan siber secara keseluruhan. Namun, ada beberapa alat yang dapat berperan dalam memitigasi risiko siber, mencegah serangan siber, dan meminimalkan kerusakan jika terjadi serangan. Perangkat lunak keamanan umum untuk membantu mendeteksi dan mengalihkan serangan siber meliputi:

- Alat keamanan email, termasuk perangkat lunak anti-phishing berbasis AI, filter spam, dan gateway email yang aman
- Perangkat lunak antivirus untuk menetralisir penyerang spyware atau malware yang mungkin digunakan untuk menargetkan keamanan jaringan untuk melakukan penelitian, menguping percakapan, atau mengambil alih akun email
- Perbaikan sistem dan perangkat lunak untuk menutup kerentanan teknis yang biasa dieksploitasi oleh peretas

- Gerbang web yang aman dan alat pemfilteran web lainnya untuk memblokir situs web berbahaya yang sering dikaitkan dengan email phishing
- Solusi deteksi dan respons ancaman menggunakan analitik, kecerdasan buatan (AI), dan otomatisasi untuk membantu tim keamanan mendeteksi ancaman yang diketahui dan aktivitas mencurigakan, serta mengambil tindakan untuk menghilangkan ancaman atau meminimalkan dampaknya. Teknologi-teknologi ini mencakup orkestrasi keamanan, otomatisasi dan respons (SOAR), manajemen insiden dan peristiwa keamanan (SIEM), deteksi dan respons titik akhir (EDR), deteksi dan respons jaringan (NDR), serta deteksi dan respons yang diperluas (XDR).

5. Keamanan ofensif

Keamanan ofensif, atau "OffSec," mengacu pada serangkaian strategi keamanan proaktif yang menggunakan taktik permusuhan—taktik yang sama yang digunakan pelaku jahat dalam serangan di dunia nyata—untuk memperkuat keamanan jaringan, bukan membahayakannya. Operasi keamanan ofensif sering kali dilakukan oleh peretas etis, profesional keamanan siber yang menggunakan keterampilan peretasan mereka untuk menemukan dan memperbaiki kelemahan sistem TI. Metode keamanan ofensif yang umum meliputi:

- Pemindaian kerentanan—menggunakan alat yang sama yang digunakan penjahat dunia maya untuk mendeteksi dan mengidentifikasi kelemahan dan kelemahan keamanan yang dapat dieksploitasi dalam infrastruktur dan aplikasi TI organisasi.

- Pengujian penetrasi—meluncurkan serangan siber tiruan untuk mengungkap kerentanan dan kelemahan sistem komputer, alur kerja respons, dan kesadaran keamanan pengguna. Beberapa peraturan privasi data, seperti Standar Keamanan Data Industri Kartu Pembayaran (PCI-DSS), menetapkan SMS penetrasi reguler sebagai persyaratan kepatuhan.
- Tim merah—memberi wewenang kepada tim peretas etis untuk meluncurkan simulasi serangan siber yang berorientasi pada tujuan terhadap organisasi.

Keamanan ofensif melengkapi perangkat lunak keamanan dan langkah-langkah keamanan defensif lainnya—sistem ini menemukan jalur atau vektor serangan siber yang tidak diketahui yang mungkin terlewatkan oleh langkah-langkah keamanan lainnya, dan hal ini menghasilkan informasi yang dapat digunakan oleh tim keamanan untuk memperkuat langkah-langkah keamanan defensif mereka.

Menurut [7], keamanan telah berevolusi dari masalah yang sempit dan spesifik menjadi masalah bisnis strategis dengan implikasi "dari ruang bawah tanah hingga ruang rapat". Poin utamanya adalah organisasi harus melindungi diri mereka sendiri. Selain itu, mereka juga harus mengembangkan strategi untuk memastikan bahwa bisnis mereka cukup tangguh untuk memanfaatkan peluang terkait digitalisasi. Selain itu, tata kelola teknologi informasi merupakan komponen tata kelola organisasi yang mencakup peran dan implementasi proses, struktur, dan mekanisme relasional. Hal ini memungkinkan pemangku kepentingan bisnis dan teknologi informasi (TI) untuk melakukan tugas mempromosikan penyelarasan bisnis atau TI serta pembentukan dan

perlindungan nilai bisnis TI. Evaluasi "Keadaan Infrastruktur" menilai sejauh mana TI mampu mempertahankan infrastruktur yang kuat dan andal yang diperlukan untuk memenuhi kebutuhan bisnis secara efektif. Hal ini dicapai dengan membandingkan setiap domain platform dengan kriteria berbasis risiko untuk menilai dampak potensial terhadap kelangsungan bisnis, keamanan, dan/atau kepatuhan [8]. Permasalahan tersebut apabila tidak ditangani dengan baik akan menimbulkan kerugian finansial yang merugikan dunia usaha dan membahayakan keberlangsungan organisasi baik dalam jangka pendek maupun jangka panjang.

Keamanan informasi harus fleksibel untuk menangani setiap situasi dan berbagai persyaratan dari informasi, sistem, atau organisasi yang berbeda [10]. Manajemen keamanan informasi (ISM) adalah pendekatan yang berkelanjutan, terstruktur dan sistematis dalam keamanan untuk mengelola dan melindungi informasi organisasi agar tidak disusupi oleh pihak yang tidak bertanggung jawab. Untuk memastikan informasi tetap aman, banyak organisasi telah menerapkan ISM dengan menetapkan dan meninjau kebijakan, proses, prosedur, dan struktur organisasi keamanan informasi (IS). Organisasi juga perlu memvalidasi beberapa faktor dan elemen ISM yang berkontribusi terhadap keberhasilan ISM untuk memandu praktisi dalam menerapkan ISM yang tepat [11].

Ada banyak standar, kerangka kerja, undang-undang, pedoman, dan referensi praktik terbaik yang tersedia untuk memberikan saran kepada manajer keamanan informasi tentang bagaimana mereka menerapkan kontrol keamanan. Sebagian besar pedoman ini hanya berlaku di negara-negara tertentu, khususnya di negara-negara yang sebagian besar menerapkan aturan perlindungan data dan privasi. Pedoman ini juga diperkuat oleh penasihat khusus industri secara

keseluruhan yang dapat membantu manajer keamanan informasi untuk memberi informasi kepada manajer eksekutif tentang penerapan kontrol terbaik untuk menjaga keselamatan dan keamanan bisnis. Manajer juga harus mempertimbangkan apa yang benar-benar penting bagi organisasi dan merancang sistem manajemen keamanan yang masih relevan, proporsional, dan mempertimbangkan toleransi risiko organisasi dan pendekatan terbaik terhadap kelangsungan bisnis [12].

Saat ini, di setiap organisasi, layanan TI harus disediakan sedemikian rupa sehingga hemat biaya, mengurangi ancaman keamanan, dan mematuhi persyaratan hukum dan peraturan. Persamaan tersebut sulit untuk dipecahkan dan, dalam beberapa kasus, mungkin tampak mustahil. Untuk bertahan dalam lingkungan ini, usulan model tata kelola keamanan sistem informasi (ISS-GOV) dalam bentuk repositori internal tampaknya sesuai untuk tujuan ini. Pelaksana saat ini memiliki kerangka kerja untuk menerapkan strategi, rencana dan proses TI, untuk menentukan metrik, tolok ukur, dan audit, serta mengintegrasikan masalah keamanan untuk mengurangi risiko [13]

Berdasarkan konsep dan perkembangan di bidang keamanan informasi tersebut, Indonesia sangat membutuhkan kerangka tata kelola keamanan informasi yang komprehensif sesuai dengan kebutuhan perkembangan sistem e-Government saat ini. Pada dasarnya terdapat hubungan antara aspek keamanan informasi dan tata kelola teknologi informasi seperti terlihat pada Gambar 1 dan juga hubungan antara keamanan TI dan keamanan siber seperti terlihat pada Gambar 2 [14]. Namun penelitian yang dilakukan oleh [15] membuktikan bahwa tata kelola keamanan siber pada instansi pemerintah di Indonesia masih kurang dan belum terintegrasi serta perlunya memadukan berbagai hal terkait [16]. Selain itu, penelitian menunjukkan bahwa terus berkembangnya internet dan

teknologi, seperti big data, membuat informasi layanan publik semakin mendapat perhatian [17], sedangkan tingkat kematangan keamanan informasi (cybersecurity) di Indonesia masih kurang [18], sehingga diperlukan suatu usulan kerangka kerja untuk mengelola keamanan informasi sesuai dengan kebutuhan pemerintahan digital Indonesia untuk mencapai tingkat kematangan keamanan informasi yang optimal. Oleh karena itu, penelitian ini bertujuan untuk mengusulkan kerangka praktik terbaik tata kelola keamanan informasi agar dapat diterapkan pada e-Government Indonesia.

Figure 1. Information security governance positioned [14]

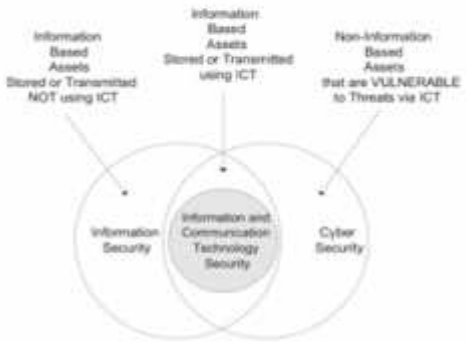


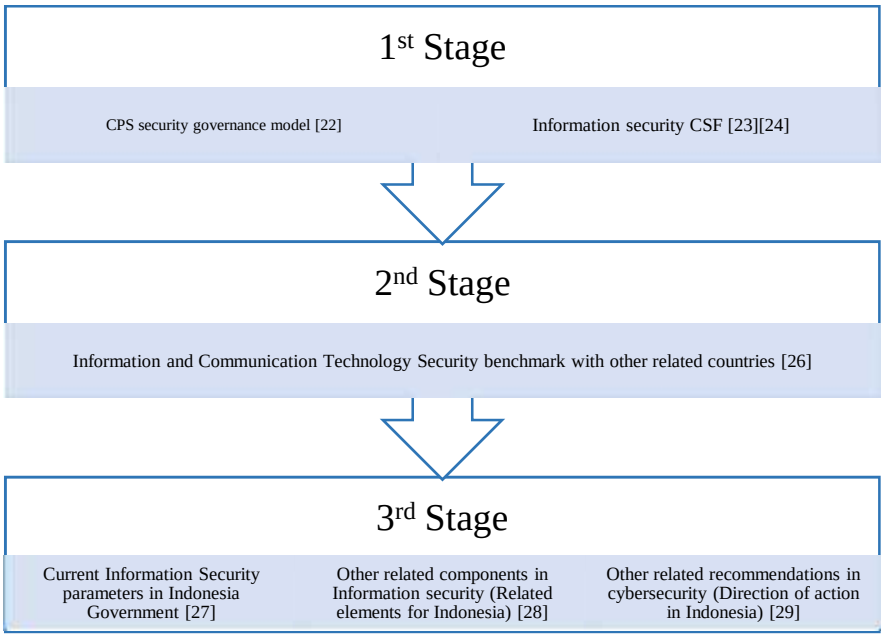
Figure 2. The relationship between information and communication security, information security and cyber security [14]

BAB III METODOLOGI PENELITIAN

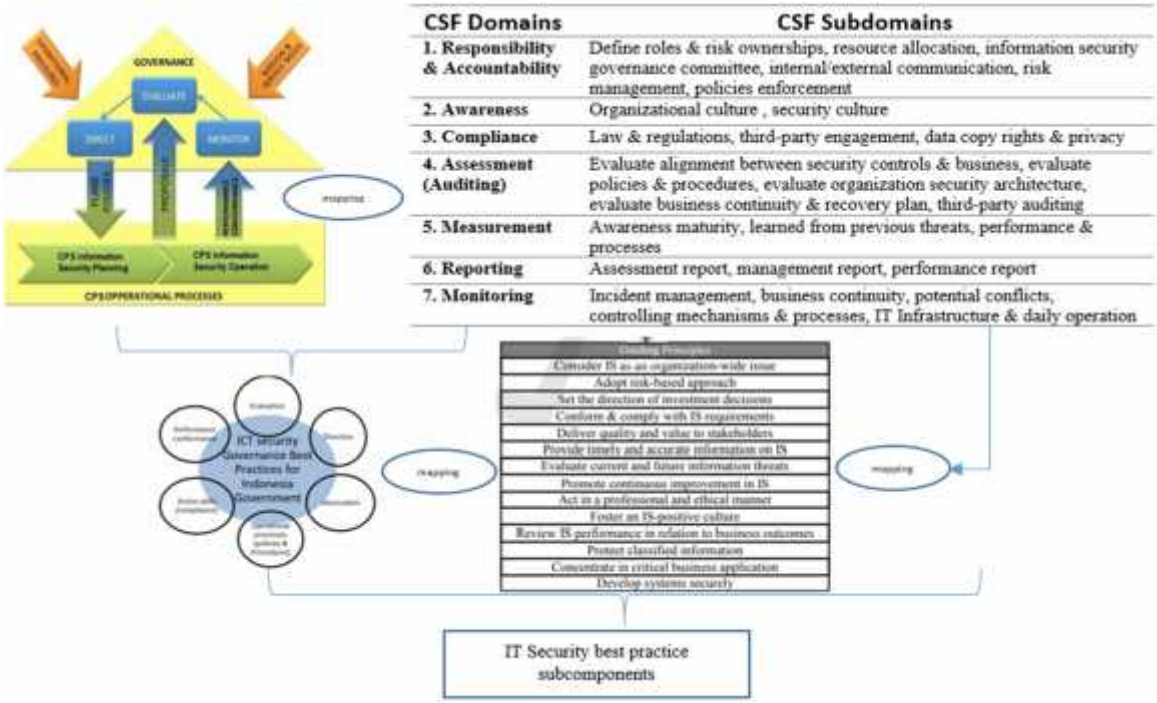
Pada dasarnya keamanan informasi merupakan hal krusial yang bekerja terintegrasi dengan tata kelola organisasi dan berkaitan dengan pengelolaan data, aplikasi, proses bisnis, dan infrastruktur/teknologi.[19]sehingga mempengaruhi berbagai aktivitas pengelolaan organisasi mulai dari tingkat operasional hingga tingkat strategis organisasi[14]. Selain itu, ada beberapa tahapan yang terlibat dalam proses siklus hidup keamanan dalam proses pengembangan keamanan informasi. Dimulai dari serangkaian penilaian, perancangan, penerapan, dan pemeliharaan aset informasi berdasarkan prinsip keamanan[20]. Oleh karena itu, komponen kerangka praktik terbaik keamanan informasi tata kelola digital di Indonesia disusun sejalan dengan konsep-konsep tersebut, yang disesuaikan dengan beberapa standar, kerangka, undang-undang, pedoman, dan referensi praktik terbaik yang terkait dengan konteks nasional Indonesia.

Dalam melaksanakan kegiatan pengembangan kerangka praktik terbaik keamanan informasi pada sistem pemerintahan elektronik Indonesia, melibatkan berbagai kajian terdahulu yang merupakan hasil penggabungan kerangka kerja terkait dan rekomendasi dari para ahli yang ahli di bidang keamanan informasi. Ketika konsep kedua kerangka kerja diterapkan secara paralel, keduanya akan menciptakan sinergi yang menguntungkan seluruh area tingkat tinggi dalam sebuah organisasi. Dengan menggabungkan prinsip-prinsip ini, seperangkat aturan komprehensif yang mencakup dan mengamankan bisnis sekaligus menumbuhkan budaya IS dapat diciptakan untuk implementasi ISG. Namun demikian, hal ini mempunyai potensi untuk disalahartikan, sehingga organisasi harus bertindak ke satu arah terlebih dahulu, misalnya berorientasi bisnis, kemudian ke arah lain, misalnya berorientasi keamanan, dan akhirnya melakukan

sintesis [21]. Berdasarkan kenyataan tersebut, penelitian ini diawali dengan mencari kerangka utama tata kelola keamanan informasi yang berasal dari kombinasi model tata kelola keamanan CPS [22] dan beberapa komponen CSF keamanan informasi yang berasal dari [23] Dan [24] berdasarkan konsep yang dikembangkan oleh Solms (2013) [25]. Kemudian komponen-komponen utamanya di-benchmark [26] dengan praktik terbaik ISG lainnya yang berasal dari negara terkait lainnya untuk mendapatkan wawasan praktis dan pembelajaran guna menyempurnakan komponen penting ini. Pada tahap akhir, komponen utama tata kelola keamanan informasi ini dilengkapi dengan parameter keamanan informasi [27], komponen terkait lainnya [28], dan rekomendasi [29], khususnya dalam konteks Indonesia, sehingga komponen utama dan masing-masing subkomponen penyusunnya dapat digabungkan seluruhnya sesuai dengan kebutuhan e-Government Indonesia. Metode penelitian ini dapat diilustrasikan pada Gambar 1, dilanjutkan dengan langkah-langkah penelitian secara rinci dalam melakukan langkah pertama metodologi penelitian (Gambar 2).



Gambar 1. Metodologi Penelitian



CSF Domains	CSF Subdomains
1. Responsibility & Accountability	Define roles & risk ownerships, resource allocation, information security governance committee, internal/external communication, risk management, policies enforcement
2. Awareness	Organizational culture , security culture
3. Compliance	Law & regulations, third-party engagement, data copy rights & privacy
4. Assessment (Auditing)	Evaluate alignment between security controls & business, evaluate policies & procedures, evaluate organization security architecture, evaluate business continuity & recovery plan, third-party auditing
5. Measurement	Awareness maturity, learned from previous threats, performance & processes
6. Reporting	Assessment report, management report, performance report
7. Monitoring	Incident management, business continuity, potential conflicts, controlling mechanisms & processes, IT Infrastructure & daily operation

Governing Principles
Consider IS as an organization-wide issue
Adopt risk-based approach
Set the direction of investment decisions
Conform & comply with IS requirements
Deliver quality and value to stakeholders
Provide timely and accurate information on IS
Evaluate current and future information threats
Promote continuous improvement in IS
Act in a professional and ethical manner
Foster an IS-positive culture
Review IS performance in relation to business outcomes
Protect classified information
Concentrate in critical business application
Develop systems securely

Gambar 2. Langkah-langkah penelitian rinci pada metodologi penelitian tahap pertama

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Penelitian yang dilakukan oleh [7] mengungkapkan bahwa keamanan harus dilihat sebagai fitur yang sangat diperlukan dalam konteks digital. Oleh karena itu, organisasi perlu mulai menyesuaikan tata kelola keamanan digital sesuai dengan kebutuhan mereka saat ini. Studi ini mendukung para praktisi dan pengambil keputusan tentang bagaimana organisasi dan pendekatan keamanan mereka terkena dampak digitalisasi. Oleh karena itu, pada bagian ini hasil dari setiap tahapan dibahas dalam setiap sub bagian untuk mendapatkan penjelasan yang jelas mengenai hasil tersebut.

4.1. Komponen utama dari tahap 1

Berdasarkan tahapan yang tertera pada metode penelitian, diperoleh hasil usulan kerangka praktik terbaik keamanan informasi di pemerintahan Indonesia, yang terdiri dari 6 (enam) kerangka utama dan kemudian sub-komponen dari masing-masing kerangka utama tersebut, yaitu evaluasi, pengarahan, observasi, kesesuaian kinerja, keterampilan tindakan (compliance), dan proses operasional (kebijakan dan prosedur). Enam kerangka praktik terbaik utama keamanan teknologi informasi bagi pemerintah Indonesia dapat dilihat pada Gambar 5. Keenam hal tersebut saling terkait satu sama lain sehingga jika salah satu komponen atau subkomponen diabaikan maka akan mempengaruhi kinerja secara keseluruhan. Hal ini berpotensi melemahkan sistem pemerintahan yang sudah berjalan. Oleh karena itu, perlu adanya koordinasi yang sinergis antara keduanya pada tingkat yang strategis agar keseimbangan dan kesesuaian antar keduanya dapat terjaga dengan baik sehingga tujuan pemerintah Indonesia dapat tercapai.

Setiap komponen dan subkomponen perlu dinilai efektivitasnya masing-masing agar sesuai dengan kebutuhan sistem.

Gambar 3. Komponen utama kerangka praktik terbaik keamanan teknologi informasi untuk pemerintah indonesia

4.2. Hasil dari tahap 2 (membandingkan hasil dari tahap pertama dengan praktik terbaik tata kelola TIK yang ada di negara tertentu)

Praktik tata kelola TIK saat ini di beberapa negara sedang menghadapi perubahan yang cepat akibat berbagai tantangan yang datang ke wilayah pemerintahan. Oleh karena itu, mereka perlu membangun sistem pemerintahan digital yang aman agar siap dan mengambil tindakan yang tepat ketika menghadapi masalah keamanan.Pada paragraf berikut disajikan pembahasan singkat mengenai praktik terbaik tata kelola keamanan teknologi informasi dan komunikasi dari negara-negara terkait dengan mempertimbangkan aspek-aspek kunci dalam pemerintahan digital Indonesia [30][31], yang terdiri dari Amerika Serikat, Malaysia dan Afrika karena sistem politik, indeks sumber daya manusia dan geolokasi yang masing-masing dekat dengan Indonesia.

Pemerintah Amerika mempunyai cara unik dalam mengatur fungsi keamanan fisik dan siber yang diterapkan pada banyak isu dan pemangku kepentingan yang saling bergantung. Langkah-langkah tersebut telah dikembangkan dan diterapkan sedemikian rupa selama bertahun-tahun. Hal ini terus ditingkatkan dan merupakan hasil dari komitmen yang terus menerus dari para pionir dari pejabat negara dan cabang administrasi pemerintahan, pendidikan, swasta dan organisasi nirlaba. Di lima negara bagian, gubernur telah mempunyai kepemimpinan dan tanggung jawab untuk masalah ini [32]. Aspek fungsional yang termasuk dalam kerangka keamanan terdiri dari Identifikasi, Perlindungan, Deteksi, Respons, dan Pemulihan dan masing-masing aspek tersebut disertai dengan komponen dan subkomponennya masing-masing [33].

Data dikumpulkan oleh [34] melalui analisis dokumen dan wawancara telah mengkonfirmasi bahwa ISG terdapat dalam beberapa dokumen sektor publik Malaysia. Unsur dalam ISG berasal dari perpaduan aspek keamanan informasi ICT dengan non-ICT sehingga suatu kebijakan ISG menjadi utuh dan tidak tumpang tindih. Pengembangan kerangka ISG telah menjadi program terpadu yang melibatkan lembaga pembuat kebijakan dalam administrasi sektor publik di Malaysia. Pembangunan terpadu telah menghasilkan kerangka ISG yang komprehensif untuk digunakan oleh lembaga-lembaga sektor publik di Malaysia. Komponennya adalah pendekatan tata kelola, praktik yang baik, manajemen risiko, manajemen organisasi, pelatihan dan kesadaran, metode implementasi, serta peraturan perundang-undangan. Keempat komponen tersebut akan menjalani siklus proses desain, implementasi, penilaian, dan tindak lanjut yang berkesinambungan. Elemen-elemen ini dapat digabungkan dengan prinsip-prinsip keamanan siber Malaysia [35].

Model keamanan informasi yang berlaku di Nigeria ditekankan pada aspek keamanan secara umum. Model tersebut menunjukkan bagaimana sistem e-Government berhubungan dengan pelanggannya dengan menggunakan otentikasi sertifikat dua arah dengan otentikasi pengguna yang valid untuk setiap layanan. Setelah titik otentikasi, pengguna masuk dan menjalankan layanan yang ditentukan. Sistem ini memastikan bahwa semua komunikasi antar pihak dalam infrastruktur e-Government dienkripsi. Kerangka kerja tersebut merekomendasikan penggunaan kunci sesi karena kunci sesi dihasilkan secara acak, sehingga menyulitkan penyerang untuk mencegat pesan di jaringan. Kerangka kerja ini memiliki middleware keamanan, yang pada dasarnya merupakan penghubung antara sistem infrastruktur kunci publik dan aplikasi. Semua aplikasi dijalankan untuk memastikan bahwa sistem secara umum aman. Middleware ini bertindak sebagai antarmuka antara aplikasi, kontrol akses, manajemen server, alat kriptografi, dan mekanisme fisik penting lainnya. Kontrol akses berbasis peran memungkinkan penugasan tanggung jawab yang tepat berdasarkan kebijakan yang ditentukan dalam kerangka strategis dan terutama didasarkan pada pertimbangan hierarki. Hal ini memungkinkan administrator sistem untuk mengelola akses pengguna secara dinamis, sehingga lebih mudah untuk melihat siapa, di mana, kapan, dan kapan koneksi dimulai. Pengguna valid yang mendapatkan akses juga diidentifikasi dan dilaporkan sebagaimana mestinya[36].

Komponen utama tata kelola keamanan teknologi informasi pada e-Government Indonesia hasil tahap pertama ini kemudian dibandingkan dengan negara lain dalam menangani permasalahan yang sama untuk menyempurnakannya. Melihat Tabel 1, Amerika memiliki seluruh komponen utama, sedangkan Malaysia dan Afrika Selatan memiliki beberapa komponen

utama. Namun demikian, negara-negara ini saling melengkapi dan dapat memvalidasi temuan penelitian bahwa pemerintahan digital Indonesia memerlukan seluruh komponen ini untuk melindungi sistem digital secara memadai dalam menjalankan operasional sehari-hari dengan para pemangku kepentingan terkait.

Tabel 1.Membandingkan komponen utama ISG

Negara / Komponen-komponen kunci	Amerika Serikat	Malaysia	Afrika Selatan	Indonesia (Hasil)
Evaluasi	√			diperlukan
Arah	√	√		diperlukan
Pengamatan	√	√	√	diperlukan
Proses operasional (kebijakan dan prosedur)	√	√		diperlukan
Keterampilan tindakan (kepatuhan)	√	√	√	diperlukan
Kesesuaian kinerja	√		√	diperlukan

4.3. Hasil dari tahap 3

Pada bagian ini, masing-masing komponen utama yang telah dijadikan acuan (benchmark) dengan negara-negara terkait tertentu akan dibahas satu per satu secara lebih rinci. Ketika membahas setiap komponen utama, maka dijabarkan dengan parameter keamanan informasi terkini, elemen terkait, serta rekomendasi dalam konteks Indonesia, khususnya untuk memperoleh gambaran lengkap/besar tentang kerangka praktik terbaik tata kelola keamanan informasi di pemerintahan Indonesia. Namun, kesenjangan dalam setiap subkomponen praktik terbaik juga dapat dilihat sebagai hasil lain yang tidak dapat dihindari. Namun demikian, kesenjangan ini dapat dimanfaatkan untuk pengembangan tata kelola keamanan informasi di masa depan di Indonesia dan negara terkait lainnya.

4.3.1. Subsub bagian 1 (Evaluasi)

Tahap evaluasi yang sering juga disebut tahap penilaian atau tahap audit ini berfungsi untuk melakukan evaluasi dengan menggunakan Cyber-Physical

System (CPS) terhadap kondisi saat ini dan masa yang akan datang. Setiap administrator sistem elektronik harus memeriksa dan membuat penilaian tentang penggunaan CPS saat ini dan masa depan dengan memasukkan strategi, pengisian, dan pengaturan penyediaan (internal, eksternal, atau keduanya). Acuan standar penilaian mengikuti CC (Common Criteria). Ini adalah kumpulan standar dan konfigurasi teknis yang dikenal secara global dan lokal yang memungkinkan penilaian keamanan produk dan teknologi informasi [22]. Bagaimana masyarakat dapat menilai keamanan informasi untuk administrasi publik memerlukan pendekatan sistematis yang meningkat berdasarkan kebutuhan perbaikan berkelanjutan [37]. Model evaluasi yang dikembangkan oleh Zuo [38] dapat dijadikan tolok ukur disertai dengan pendekatan multidimensi sosio-teknis [39]. Implementasi audit bergantung pada standar dan kerangka kerja organisasi, manajemen, dan keamanan infrastruktur TI yang canggih seperti Cobit dan ISO 17799 [40].

Berdasarkan peraturan pemerintah Indonesia no. 59 Tahun 2020 tentang Keamanan Informasi khususnya evaluasi yang diklaim sangat penting untuk mendukung pengelolaan sistem e-Government Indonesia, evaluasi harus diselaraskan dengan tujuan keamanan. Selain itu, evaluasi juga dapat dilakukan oleh pihak eksternal melalui penilaian tingkat kematangan agar dapat segera melakukan optimalisasi sistem keamanan informasi. Hingga saat ini, framework COBIT 5 [1] dan ISO 27001:2013 [41] secara umum digunakan untuk menganalisis tingkat kematangan sistem keamanan informasi khususnya dalam konteks Indonesia [42]. Meskipun demikian, cara lain yang dapat digunakan untuk menilai efisiensi keamanan informasi adalah sistem pakar [43]. Oleh karena itu, Indonesia perlu menggabungkan sistem tersebut dengan alat lain agar lima sub-komponen berikut dapat diukur dengan benar dan sesuai kebutuhan.

Kelima sub-komponen ini fokus pada evaluasi keselarasan antara kontrol keamanan dan bisnis, evaluasi kebijakan dan prosedur, evaluasi keamanan organisasi, evaluasi kelangsungan bisnis dan rencana pemulihan, serta audit pihak ketiga.

4.3.2. Subsub bagian 2 (Direction)

Tahap pengarahan secara langsung melayani penyusunan dan implementasi berbagai rencana dan kebijakan untuk memastikan penggunaan CPS dapat terhubung dengan tujuan sistem keamanan [22]. Selain itu, hal ini juga dapat dicapai dengan menyoroti dan mengatur poin-poin penting dari kebijakan keamanan informasi, termasuk tantangan utama dalam implementasinya dengan perlunya meninjau dan menetapkan kebijakan dalam proses yang berkelanjutan dan kerangka manajemen risiko yang menyeluruh [44]. Tahapan ini diperlukan untuk mengetahui kebutuhan yang harus ditingkatkan dari sistem keamanan informasi yang ada agar sistem dapat berjalan lebih baik lagi kedepannya.

4.3.3. Subsub bagian 3 (Observation)

Pada tahap pengamatan/pemantauan, terdapat dua fungsi utama teknologi informasi dalam sistem keamanan, yaitu memantau kesesuaian antara sistem dengan kebijakan dan memantau pelaksanaan sistem terhadap rencana [22]. Selain itu, pengamatan yang berkelanjutan dianggap sebagai faktor penting yang memungkinkan terjadinya potensi risiko, kerentanan, dan ancaman yang mungkin dihadapi oleh hampir semua institusi secara rutin [23]. Sebuah studi penelitian menganalisis teori privasi, kepercayaan, komitmen, dan kepatuhan untuk merumuskan model yang menjelaskan fenomena yang diamati di lingkungan kerja nyata. Penelitian dilakukan melalui pemantauan informasi organisasi dalam

praktiknya dan menghasilkan kesimpulan bahwa pemantauan informasi dapat meningkatkan praktik Manajemen Keamanan Informasi (ISM) dalam organisasi [45]. Jika praktik ISM berjalan dengan baik, maka praktik organisasi secara keseluruhan akan meningkat. Terdapat 5 (lima) subkomponen penting dalam komponen observasi ini yang dapat dilihat pada Tabel 2. Selain itu, metode pemantauan keamanan informasi yang direkomendasikan [46] [47] dapat dijadikan pedoman dalam pelaksanaan pemantauan keamanan informasi di Indonesia.

Tabel 2. Subkomponen Kegiatan Observasi

Subkomponen praktik terbaik	Parameter IS di Pemerintah Indonesia [27]	Elemen terkait untuk Indonesia [28]	Arah tindakan di Indonesia (Rekomendasi) [29]	Hasil/yang akan dicapai (kegiatan ITSG)
Manajemen insiden	-	ancaman/serangan: Ancaman/serangan fisik, Ancaman/serangan logis	-	Perlu pengembangan lebih lanjut
Keberlangsungan bisnis	-	mgmt. prosedur:Aset, Insiden, Kontinuitas Bisnis, Operasional, Manajemen Risiko.	-	Perlu pengembangan lebih lanjut
Potensi konflik	-	Lingkungan: Politik, Sosial, Ekonomi.	-	Perlu pengembangan lebih lanjut
Mekanisme dan proses pengendalian	-	-	Membentuk unit di bawah kementerian terkait untuk secara formal memantau dan mengendalikan infrastruktur nasional guna membantu menjamin keamanan dan ketahanan Indonesia.	Perlu pengembangan lebih lanjut
Infrastruktur TI dan operasi sehari-hari	Teknologi	Teknologi	-	Perlu pengembangan lebih lanjut

Berdasarkan hasil penelitian yang ditunjukkan pada Tabel 2, terlihat bahwa masing-masing sub komponen best practice perlu dikembangkan lebih lanjut karena belum lengkapnya kegiatan konkrit yang tersedia saat ini. Dalam hal beberapa subkomponen praktik terbaik seperti Manajemen Insiden, Kelangsungan Bisnis, Potensi Konflik, serta Mekanisme dan Proses

Pengendalian, ketersediaan kegiatan-kegiatan ini di pemerintah Indonesia masih belum ada, meskipun penelitian dan rekomendasi terkait telah muncul. Terlebih lagi, dalam hal infrastruktur TI dan subkomponen operasi sehari-hari, Indonesia telah memberikan perhatian pada bagian ini dari sudut pandang teknologi, namun aktivitas terkait masih kurang. Oleh karena itu, seluruh kegiatan dalam subkomponen praktik terbaik ini perlu dikembangkan dengan menggabungkan parameter, elemen, dan rekomendasi terkait. Misalnya, kita dapat mengembangkan berbagai aktivitas berdasarkan elemen terkait yang tersedia dalam manajemen insiden, seperti cara menangani ancaman fisik dan logis. Selain itu, dalam mekanisme pengendalian dan subkomponen proses, unsur-unsur terkait perlu dikembangkan sedemikian rupa sehingga membentuk unit yang memantau dan mengendalikan infrastruktur TI nasional.

4.3.4. Subsub Bagian 4 (Kesesuaian Kinerja)

Kinerja dan perubahan organisasi sama-sama sedang berlangsung, dan keduanya diperlukan untuk melacak dan mengevaluasi apakah prinsip, kebijakan, dan prosedur ISG berjalan sesuai dengan indikator dan kriteria yang telah ditentukan [23]. Mengukur kinerja keamanan informasi merupakan komponen penting dari keamanan informasi dalam sistem manajemen organisasi. Menurut sebuah penelitian, keamanan informasi didefinisikan dan diterapkan dengan sengaja, namun pengukurannya terutama diterapkan pada tingkat teknis dan operasional, sementara manajemen strategis masih belum memadai [39]. Oleh karena itu, tiga subkomponen best practice domain kesesuaian kinerja yang dapat dilihat pada Tabel 3 merupakan tujuan yang penting untuk dicapai. Penerapan aktivitas kesesuaian kinerja melibatkan pengukuran dan pelaporan informasi sehingga kinerja dapat dibandingkan pada setiap periode waktu.

Tabel 3. Subkomponen Kegiatan Kesesuaian Kinerja

Subkomponen praktik terbaik	Parameter IS di Pemerintah Indonesia [27]	Elemen terkait untuk Indonesia [28]	Arah tindakan di Indonesia (Rekomendasi) [29]	Hasil/yang akan dicapai (kegiatan ITSG)
Memberikan informasi yang tepat waktu & akurat tentang kinerja IS	-	Pengukuran: kematangan kesadaran, pembelajaran dari ancaman, kinerja & proses sebelumnya.	-	Perlu pengembangan lebih lanjut
	-	Pelaporan: laporan penilaian, laporan pengukuran, laporan kinerja.	Menciptakan sistem pelaporan tunggal bagi penyelenggara sistem elektronik layanan publik untuk melaporkan dan mengungkapkan insiden kejahatan dunia maya dan pelanggaran data, sehingga dapat diambil tindakan.	Perlu pengembangan lebih lanjut
Tinjau kinerja IS dalam kaitannya dengan hasil bisnis	-	-	Meninjau undang-undang yang ada untuk memastikan bahwa undang-undang tersebut tetap relevan dan efektif dalam memerangi kejahatan dunia maya.	Perlu pengembangan lebih lanjut
Mempromosikan perbaikan berkelanjutan dalam IS	-	-	Memperkuat kemampuan penegakan hukum dan jaksa untuk menyelidiki kejahatan dunia maya dan membawa mereka yang bertanggung jawab ke pengadilan.	Perlu pengembangan lebih lanjut

Demi kesesuaian kinerja, pemerintah Indonesia masih belum mengetahui kegiatan apa yang harus dilakukan untuk menangani masing-masing subkomponen praktik terbaik ini, khususnya dalam hal memberikan informasi yang tepat waktu dan akurat mengenai kinerja SI, meninjau kinerja SI dalam kaitannya dengan hasil bisnis, dan mempromosikan perbaikan berkelanjutan dalam IS. Oleh karena itu, meskipun unsur-unsur atau rekomendasi tertentu yang terkait tidak tersedia di beberapa bagian, kita harus mengembangkan kegiatan-kegiatan tersebut berdasarkan kedua hal tersebut. Misalnya, dalam hal memberikan informasi yang tepat waktu dan akurat mengenai kinerja sistem informasi, kita harus menggabungkan istilah-istilah ini antara elemen pelaporan dan rekomendasi dalam sistem pelaporan untuk mengembangkan berbagai aktivitas yang berkaitan dengan bagian subkomponen ini. Hal ini tentunya

dilakukan tanpa mengabaikan unsur-unsur terkait keamanan informasi di Indonesia.

4.3.5. Subsub bagian 5 (Keterampilan tindakan/kepatuhan)

Kepatuhan terhadap peraturan perundang-undangan sangatlah penting dan menjadi salah satu elemen kunci untuk memastikan ISG organisasi efektif dan berkelanjutan [23]. Aturan dan regulasi eksternal sering kali mengatur kemampuan organisasi untuk mengumpulkan informasi, melakukan investigasi, dan mengendalikan jaringan, serta aktivitas lain atas informasi yang diperoleh dari keamanan teknologi. Selain itu, organisasi harus mengembangkan beberapa persyaratan untuk mematuhi aturan-aturan ini untuk melindungi dan merancang sistem dan aplikasi baru, dan juga menentukan berapa lama untuk menyimpan data, atau untuk melakukan enkripsi dan tokenisasi data sensitif [48].

Dua jenis kepatuhan utama adalah kepatuhan terhadap peraturan dan kepatuhan industri. Ketidakpatuhan mempunyai konsekuensi yang berbeda-beda tergantung pada seperangkat aturan yang bersangkutan. Dalam hal kepatuhan industri, hilangnya hak istimewa terkait kepatuhan dapat terjadi. Dalam hal kepatuhan terhadap peraturan, ketidakpatuhan dapat mengakibatkan hukuman yang lebih berat, termasuk penahanan karena melanggar hukum terkait [48].

Menurut sebuah penelitian, tekanan koersif, tekanan normatif, dan tekanan mimesis mempunyai pengaruh yang signifikan terhadap kepatuhan keamanan informasi organisasi. Ini menyiratkan bahwa keunggulan kepatuhan keamanan informasi mendorong manajemen untuk meningkatkan komitmen mereka terhadap kepatuhan keamanan informasi [49]. Namun tingkat kesadaran dalam hal kepatuhan terhadap keamanan informasi juga perlu mendapat perhatian [50].

Berdasarkan konsep-konsep tersebut, subkomponen penting yang berkaitan dengan kepatuhan dapat dilihat pada Tabel 4.

Tabel 4. Subkomponen Kegiatan Kepatuhan

Subkomponen praktik terbaik		Parameter IS di Pemerintah Indonesia [27]	Elemen terkait untuk Indonesia [28]	Arah tindakan di Indonesia (Rekomendasi) [29]	Hasil/yang akan dicapai (kegiatan ITSG)
Sesuaikan & patuhi persyaratan IS internal & eksternal	hukum & peraturan	-	Hukum & Peraturan	Kembangkan strategi pemasaran standar untuk mempromosikan privasi online untuk melindungi data pribadi.	Perlu pengembangan lebih lanjut
	Keterlibatan pihak ketiga	-	Kerja sama:Pemerintahan, Nasional, dan Internasional.	Menciptakan dan membangun kemampuan sipil dan militer yang berdedikasi untuk membantu memastikan bahwa Indonesia memiliki kemampuan untuk melindungi kepentingan nasional di dunia maya.	Perlu pengembangan lebih lanjut
	Hak penyalinan data dan privasi	-	Hukum: Penipuan Komputer, Akses Ilegal, Interferensi Data, Pelanggaran Hak Cipta, Pornografi Anak.	-	Perlu pengembangan lebih lanjut

Subkomponen praktik terbaik dalam konteks kepatuhan hanya ada satu, yaitu mematuhi dan mematuhi persyaratan keamanan informasi internal dan eksternal. Subkomponennya terdiri dari hukum dan peraturan, keterlibatan pihak ketiga, hak salinan data, dan privasi. Berdasarkan tabel di atas, Indonesia masih belum memberikan perhatian terhadap ketiga elemen penyusun subkomponen ini karena belum adanya parameter keamanan informasi. Dalam konteks ini, pemerintah Indonesia perlu mengembangkan kegiatan-kegiatan terkait dalam subkomponen ini dengan menggabungkan parameter, elemen, dan rekomendasi terkait. Misalnya, dalam keterlibatan pihak ketiga, unsur kerja sama dan rekomendasi dalam menciptakan dan membangun kemampuan sipil dan militer yang berdedikasi perlu digabungkan dan diperluas sehingga dapat menciptakan

berbagai kegiatan dalam konteks ini sesuai dengan kebutuhan pemerintah Indonesia.

4.3.6. Subsub bagian 6 (proses operasional (kebijakan dan prosedur))

Menentukan kebijakan atau prosedur mungkin relevan untuk melindungi jenis informasi tertentu (misalnya kode sumber untuk produk perangkat lunak yang kompleks). Dalam hal ini, organisasi harus mempertimbangkan seberapa berharganya informasi tersebut, apa dampak buruk yang dialami, dan apakah penurunan risiko sepadan dengan biaya (uang atau ketidaknyamanan) dari tindakan perlindungan seperti pembatasan akses dan lain-lain [51]. Sebagian besar organisasi menyadari perlunya pemantauan dan peningkatan manajemen risiko dan proses keamanan internal dengan menggunakan prosedur tata kelola keamanan [52]. Selain itu juga perlu didukung dengan kebijakan yang dapat dikembangkan [53] dan digunakan kembali [54] untuk beradaptasi dengan perubahan organisasi. Terdapat 10 (sepuluh) subkomponen penting dalam kegiatan operasional pengambilan kebijakan dan prosedur di bidang keamanan teknologi informasi seperti terlihat pada Tabel 5.

Tabel 5. Subkomponen Kegiatan Proses Operasional

Subkomponen praktik terbaik	Parameter IS di Pemerintah Indonesia[27]	Elemen terkait untuk Indonesia [28]	Arah tindakan di Indonesia (Rekomendasi) [29]	Hasil/yang akan dicapai (kegiatan ITSG)
Pertimbangkan IS sebagai isu organisasi yang luas:				
a. mengintegrasikan IS dengan aktivitas bisnis	Program kerja dan strategi	-	Mengembangkan strategi keamanan siber nasional (NCSS).	Perlu pengembangan lebih lanjut
b. penyelarasan strategis yang sedang berlangsung	-	-	Mempromosikan persyaratan keamanan siber dalam proses pengadaan pemerintah untuk mengelola pertahanan siber nasional.	Perlu pengembangan lebih lanjut
c. menentukan peran & tanggung jawab IS yang jelas dan bertanggung jawab.	-	Layanan keamanan: Mencegah, Mendeteksi, Respons. Sasaran keamanan:	Meningkatkan tingkat kepercayaan yang lebih besar terhadap layanan online, seperti layanan e-Government dan e-commerce.	Perlu

		Kerahasiaan, Integritas, Ketersediaan, Privasi, Keaslian, Non-Penyangkalan.		pengembangan lebih lanjut
Bertindak secara profesional dan etis	"Tata Kelola ISIS"	Organisasi:Komite (Kebijakan & Koord.), Pusat Operasi, Tim Tanggap Darurat.	Memperkuat peran dan fungsi koordinasi ID-SIRTII/CC sebagai CERT nasional.	Perlu pengembangan lebih lanjut
Memberikan kualitas & nilai kepada pemangku kepentingan: a. Komunikasi yang efektif	-	-	Mengembangkan strategi komunikasi keamanan siber untuk memperkuat dan memperluas kampanye keamanan siber nasional.	Perlu pengembangan lebih lanjut
b. Rencana kelangsungan bisnis/pemulihan bencana yang efektif	-	-	-	Perlu pengembangan lebih lanjut
Mengadopsi pendekatan berbasis risiko	"Tata Kelola Risiko ISIS"	-	-	Perlu pengembangan lebih lanjut
Lindungi informasi rahasia	"Tata Kelola Aset"	Aset: Berwujud, Tidak Berwujud.	Membuat daftar resmi CNI melalui konsultasi multipihak, dan bekerja sama dengan perusahaan yang memiliki dan mengelola CNI.	Perlu pengembangan lebih lanjut
Berkonsentrasi pada aplikasi bisnis penting	-	-	Menetapkan prioritas aset tanggap darurat jika terjadi kegagalan layanan yang bertujuan untuk mengurangi dampak.	Perlu pengembangan lebih lanjut
Kembangkan sistem dengan aman	Kerangka ISG	-	-	Perlu pengembangan lebih lanjut
Menumbuhkan budaya positif IS (budaya organisasi dan keamanan[55])	-	Budaya keamanan: Nilai Kolektif, Norma & Pengetahuan, Asumsi & Keyakinan Dasar, Artefak & Kreasi.	Mengembangkan portal online tunggal yang otoritatif untuk meningkatkan kesadaran dunia maya di kalangan pemerintah, dunia usaha, dan masyarakat sipil di seluruh negeri.	Perlu pengembangan lebih lanjut
			Meningkatkan kesadaran di kalangan pejabat senior pemerintah dan anggota dewan operator infrastruktur nasional yang penting mengenai risiko dunia maya, dan tindakan yang dapat mereka ambil untuk melindungi informasi sensitif terhadap keamanan.	
	-	Kompetensi manusia: Sec. Operasi & Manajemen,	Memberikan solusi keamanan siber berbasis insentif untuk produk keamanan siber lokal atau pasar asuransi siber.	

		Peretasan Etis, Forensik Komputer, Sec. Pemrograman, Bagian. Implementasi & Konferensi, Sec. Arsitektur & Pengembangan, Detik. Kebijakan & Pengembangan, Kriptografi, Bagian. Analisis.	Melakukan latihan manajemen krisis di tingkat nasional dengan mengundang pemangku kepentingan nasional yang relevan untuk memastikan persiapan respons terhadap insiden siber nasional dikelola dengan baik dan kuat.	Perlu pengembangan lebih lanjut
			Mempromosikan program pelatihan dan pendidikan keamanan siber yang dirancang untuk semua karyawan di semua tingkatan di organisasi pemerintah, perusahaan milik negara, penyedia infrastruktur penting swasta, dan usaha kecil dan menengah.	
Menetapkan arah keputusan investasi	-	-	Identifikasi pusat keunggulan dalam penelitian dan pendidikan keamanan siber untuk menemukan kekuatan dan menyediakan investasi terfokus untuk mengatasi kesenjangan.	Perlu pengembangan lebih lanjut
			Membuat pendaftaran tingkat nasional untuk pakar jaminan informasi dan keamanan siber di sektor publik dan swasta sebagai cara untuk mendatangkan talenta baru ke dalam profesi ini.	

Dalam konteks ini, untuk beberapa bagian, lebih mudah untuk membuat berbagai aktivitas yang berkaitan dengan setiap subkomponen praktik terbaik karena adanya serangkaian parameter, elemen, dan rekomendasi keamanan informasi seperti perlindungan informasi rahasia. Karena parameter IS terkait di pemerintahan Indonesia belum komprehensif, maka aktivitas terkait belum dapat dihasilkan. Namun demikian, di sisi lain, diperlukan upaya yang lebih besar untuk menciptakan kegiatan tersebut karena tidak adanya parameter, elemen, atau rekomendasi terkait seperti kelangsungan bisnis yang efektif atau rencana pemulihan bencana. Oleh karena itu, pengembangan lebih lanjut berbagai kegiatan di setiap subkomponen menjadi penting untuk mengatur keamanan informasi dalam sistem pemerintahan digital Indonesia secara holistik.

Secara keseluruhan penelitian ini memberikan hasil secara umum mengenai enam komponen utama dan masing-masing subkomponen pendukung.

Apalagi dengan menggunakan konsep analisis sebab-akibat[56]dalam menganalisis keterkaitan data antara enam komponen utama beserta subkomponennya masing-masing, diperoleh kesimpulan bahwa terdapat hubungan yang kuat antara komponen yang satu dengan komponen yang lain. Apabila salah satu komponen diabaikan atau tidak dilaksanakan dengan baik maka akan mengakibatkan terganggunya sistem keamanan informasi secara keseluruhan. Hal ini terlihat dari proses komponen-komponen (baik berupa kebijakan maupun prosedur) yang sedang berjalan. Namun demikian, jika komponen-komponen tersebut tidak dikaji ulang secara berkala, maka tingkat efektivitas pencapaian kinerja pemerintah akan sulit diukur. Hal ini disebabkan kesulitan dalam mencari solusi atas berbagai keluhan pengguna.

Berdasarkan hasil penelitian yang diperoleh dari ketiga tahapan tersebut, terlihat bahwa beberapa aktivitas yang dihasilkan belum optimal pada setiap subkomponen ditinjau dari parameter IS yang ada untuk pemerintah Indonesia, elemen terkait, dan serangkaian rekomendasi. Oleh karena itu, seluruh aktivitas di dalam setiap subkomponen harus digabungkan dan dikembangkan sesuai dengan kebutuhan yang telah dijelaskan di setiap komponen untuk memenuhi gambaran yang lebih luas mengenai persyaratan tata kelola keamanan TI. Apalagi hal ini disebabkan belum adanya sinergi antara penerapan tata kelola TI saat ini dengan tata kelola keamanan TI, sehingga kegiatan terkait tata kelola keamanan informasi perlu ditingkatkan efektivitasnya dalam konteks pemerintahan digital Indonesia dan kebutuhan masa depan. Selain itu, keamanan teknologi informasi di Indonesia perlu terus dikembangkan seiring dengan perkembangan infrastruktur teknologi informasi dan pemenuhan gaya hidup masyarakat di masa depan.

BAB V PENUTUP

Penelitian ini menyimpulkan bahwa terdapat enam komponen utama penyusunan kerangka praktik terbaik tata kelola keamanan informasi yang dapat digunakan oleh pemerintah Indonesia, yang terdiri dari evaluasi, pengarahan, pemantauan, kesesuaian kinerja, keterampilan tindakan (compliance), dan proses operasional (kebijakan dan prosedur) komponen. Masing-masing komponen utama dan subkomponen tersebut saling mendukung satu sama lain, sehingga semua hal tersebut harus dilakukan secara sinergis dan proporsional. Dalam masing-masing komponen utama dan subkomponen pendukung tersebut, dapat dihasilkan kegiatan-kegiatan yang relevan namun masih memerlukan pengembangan lebih lanjut. Mengingat masih adanya kekurangan kegiatan pada masing-masing subkomponen, maka perlu dilakukan pengembangan secara terus menerus untuk kebutuhan di masa yang akan datang. Efektivitasnya juga perlu dianalisis sesuai dengan kebutuhan pemerintah pusat Indonesia di masa depan. Namun demikian, kerangka praktik terbaik tata kelola keamanan informasi ini harus selaras dengan tata kelola teknologi informasi, yang berdampak pada arsitektur TI dalam organisasi.

Daftar Pustaka

[1] R. Umar, I. Riadi, and E. Handoyo, "Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI)," *J. Sist. Inf. Bisnis*, vol. 9, no. 1, p. 47, 2019.

[2] F. Khan, R. Lakshmana Kumar, S. Kadry, Y. Nam, and M. N. Meqdad, "Cyber physical systems: A smart city perspective," *Int. J. Electr. Comput. Eng.*, vol. 11, no. 4, pp. 3609–3616, 2021.

[3] M. Rizal and Y. Yani, "Cybersecurity Policy and Its Implementation in Indonesia," *JAS (Journal ASEAN Studies).*, vol. 4, no. 1, p. 61, 2016.

[4] A. B. Setiawan, Kautsarina, O. Rafizan, and A. S. Sastrosubroto, "Development of the information and communication technology service industry in Indonesia," *Aust. J. Telecommun. Digit. Econ.*, vol. 5, no. 3, pp. 50–82, 2017.

[5] D. Kardono, "Materi 5: Keamanan SPBE," *19 November 2020*, 2020. https://www.menpan.go.id/site/download/file/6341-materi-5-keamanan-spbe (accessed Jan. 20, 2021).

[6] W. Lidster and S. S. M. Rahman, "Obstacles to Implementation of Information Security Governance," *Proc. - 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust. 2018*, pp. 1826–1831, 2018.

[7] S. Leonelli, "Data Governance is Key to Interpretation: Reconceptualizing Data in Data Science," *Harvard Data Sci. Rev.*, vol. 1, no. 1, Jun. 2019.

[8] S. De Haes, W. Van Grembergen, J. Anant, and T. Huygh, *Enterprise Governance of Information Technology. Achieving Alignment and Value in Digital Organizations*. Switzerland: Springer Nature, 2020.

[9] N. Shariffuddin and A. Mohamed, "IT Security and IT Governance Alignment: A Review," *Proceedings of the 3rd International Conference on Networking, Information Systems & Security*, no. 24, pp. 1-8, 2020.

[10] B. Lundgren and N. Möller, "Defining Information Security," *Sci. Eng. Ethics*, vol. 25, no. 2, pp. 419–441, 2019.

[11] M. Zammani and R. Razali, "An empirical study of information security management success factors," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 6, no. 6, pp. 904–913, 2016.

[12] T. Campbell, *Practical Information Security Management: A Complete Guide to Planning and Implementation*. Australia: Apress Publisher, 2016.

[13] M. Zaydi and B. Nassereddline, "A Conceptual Hybrid Approach for Information Security Governance Introduction," *Int. J. Math. Comput. Sci.*, vol. 16, no. 1, pp. 47–66, 2021.

[14] S. H. von Solms and R. von Solms, *Information security governance*. New York: Springer Science & Business Media, LLC, 2009.
[15] H. Ardiyanti, "Cyber-Security Dan Tantangan Pengembangannya Di Indonesia," *Politica*, vol. 5, no. 1, pp. 95–110, 2014.
[16] Z. Mounia and N. Bouchaib, "A New Comprehensive Solution to Handle Information Security Governance in Organizations," *Proceedings of the 2nd International Conference on Networking, Information Systems & Security*, no. 50, pp. 1-5, 2019.
[17] C. Wang and X. Jin, "The Researches on Public Service Information Security in the Context of Big Data," in *Proceedings of the 2020 2nd International Conference on Big Data and Artificial Intelligence*, 2020, pp. 86–92.
[18] A. B. Setiawan, "Dalam Penerapan E-Government," *J. Masy. Telemat. dan Inf.*, vol. 4, no. 2, pp. 109–126, 2013.
[19] E. Prima, R. Lumanto, and Z. A. Hasibuan, "Evaluation of Government Public Key Infrastructure Implementation based on eGovAMAN Framework," *4th International Symposium on Chaos Revolution in Science, Technology and Society*. Chaosware, 2013.
[20] E. Prima, Y. G. Sucahyo, and Z. A. Hasibuan, "Mapping the certification authority for e-government procurement system into eGovAMAN framework," in *2013 International Conference on Advanced Computer Science and Information Systems (ICACSIS)*, 2013, pp. 61–65.
[21] DHS, "State Cybersecurity Governance Case Studies," 2017.
[22] Carnegie Mellon University, "Cyber Resilience Review," 2020. [Online]. Available: www.dhs.gov/pcii.
[23] A. Jamil and Z. Mohammad Yusof, "Information Security Governance Framework of Malaysia Public Sector," *Asia-Pacific J. Inf. Technol. Multimed.*, vol. 07, no. 02, pp. 85–98, 2018.
[24] S. Perumal, S. A. Pitchay, G. N. Samy, B. Shanmugam, P. Magalingam, and S. H. Albakri, "Transformative cyber security model for Malaysian government agencies," *Int. J. Eng. Technol.*, vol. 7, no. 4, pp. 87–92, 2018.
[25] Sam Neekpoa Deekue, "A strategic framework for e-government security (the case in Nigeria)," University of Bedfordshire, 2016.
[26] J. Van't Wout, M. Waage, H. Hartman, M. Stahlecker, and A. Hofman, *The integrated architecture framework explained: Why, what, how*. Berlin Heidelberg: Springer-Verlag, 2010.
[27] B. Rahardjo, *Keamanan Informasi & Jaringan*. Bandung: PT Insan Infonesia, 2017.
[28] Y. Li, T. Stafford, B. Fuller, and S. Ellis, "Information Securing in Organizations: A Dialectic Perspective," in *Proceedings of the 2019 on*

Computers and People Research Conference, 2019, pp. 125–130.
[29] A. B. Setiawan, A. Syamsudin, and A. S. Sastrosubroto, "Information security governance on national cyber physical systems," *2016 Int. Conf. Inf. Technol. Syst. Innov (ICITSI)*, 2016.
[30] S. AlGhamdi, K. T. Win, and E. Vlahu-Gjorgievska, "Information security governance challenges and critical success factors: Systematic review," *Comput. Secur.*, vol. 99, 2020.
[31] G. Gashgari, R. Walters, and G. Wills, "A proposed best-practice framework for information security governance," *IoTBDS 2017 - Proc. 2nd Int. Conf. Internet Things, Big Data Secur.*, no. IoTBDS, pp. 295–301, 2017.
[32] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *Comput. Secur.*, vol. 38, pp. 97–102, 2013.
[33] Capgemini, "Information Security Benchmark" *Research Report*, 2019.
[34] BSSN, "Indeks KAMI Versi 4" *Indonesia Security Guideline Document*, 2019.
[35] F. Setiadi, A. Rubhasy, and Z. A. Hasibuan, "Identifying and validating components for national cyber security framework," *Proc. 3rd Int. Conf. Informatics Comput. ICIC 2018*, pp. 1–5, 2018.
[36] Y. Nugraha, "The Future of Cyber Security Capacity in Indonesia" *Research Report*, 2016.
[37] E. K. Szczepaniuk, H. Szczepaniuk, T. Rokicki, and B. Klepacki, "Information security assessment in public administration," *Comput. Secur.*, vol. 90, 2020.
[38] J. Zuo, Y. Lu, H. Gao, R. Cao, Z. Guo, and J. Feng, "Comprehensive information security evaluation model based on multi-level decomposition feedback for IoT," *Comput. Mater. Contin.*, vol. 65, no. 1, pp. 683–704, 2020.
[39] K. Prislan, A. Mihelič, and I. Bernik, "A real-world information security performance assessment using a multidimensional socio-technical approach," *PLoS ONE*, vol. 15, no. 9 September. 2020.
[40] M. Gulzira, B. Gulmira, S. Altynbek, and O. Assel, "The Audit Method of Enterprise's Information Security," *Proceedings of the 6th International Conference on Engineering & MIS*, no. 9, pp. 1-5, 2020.
[41] V. Monev, "Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002," in *2020 International Conference on Information Technologies (InfoTech)*, 2020, pp. 1–5.
[42] D. Sulistyowati, F. Handayani, and Y. Suryanto, "Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS, " *Int. J. Informatics Vis.*, vol. 4,

no. 4, pp. 225–230, 2020.
[43] A. Erulanova, G. Soltan, A. Baidildina, M. Amangeldina, and A. Aset, "Expert System for Assessing the Efficiency of Information Security," in *2020 7th International Conference on Electrical and Electronics Engineering (ICEEE)*, Apr. 2020, pp. 355–359.
[44] T. Tagarev and D. Polimirova, "Main Considerations in Elaborating Organizational Information Security Policies," in *Proceedings of the 20th International Conference on Computer Systems and Technologies*, 2019, pp. 68–73.
[45] S. E. Change, A. Y. Liu, and Y. T. J. Jang, "Exploring trust and information monitoring for information security management," *Proc. - 2017 10th Int. Congr. Image Signal Process. Biomed. Eng. Informatics (CISP-BMEI 2017)*, pp. 1–5, 2018.
[46] V. G. Eryshov and D. V. Ilina, "Method of the information security monitoring process in information and telecommunication systems based on the application of methods of markov random processes," *2020 Wave Electron. its Appl. Inf. Telecommun. Syst. WECONF 2020*, pp. 1-4, 2020.
[47] F. O. Sönmez, "A conceptual model for a metric based framework for the monitoring of information security tasks' efficiency," *Procedia Comput. Sci.*, vol. 160, pp. 181–188, 2019.
[48] Jason Andreas, *Foundations of Information Security*. San Francisco: No Starch Press, 2019.
[49] A. AlKalbani, H. Deng, B. Kam, and X. Zhang, "Information Security Compliance in Organizations: An Institutional Perspective," *Data Inf. Manag.*, vol. 1, pp. 104–114, 2017.
[50] M. Lubis, R. Fauzi, P. Liandani, and A. Lubis, "Information Security Awareness (ISA) towards the Intention to Comply and Demographic Factors: Statistical Correspondence Analysis," *Proceedings of the 8th International Conference on Computer and Communications Management*, 2020, pp. 79–84.
[51] J. R. Vacca, *Computer and Information Security Handbook (Third Edition)*, Third Edition. Boston: Morgan Kaufmann, 2017.
[52] M. Asgarkhani, E. Correia, and A. Sarkar, "An overview of information security governance," *2017 Int. Conf. Algorithms, Methodol. Model. Appl. Emerg. Technol. ICAMMAET 2017*, vol. 2017-January, pp. 1–4, 2017.
[53] H. Paananen, M. Lapke, and M. Siponen, "State of the art in information security policy development," *Comput. Secur.*, vol. 88, p. 101608, 2020.
[54] J. Lobo, E. Bertino, and A. Russos, "On security policy migrations," *Proc. ACM Symp. Access Control Model. Technol. SACMAT*, pp. 179–188, 2020.

[55] M. N. Masrek, Q. N. Harun, and M. K. Zaini, “Information Security Culture for Malaysian Public Organization: a Conceptual Framework,” *4Th Int. Conf. Educ. Soc. Sci. (Intcess 2017)*, February 2017, pp. 156–166.
[56] W. Jatmiko, H. B. Santoso, S. C. Purbarani, A. R. Syulistyo, D. Marhaeni, D. Firmansyah, M. Yusuf, N. A. Laili, “Penulisan Artikel Ilmiah”. Depok: UI Publishing, 2015.
[55] https://www.cisco.com/c/en/us/products/security/what-is-it-security.html#~types-of-it-security diakses tanggal 5 Februari 2024.
[55] https://www.ibm.com/topics/it-security diakses tanggal 5 Februari 2024
[55] https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security diakses tanggal 5 Februari 2024.

BIODATA PENELITI

PUSAT PENELITIAN DAN PENERBITAN LP2M
UNIVERSITAS ISLAM NEGERI AR-RANIRY BANDA ACEH

A. Identitas Diri

1.	Nama Lengkap *(dengan gelar)*	**Rika Yuliana**
2.	Jenis Kelamin L/P	P
3.	Jabatan Fungsional	Lektor
4.	NIP	198407132014032001
5.	NIDN	2013078403
6.	NIPN *(ID Peneliti)*	
7.	Tempat dan Tanggal Lahir	Kuala Simpang, 13 Juli 1984
8.	E-mail	rika.yuliana@ar-raniry.ac.id
9.	Nomor Telepon/HP	081262600357
10.	Alamat Kantor	Gedung Fakultas Sains dan Teknologi
11.	Nomor Telepon/Faks	
12.	Bidang Ilmu	Teknologi Informasi
13.	Program Studi	Teknologi Informasi
14.	Fakultas	Fakultas Sains dan Teknologi

B. Riwayat Pendidikan

No.	Uraian	S1	S2	S3
1.	Nama Perguruan Tinggi	IPB	ITB	
2.	Kota dan Negara PT	Bogor, Indonesia	Bandung, Indonesia	
3.	Bidang Ilmu/ Program Studi	Teknologi Industri Pertanian	Informatika	
4.	Tahun Lulus	2006	2012	

C. Pengalaman Penelitian dalam 3 Tahun Terakhir

No.	Tahun	Judul Penelitian	Sumber Dana
1.			
2.			
3.			
dst.			

D. Pengalaman Pengabdian Kepada Masyarakat dalam 3 Tahun Terakhir

No.	Tahun	Judul Pengabdian	Sumber Dana
1.	2018	Sosialisasi proditeknologi informasi	prodi
2.	2022	Islam dana sosial media	prodi
3.	2024	Stunting dan teknologi digital	prodi

dst.			

E. Publikasi Artikel Ilmiah dalam Jurnal dalam 5 Tahun Terakhir

No.	Judul Artikel Ilmiah	Nama Jurnal	Volume/Nomor/Tahun/Url
1.			
2.			
dst.			

F. Karya Buku dalam 5 Tahun Terakhir

No.	Judul Buku	Tahun	Tebal Halaman	Penerbit
1.				
2.				
dst.				

G. Perolehan HKI dalam 10 Tahun Terakhir

No.	Judul/Tema HKI	Tahun	Jenis	Nomor P/ID
1.				
2.				
dst.				

Demikian biodata ini saya buat dengan sebenarnya.

Banda Aceh, 15 Januari 2024
Ketua/Anggota Peneliti,

Rika Yuliana
NIDN. 1984078403