Pembentukan Ekosistem *Local Government Information Sharing and Analysis Center* (LocalGov-ISAC) dengan *Toolkit* ENISA ISAC *in a Box* pada Sektor Pemerintah Daerah Indonesia

Fandi Aditya Putra
Badan Siber dan Sandi Negara, fandi.aditya@bssn.go.id

Abstrak

Information Sharing and Analysis Center (ISAC) merupakan *best practice* yang dapat diterapkan untuk membantu organisasi dalam mengatasi dampak serangan siber, salah satunya yaitu pada layanan sistem pemerintahan berbasis elektronik sektor Pemerintah Daerah di Indonesia. Penelitian ini mengusulkan pembentukan ekosistem *Local Government Information Sharing and Analysis Center* (LocalGov-ISAC) di Indonesia dengan memanfaatkan *toolkit ENISA ISAC in a Box* tahap *build.* Hasil penelitian ini yaitu kondisi sektor Pemerintah Daerah di Indonesia masih minim dalam penerapan analisis dan berbagi informasi keamanan siber. Pemerintah Daerah masih berfokus pada pembentukan ekosistem CSIRT. Pembentukan LocalGov-ISAC mengikuti tahap *ENISA ISAC in a Box* dengan menghasilkan 5 sasaran dan tujuan pembentukan LocalGov-ISAC, ruang lingkup sebanyak 6 program kegiatan, keanggotaan LocalGov-ISAC di Indonesia, tata kelola LocalGov-ISAC di Indonesia, metode pertukaran informasi, dan pembiayaan LocalGov-ISAC. Pengembangan ekosistem LocalGov-ISAC di Indonesia yang dihasilkan melibatkan klasifikasi informasi serta sifat informasi dari informasi yang dipertukarkan antar entitas di dalamnya. Keseluruhan hasil ini berdasarkan tahapan *build* yang terdiri dari tujuan, ruang lingkup, keanggotaan, tata kelola, metode pertukaran informasi, dan pembiayaan.

Kata kunci: ekosistem, *ISAC in a Box,* LocalGov-ISAC, Pemerintah Daerah.

Abstract

Information and Analysis Center (ISAC) is a best practice applied to assist organizations in overcoming cyber-attack impact, including electronic-based government system services for the Local Government sector in Indonesia. This study proposes the establishment of a Local Government Information Sharing and Analysis Center (LocalGov-ISAC) ecosystem in Indonesia by utilizing the ENISA ISAC toolkit in a Box. The result of this study is that the condition of the local government sector in Indonesia has not yet implemented cybersecurity analysis and information sharing. Local governments are still focusing on establishing the CSIRT ecosystem. The Building of LocalGov-ISAC follows the ENISA ISAC in a Box stage by producing 5 goals and purposes for establishing LocalGov-ISAC, 6 programs of areas and activities, LocalGov-ISAC participants in Indonesia, LocalGov-ISAC governance structure in Indonesia, information exchange and communication process, and funding LocalGov-ISAC in Indonesia. The development of LocalGov-ISAC ecosystem in Indonesia involves the classification of information and the nature of information between entities. All of these results are based on the build stages consisting of goal and purpose, area and activities, participants, governance structure, information exchange and communication, and funding.

Keywords: : ecosystem, ISAC in a Box, LocalGov-ISAC, Local Government.

1. PENDAHULUAN

Peningkatan insiden siber pada setiap sektor yang termasuk di dalam infrastruktur informasi kritis merupakan permasalahan yang harus diatasi oleh berbagai entitas yang terlibat. Berbagi informasi keamanan siber atau *Cybersecurity Information Sharing* (CIS) antar organisasi adalah strategi penting dalam mengatasi dampak serangan siber [1, 2]. Permasalahan yang dialami oleh sektor Pemerintah Daerah di Indonesia yaitu sebanyak 33.748 kali terdapat peretasan terhadap situs pemerintah dengan mayoritas kejadian berasal dari sektor instansi daerah [3]. Kesiapan instansi Pemerintah Daerah juga merupakan tantangan tersendiri, terutama dalam menjamin keamanan layanan Sistem Pemerintahan Berbasis Elektronik (SPBE).

CIS dapat bermanfaat dalam mempersiapkan semua pemangku kepentingan dalam menilai kerentanan, memahami potensi dan konsekuensi insiden, mencegah, melindungi, serta menanggapi serta memulihkan berbagai ancaman siber [4]. Implementasi CIS dapat dilakukan dengan menerapkan *Information Sharing and Analysis Center* (ISAC). Penerapan ISAC memiliki banyak keuntungan, seperti hasil pembelajaran dari serangan siber di masa lalu untuk dianalisis dan dipahami instansi lainnya dalam menangani ancaman siber di masa depan.

Beberapa penelitian telah membahas solusi ISAC sebagai strategi dalam menangani serangan siber bagi organisasi, seperti pembuatan model berbagi informasi keamanan siber, salah satunya yaitu pada sektor kesehatan [5, 6]. Di sektor pemerintah, terdapat penelitian yang mengusulkan model CIS antar pemerintah dengan teknologi *Blockchain* [7].

Beberapa penelitian lainnya juga membahas terkait kolaborasi keamanan siber dengan model aktivitas operasi keamanan siber dan model kematangan berbagi informasi intelijen ancaman siber antar organisasi [8-10]. Selain itu, keamanan informasi dalam berbagi informasi juga difokuskan beberapa penelitian dengan memperhatikan mengenai teknik kriptografinya [11-16].

Pertukaran informasi serangan siber antar organisasi pada ISAC dengan berklasifikasi informasi rahasia harus diamankan dengan baik [17, 18]. Pembentukan ISAC harus memperhatikan kondisi penerapan berbagi informasi keamanan siber yang terjadi sebelumnya. Oleh karena itu, dibutuhkan *best practice* yang dapat memperhatikan keseluruhan komponen tersebut dalam penerapan ISAC.

Pemerintah Daerah memiliki layanan SPBE yang layanan tersebut termasuk ke dalam sektor infrastruktur informasi kritis atau vital nasional, seperti yang dimuat dalam Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (IIV). Penerapan ISAC dapat membantu Pemerintah Daerah dalam menjamin keamanan pada layanan SPBE. Negara lain yang cukup matang dalam menerapkan ISAC dengan melibatkan sektor Pemerintah Daerah yaitu seperti Amerika Serikat [19], Australia [20], dan Inggris [21].

Dalam penelitian ini, diusulkan pembentukan ekosistem ISAC untuk diterapkan pada sektor Pemerintah Daerah di Indonesia, yaitu *Local Government Information Sharing and Analysis Center* (LocalGov-ISAC). Analisis pembentukan LocalGov-ISAC ini mengacu pada *best practice* yaitu *ENISA ISAC in A Box* pada tahap *build.* Usulan ini dapat dimanfaatkan organisasi atau berbagai pihak di sektor Pemerintah Daerah untuk penyelenggaraan ISAC pada sektor Pemerintah Daerah dalam rangka peningkatan kapabilitas keamanan siber terkait layanan SPBE.

Penelitian ini terdiri dari struktur penulisan sebagai berikut: Bagian I berisi pendahuluan, Bagian II berisi landasan teori, Bagian III berisi metodologi penelitian, Bagian IV berisi hasil penelitian dan analisis, serta Bagian V berisi kesimpulan.

2. LANDASAN TEORI

Bagian 2 berisi Pemerintah Daerah, *Information Sharing and Analysis Center,* Local Gov-ISAC di Negara Lain, dan *ISAC in a Box.*

2.1. Pemerintah Daerah

Pemerintah Daerah terdiri dari unsur penyelenggara pemerintahan daerah yang di dalamnya terkait urusan pemerintahan dengan kewenangan daerah otonom [22]. Indonesia menerapkan Pemerintah Daerah yang terdiri atas perangkat Daerah, seperti Sekretariat Daerah, Sekretariat DPRD, Inspektorat, Dinas, dan Badan [23].

Di Indonesia, kapabilitas keamanan siber pada Pemerintah Daerah juga turut mendorong jalannya keamanan Sistem Pemerintahan Berbasis Elektronik (SPBE). Pemerintah, baik Pusat maupun Daerah, mengomunikasikan dan mendokumentasikan kegiatan manajemen keamanan SPBE satu sama dengan yang lainnya [24]. Keamanan SPBE juga melibatkan keamanan informasi yang berada di dalam SPBE, yang melibatkan infrastruktur teknologi informasi, seperti sistem, aplikasi, komunikasi data, pengolahan dan penyimpanan data, hingga perangkat elektronik lainnya [25].

2.2. *Information Sharing and Analysis Center*

Analisis dan berbagi informasi keamanan siber adalah kegiatan yang dilakukan oleh *Information Sharing and Analysis Center* (ISAC) [26]. ISAC memiliki manfaat seperti kesadaran keamanan siber, kepercayaan dan kemitraan yang kuat antar entitas, otomatisasi proses, hubungan timbal balik antar entitas, fleksibilitas tata kelola berbagi informasi, aksesibilitas keanggotaan, pengurangan biaya insiden siber, peningkatan reputasi publik, penurunan risiko keamanan siber, serta pemberian informasi yang andal dan relevan [6]. Model ISAC diterbitkan oleh *The European Union Agency for Network and Information Security* (ENISA) [26]. Dalam model ENISA, terdapat tata kelola dan gaya kolaborasi seperti pertemuan rutin, grup kerja bersama, konferensi, dan kegiatan lainnya, untuk menentukan seberapa sering dan dalam format tertentu ISAC tersebut diadakan [26]. Adapun berbagai sektor di dalam ISAC yaitu sektor energi, distribusi dan pemasok air minum, kesehatan, keuangan, perbankan, transportasi kereta, transportasi udara, maritim, transportasi darat, distribusi makanan, dan lain sebagainya [26].

2.3. LocalGov-ISAC di Negara Lain

Amerika Serikat telah mengimplementasikan berbagai ISAC, salah satunya yaitu *Multi-State ISAC* (MS-ISAC) [19]. MS-ISAC dibiayai oleh U.S. Department of Homeland Security dalam melakukan pencegahan, perlindungan, respons insiden, dan pemulihan ancaman siber bagi Negara Bagian, Pemerintah Lokal, Suku, dan Teritorial (SLTT) Amerika Serikat [19]. MS-ISAC terdiri dari negara bagian sebanyak 50 (lima puluh) negara bagian dengan anggota distrik, wilayah teritorial, hingga pemerintah lokal, serta anggota kota madya [27]. Alasan MS-ISAC terbentuk di Amerika Serikat karena infrastruktur kritis yang diatur yaitu salah satunya terkait fasilitas administrasi pemerintahan.

Di Britania Raya, berbagi informasi keamanan siber diterapkan di dalam *Cyber-Security Information Sharing Partnership* (CiSP) [21]. Britania Raya menerapkan berbagi informasi keamanan siber di lingkungan lokal pemerintahan yang melibatkan Irlandia Utara [21]. Hasil dari berbagi informasi ini diharapkan dapat membentuk komunitas berbagi informasi antar anggota lokal yang berkaitan dengan

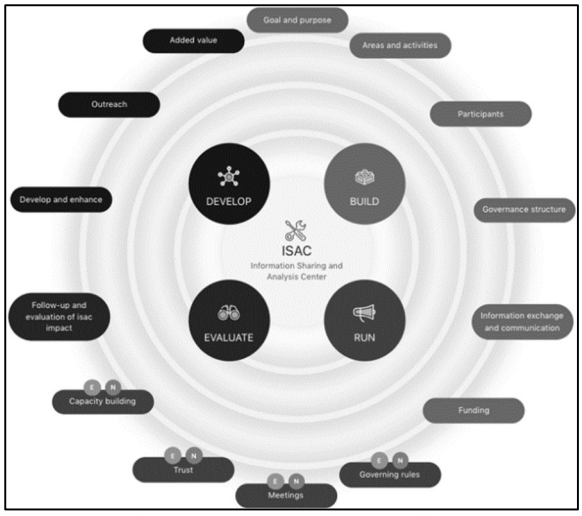
ancaman siber [21]. Sektor pemerintah sendiri di Britania Raya menjadi layanan esensial yang termasuk pada sektor infrastruktur kritis nasional [28].

Negara di Eropa yang menerapkan ISAC pada sektor pemerintahan yaitu pada Finlandia [28]. Finlandia menerapkan FI-ISAC dan National Cyber Security Center Finland (NCSC-FI) [28]. Sektor Pemerintahan yang bergabung ke dalam ISAC ini terdiri dari 50 organisasi yang berpartisipasi, namun berfokus pada Pemerintah Pusat [28]. Tujuan dari terbentuknya kelompok ISAC ini untuk menjamin keamanan siber pada teknologi digital masa depan.

Australia juga melibatkan Pemerintah Daerah (meliputi Pemerintah Bagian dan Pemerintah Teritorial) ke dalam proses berbagi informasi keamanan siber di Australia [20]. Pada jaringan berbagi informasi siber Australia, terdapat Joint Cyber Security Centres (JCSC) yang diinisiasi oleh Australia Cyber Security Strategy sebagai portal berbagi informasi siber dengan melibatkan pemerintah di Australia, termasuk sektor privat dan sektor pemerintah daerah [20].

2.4. *ISAC in a Box*

Salah satu *toolkit* yang dapat digunakan untuk membentuk, mengembangkan, menjalankan, hingga mengevaluasi ISAC yaitu *ISAC in a Box* yang diterbitkan oleh ENISA. Syarat kebutuhan ISAC ini meliputi aktivitas, dokumen, dan alat yang diperlukan untuk menyiapkan dan menjalankan ISAC [29]. *Toolkit* ini dapat dimanfaatkan pengguna dalam memberikan panduan praktis dan sarana bagi industri untuk membentuk ISAC dan mengembangkan ISAC yang sudah ada. *Toolkit* tersebut ditunjukkan pada Gambar 1.



Gambar 1. *ENISA ISAC in a Box Toolkit* [29]

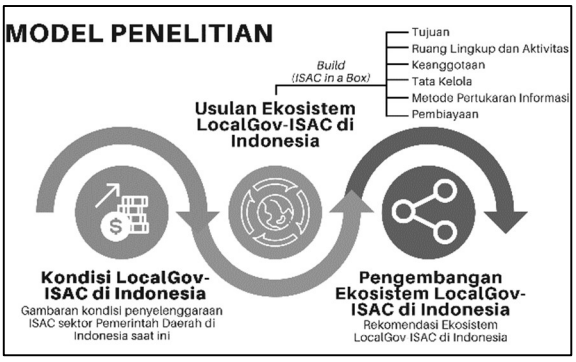
Toolkit pada *ISAC in a Box* terdiri dari empat fase, yaitu fase *build,* fase *run,* fase *evaluate,* dan fase *develop.* Dalam penelitian ini, ISAC pada sektor Pemerintah Daerah belum dibangun sehingga proses dalam penelitian ini memanfaatkan tahap *build.* Pembangunan ISAC diperlukan dengan dukungan ekosistem keamanan siber. Berdasarkan hasil pembentukan CSIRT di Indonesia, CSIRT di lingkungan Kabupaten/Kota baru terbentuk sebanyak 17 CSIRT dari total 514 Kabupaten/Kota di Indonesia [30]. Oleh karena itu, ISAC belum dapat secara aktif berjalan di sektor Pemerintah Daerah.

Pada fase *build*, fase ini terdiri dari penetapan sasaran dan tujuan, ruang lingkup dan aktivitas, keanggotaan ISAC, tata kelola analisis dan berbagi informasi keamanan siber, metode pertukaran informasi, dan pembiayaan ISAC.

3. METODE PENELITIAN

Penelitian ini merupakan penelitian kualitatif dengan deskripsi mengenai analisis dan rekomendasi pembentukan dan pengembangan ISAC di sektor Pemerintah Daerah dalam penelitian ini memanfaatkan *best practice* berupa *toolkit* yaitu ENISA *ISAC in a Box* dan berfokus pada tahap *build* pada sektor Pemerintah Daerah di Indonesia. Tahap *build* merupakan fokus utama penelitian ini yaitu dalam pembangunan dan pengembangan ISAC di lingkungan Pemerintah Daerah.

Penelitian ini memanfaatkan *toolkit* ENISA *ISAC in a Box,* serta peraturan perundang-undangan terkait keamanan siber dan Pemerintah Daerah yang telah diterapkan di Indonesia. Gambar 2 menunjukkan model pada penelitian ini. Model ini terdiri dari 3 (tiga) tahapan, yaitu melihat kondisi ekosistem LocalGov-ISAC di Indonesia, usulan ekosistem LocalGov-ISAC di Indonesia yang meliputi tujuan, ruang lingkup dan aktivitas, keanggotaan, tata kelola, metode pertukaran informasi, dan skema pembiayaan kegiatan pada LocalGov-ISAC di Indonesia. Terakhir, rekomendasi implementasi ekosistem LocalGov-ISAC di Indonesia.



Gambar 2. Model Penelitian

Objek penelitian ini adalah ekosistem berbagi informasi keamanan siber antar CSIRT Pemerintah Daerah (CSIRT Daerah) di Indonesia. Tahapan penelitian ini memuat analisis sebagai berikut:

1. Mengidentifikasi kondisi penerapan berbagi informasi keamanan siber dan implementasi ISAC di lingkungan Pemerintah Daerah di Indonesia.
2. Menyusun rekomendasi dan analisis

pembentukan LocalGov-ISAC di Indonesia berdasarkan *best practice ISAC in a Box.* Rekomendasi dan analisis ini terdiri dari tujuan, ruang lingkup dan aktivitas, tata kelola, metode pertukaran informasi, dan pembiayaan.
3. Mendeskripsikan rekomendasi pengembangan ekosistem LocalGov-ISAC di Indonesia.

4. HASIL PENELITIAN DAN ANALISIS

Dalam Bagian 4, hasil penelitian dan analisis terdiri dari Kondisi LocalGov-ISAC di Indonesia, *Building* LocalGov-ISAC di Indonesia berdasarkan *ISAC-in-a-Box,* dan Pengembangan Ekosistem LocalGov-ISAC di Indonesia.

4.1. Kondisi LocalGov-ISAC di Indonesia

LocalGov-ISAC merupakan istilah yang dibuat untuk menunjukkan eksistensi ISAC pada sektor Pemerintah Daerah di Indonesia. Sektor Pemerintah Daerah di Indonesia juga turut serta dalam peningkatan kapabilitas keamanan siber pada masing-masing instansi Pemerintah Daerah. Setiap Pemerintah Daerah, baik di tingkat provinsi maupun kabupaten/kota, menyiapkan sumber daya keamanan siber dalam menghadapi ancaman siber yang dapat berdampak pada layanan SPBE.

Penyiapan dan pemanfaatan sumber daya keamanan siber ini dibentuk ke dalam wadah yang dinamakan *Computer Security Incident Response Team* (CSIRT). CSIRT setiap provinsi, kabupaten/kota memiliki tugas dan fungsi yang berkaitan dengan layanan dan dukungan tanggap insiden siber pada instansinya tersebut. Pembentukan CSIRT di sektor Pemerintah Daerah masih belum menyeluruh dan masih terus bertambah setiap tahunnya. Selain itu, fokus pengembangan ekosistem keamanan siber masih di tahap pengembangan ekosistem CSIRT terkait penanganan insiden siber, kebijakan keamanan informasi, dan persandian. Komunikasi dan koordinasi antar CSIRT di Pemerintah Daerah juga masih minim berdasarkan sedikitnya hasil publikasi kolaborasi antar Pemerintah Daerah terkait insiden siber.

CSIRT Daerah dapat dimanfaatkan dalam forum berbagi informasi keamanan siber pada sektor Pemerintah Daerah. Sesuai Peraturan Presiden Republik Indonesia Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital, forum analisis dan berbagi informasi keamanan siber dapat diselenggarakan oleh Penyelenggara Infrastruktur Informasi Vital, salah satunya di sektor administrasi pemerintahan. Pertambahan jumlah CSIRT Daerah yang diiringi dengan peningkatan ancaman siber bagi Pemerintah Daerah (baik CSIRT Daerah dan entitas lainnya, seperti Perangkat Daerah yang memanfaatkan layanan SPBE) membawa kebutuhan ekosistem berbagi informasi keamanan siber yang khusus di sektor Pemerintah Daerah.

4.2. *Building* LocalGov-ISAC di Indonesia berdasarkan *ISAC-in-a-Box*

4.2.1 Tujuan LocalGov-ISAC di Indonesia

LocalGov-ISAC di Indonesia harus memiliki tujuan yang terdiri dari sasaran dan tujuan. Sasaran dan tujuan tersebut dapat dituangkan ke dalam *Term of Reference.* Sasaran dan tujuan yang dapat dijadikan acuan untuk LocalGov-ISAC yaitu salah satunya untuk *situational awareness* mengenai ancaman dan kerentanan siber pada sektor Pemerintah Daerah, baik dalam lingkup komunitas maupun instansi Pemerintah Daerah tersebut.

Sasaran dan tujuan selain dari *situational awareness* yaitu antisipasi efisiensi Anggaran Pendapatan dan Belanja Negara (APBN) yang digunakan untuk penanggulangan insiden siber, efisiensi penanganan atau respons insiden siber, *lesson learned* praktik keamanan siber pada masing-masing instansi, hingga peningkatan budaya dan kapabilitas keamanan siber bagi pemangku kepentingan pada sektor yang berkaitan dengan Pemerintah Daerah.

4.2.2 Ruang Lingkup dan Aktivitas LocalGov-ISAC di Indonesia

LocalGov-ISAC di Indonesia memiliki aktivitas yang berhubungan dengan berbagi informasi dan analisis keamanan siber antar entitas di sektor Pemerintah Daerah. Ruang lingkup tersebut dirincikan ke dalam aktivitas dengan program sebagai berikut [31]:
1. *Cyber Session:* Program dengan sesi diskusi berbagi keamanan siber terkait praktik pertahanan siber, inteligensi ancaman siber, hingga kerentanan siber di sektor Pemerintah Daerah.
2. *Cyber Portal: Platform* yang memfasilitasi program pertukaran dan berbagi informasi keamanan siber antar entitas sektor Pemerintah Daerah.
3. Kolaborasi Penelitian Ancaman Siber: Program yang memfasilitasi penelitian terkait ancaman hingga kerentanan siber antar entitas.
4. *Cyber Exchange Forum:* Program yang memfasilitasi forum antar anggota yang berisi analis insiden siber, seperti diskusi panel, strategi, hingga sesi berbagi pengetahuan keamanan siber.
5. *ISAC Annual Conference:* Program yang berupa konferensi terkait forum berbagi informasi keamanan siber yang membahas isu-isu terkait keamanan siber pada sektor Pemerintah Daerah.
6. *ISAC Webiste:* Program yang berupa *platform* untuk menyediakan informasi keamanan siber bagi pemangku kepentingan di sektor Pemerintah Daerah.

4.2.3 Keanggotaan LocalGov-ISAC di Indonesia

Keanggotaan LocalGov-ISAC dapat bersifat mandatori atau sukarela. BSSN sebagai salah satu entitas dalam LocalGov-ISAC dapat berperan dalam

mengembangkan ekosistem dan penentuan kebijakan teknis terkait ISAC di sektor Pemerintah Daerah. Anggota ini terdiri dari perwakilan dari masing-masing instansi Pemerintah Daerah. Anggota yang terlibat di dalam LocalGov-ISAC tersebut harus memiliki kapabilitas di ranah keamanan siber, dapat berkomunikasi dan berkontribusi dalam diskusi pada sebuah forum.

Anggota utama yang ada pada LocalGov-ISAC terdiri dari seluruh instansi Pemerintah Daerah di Indonesia, yang terdiri dari Pemerintah Provinsi maupun Pemerintah Kabupaten/Kota. Perwakilan instansi Pemerintah Daerah tersebut yaitu personel dari Dinas yang membidangi keamanan siber pada instansi tersebut, seperti CSIRT masing-masing Pemerintah Daerah. Anggota lainnya juga dapat diperluas dalam lingkup komunitas instansi Pemerintah Daerah seperti perangkat daerah lainnya yang memiliki layanan SPBE. Selain instansi Pemerintah Daerah, BSSN juga turut ikut serta sebagai anggota di dalam LocalGov-ISAC.

4.2.4 Tata Kelola LocalGov-ISAC di Indonesia

Tata kelola memiliki peran yang sangat penting dalam keberlangsungan kegiatan LocalGov-ISAC di Indonesia. Tata kelola berhubungan dengan pemanfaatan sumber daya, pengelolaan risiko, hingga pencapaian tujuan berbagi informasi keamanan siber yang dijalankan oleh LocalGov-ISAC. Dalam mewujudkannya, terdapat peran entitas di dalamnya, seperti Instansi Pemerintah Daerah dan BSSN.

BSSN dapat berperan dalam memantau informasi keamanan siber yang dipertukarkan di dalam ekosistem berbagi informasi LocalGov-ISAC. Hasil pemantauan tersebut dapat dijadikan bahan kebijakan teknis, peningkatan dan pengembangan kapabilitas ekosistem keamanan siber di sektor Pemerintah Daerah. juga berperan sebagai *implementor* atau anggota dengan memberikan analisis dan berbagi informasi.

BSSN dapat bertindak sebagai *developer* dengan tugas dan fungsi di bidang pengembangan ekosistem keamanan siber di sektor Pemerintah Daerah. Developer juga dapat berisi unit di BSSN yang membidangi tata kelola dan manajemen risiko keamanan siber di sektor Pemerintah Daerah. Berkaitan dengan kebijakan, BSSN juga dapat mengampu pengembangan kebijakan teknis dan tata kelola dalam lingkup yang lebih luas, dengan LocalGov-ISAC yang berkomunikasi dengan ISAC pada sektor lainnya. Selain itu, keterlibatan BSSN sebagai *implementor* ini berkaitan dengan unit di BSSN yang berkaitan dengan tugas dan fungsi operasi keamanan siber.

Instansi Pemerintah Daerah berperan dalam membagi informasi keamanan siber berdasarkan klasifikasi informasi. Pihak yang berhak dalam informasi tersebut dapat dibagi berdasarkan tingkat sensitivitas informasi di dalamnya. Pihak lainnya yang juga dapat berperan seperti instansi dalam lingkup perangkat daerah yang memiliki layanan SPBE dapat berbagi informasi hingga menerima informasi yang dipertukarkan dengan klasifikasi informasi tertentu.

4.2.5 Metode Pertukaran Informasi LocalGov-ISAC di Indonesia

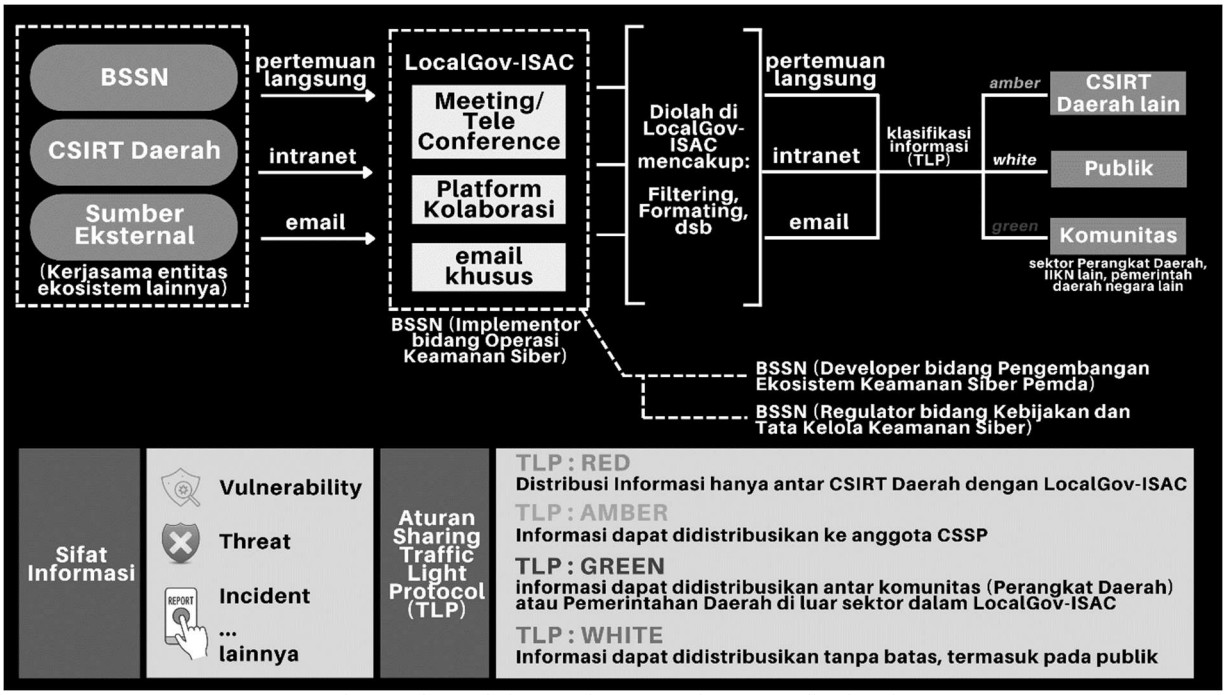
Metode pertukaran informasi dapat dilakukan dengan pertemuan langsung, baik melalui *tele conference* atau rapat. Informasi juga dapat dipertukarkan dengan *platform* kolaborasi melalui jaringan intranet. Pertukaran informasi juga dapat menggunakan *email* khusus bagi anggota.

Informasi yang dipertukarkan dapat berupa informasi mengenai ancaman siber, kerentanan siber, insiden siber, respons dan mitigasi insiden siber, *good practice,* intelijen ancaman siber, dan informasi terkait keamanan siber lainnya. Informasi tersebut perlu memanfaatkan klasifikasi informasi, salah satunya seperti pemanfaatan *Traffic Light Protocol* (TLP) [32].

4.2.6 Pembiayaan LocalGov-ISAC di Indonesia

Program LocalGov-ISAC dilakukan dengan inisiasi pendekatan berbasis administrasi pemerintahan yang tentunya melibatkan sektor Pemerintah Daerah dan BSSN di Indonesia. Program dapat diinisiasi oleh BSSN dalam membangun LocalGov-ISAC di Indonesia. LocalGov-ISAC di Indonesia ini dijalankan oleh seluruh instansi Pemerintah Daerah di Indonesia. Pembiayaan terkait juga dapat diinisiasi oleh BSSN dengan kolaborasi anggaran pada instansi Pemerintah Daerah di Indonesia. BSSN sebagai pembina keamanan siber dan juga bertanggung jawab terkait pengembangan kapabilitas keamanan siber di sektor Pemerintah Daerah juga dapat berperan dalam pengembangan *platform,* regulasi dan mekanisme program, hingga kolaborasi sumber daya untuk LocalGov-ISAC.

Program seperti forum hingga konferensi yang dilakukan oleh LocalGov-ISAC dapat diinisiasi oleh salah satu instansi Pemerintah Daerah. Inisiasi ini dapat diperoleh dari pertemuan yang menghasilkan kesepakatan penanggung jawab dengan pelaksanaan secara berkesinambungan setiap tahunnya.



Gambar 3. Rekomendasi Pengembangan LocalGov-ISAC di Indonesia

Penanggung jawab ini dapat berlangsung secara bergilir sesuai dengan kesepakatan antar anggota di dalam LocalGov-ISAC.

4.3. Pengembangan Ekosistem LocalGov-ISAC di Indonesia

Berdasarkan kondisi ISAC pada sektor Pemerintah Daerah di Indonesia, dibentuklah analisis pengembangan ekosistem LocalGov-ISAC di Indonesia berdasarkan *ISAC-in-a-Box* pada tahap *building.* Tahapan tersebut digunakan karena ISAC belum didefinisikan atau belum diimplementasikan oleh sektor Pemerintah Daerah. Berdasarkan analisis tersebut, diperoleh rekomendasi pengembangan ekosistem LocalGov-ISAC di Indonesia. Gambar 3 menunjukkan gambaran rekomendasi pengembangan LocalGov-ISAC di Indonesia.

Gambar 3 menunjukkan rekomendasi pengembangan LocalGov-ISAC di Indonesia. Gambar 3 merupakan implementasi yang mengacu pada *ISAC-in-a-Box* seperti dalam penelitian [33] dengan fokus pada implementasi di Pemerintah Daerah. Gambar 3 tersebut memiliki entitas yang terdiri dari BSSN, CSIRT Daerah (terdiri dari CSIRT yang ada di sektor Pemerintah Daerah), dan sumber eksternal. Sumber eksternal tersebut merupakan entitas di luar sektor Pemerintah Daerah di Indonesia, seperti sektor infrastruktur informasi vital/kritis lainnya maupun sektor Pemerintah Daerah di negara lain. Keseluruhan entitas tersebut berperan dalam berbagi informasi keamanan siber.

Proses pertukaran informasi dilakukan dengan pertemuan langsung atau virtual, intranet, hingga *email.* Entitas yang bertindak sebagai implementor analisis dan berbagi informasi keamanan siber pada sektor Pemerintah Daerah yaitu LocalGov-ISAC. LocalGov-ISAC ini bisa diampu oleh BSSN yang membidangi operasi keamanan siber. Dalam pengembangan keamanan siber dalam LocalGov-ISAC, BSSN juga dapat berperan dalam pengembangan ekosistem keamanan siber, hingga tata kelola, dan manajemen risiko keamanan siber pada implementasi program LocalGov-ISAC. Berkaitan dengan kebijakan pelaksanaan LocalGov-ISAC di Indonesia, BSSN juga dapat berperan dalam ranah kebijakan keamanan siber secara nasional yang tentunya memiliki interdependensi dengan penyelenggaraan ISAC pada sektor lain maupun sektor nasional.

LocalGov-ISAC berperan dalam melakukan analisis, *filtering* dan *formatting* informasi, hingga menentukan program yang ada di dalam ekosistem berbagi informasi keamanan siber. Keseluruhan aktivitas tersebut dilakukan ke dalam program yang terdiri dari *Cyber Session, Cyber Portal,* Kolaborasi Penelitian Ancaman Siber, *Cyber Exchange Forum, ISAC Annual Conference,* dan *ISAC Webiste.* LocalGov-ISAC juga harus mengatur sifat informasi dan klasifikasi informasi keamanan siber yang dipertukarkan di dalam ekosistem LocalGov-ISAC.

Klasifikasi informasi keamanan siber akan menentukan hak akses entitas yang bergabung di dalam ekosistem berbagi informasi keamanan siber pada LocalGov-ISAC, seperti informasi berklasifikasi dengan TLP: *Red, Amber, Green,* atau *White.* TLP: *Red* dengan tingkat sensitivitas informasi paling tinggi juga harus diatur lebih lanjut dalam keterlibatannya di dalam ekosistem LocalGov-ISAC.

Komunitas yang digambarkan pada Gambar 3 yaitu komunitas pada sektor Pemerintah Daerah. Ekosistem ini dapat berkembang di sektor lainnya

yang juga menerapkan ISAC. Integrasi antar sektor terkait ISAC juga dapat mengukuhkan *situational awareness* pada suatu negara. Dengan berkembangnya ancaman siber juga menuntut negara Indonesia bekerja sama dengan negara lain, salah satunya dengan berbagi informasi keamanan siber antar Pemerintah Daerah pada masing-masing negara, baik di tingkat regional hingga mancanegara.

5. PENUTUP

Berdasarkan hasil penelitian, kesimpulan dalam penelitian ini yaitu:

1. LocalGov-ISAC di Indonesia masih belum diimplementasikan di Indonesia. Namun, Instansi Pemerintah Daerah meningkatkan kapabilitas keamanan sibernya dengan membentuk CSIRT Daerah yang nantinya dapat berkontribusi besar melalui forum analisis dan berbagi informasi keamanan siber antar Pemerintah Daerah.
2. Pengembangan ekosistem LocalGov-ISAC di Indonesia dapat terlebih dahulu dibentuk, salah satunya dengan pemanfaatan *toolkit ENISA ISAC in a Box.* Dalam analisisnya diperoleh enam komponen, yaitu penetapan sasaran dan tujuan, ruang lingkup dan aktivitas, keanggotaan ISAC, tata kelola analisis dan berbagi informasi keamanan siber, metode pertukaran informasi, dan pembiayaan LocalGov-ISAC di Indonesia.
3. Terdapat 5 (lima) sasaran dan tujuan pembentukan LocalGov-ISAC dengan ruang lingkup sebanyak 6 (enam) program kegiatan. Keanggotaan LocalGov-ISAC di Indonesia terdiri dari instansi Pemerintah Daerah, termasuk Perangkat Daerah yang mengimplementasikan layanan SPBE, dan BSSN. Tata kelola memiliki keterkaitan dengan peran entitas dengan pemanfaatan sumber daya, pengelolaan risiko, hingga pencapaian tujuan dalam analisis dan berbagi informasi keamanan siber oleh LocalGov-ISAC. Metode pertukaran informasi dilakukan dengan pertemuan langsung, baik melalui *tele conference* atau rapat, *platform* kolaborasi melalui jaringan intranet, dan *email* khusus bagi anggota. Pembiayaan LocalGov-ISAC dapat diinisiasi oleh BSSN yang melibatkan kerja sama program dengan instansi Pemerintah Daerah di Indonesia.
4. Pengembangan ekosistem LocalGov-ISAC di Indonesia yang dihasilkan melibatkan klasifikasi informasi serta sifat informasi dari informasi yang dipertukarkan antar entitas di dalamnya. Kedua aspek tersebut menjadi landasan kebijakan dan penentuan keputusan atas hak entitas yang memperoleh informasi tersebut.

Saran dalam penelitian ini yaitu pembentukan ISAC pada sektor Pemerintah Daerah harus didorong dengan terimplementasinya CSIRT Daerah di Indonesia. Namun, dalam implementasinya, LocalGov-ISAC dapat diterapkan dengan anggota CSIRT Daerah yang telah ada terlebih dahulu. Penelitian ini juga dapat dikembangkan dari sisi kesiapan CSIRT Daerah untuk membentuk forum analisis dan berbagi informasi keamanan siber.

REFERENSI

[1] A. Zrahia, "Threat intelligence sharing between cybersecurity vendors: Network, dyadic, and agent views," *Journal of Cybersecurity,* vol. 4, pp. 1-16, 2018, doi: 10.1093/cybsec/tyy008.

[2] I. Vakilinia and S. Sengupta, "Fair and private rewarding in a coalitional game of cybersecurity information sharing," *IET Information Security,* vol. 13, pp. 530-540, 2019, doi: 10.1049/iet-ifs.2018.5079.

[3] S. C. Dewanti, "Urgensi Sistem Keamanan Siber Pemerintah," *Kajian Singkat Terhadap Isu Aktual dan Strategis Bidang Politik Dalam Negeri,* vol. XIII, no. 16, pp. 25-30, 2021.

[4] (2016). *Critical Infrastructure Threat Information Sharing Framework - A Reference Guide to the Critical Infrastructure Community*.

[5] J. Hautamäki and T. Kokkonen, "Model for Cyber Security Information Sharing in Healthcare Sector," in *Proc. of the 2nd International Conference on Electrical, Communication and Computer Engineering (ICECCE)*, Istanbul, Turkey, 2020: IEEE.

[6] E. M. Sedenberg and D. K. Mulligan, "Public Health as a Model for Cybersecurity Information Sharing," *JSTOR,* vol. 30, no. University of California, Berkeley, School of Law, 2015.

[7] Y. Zhang, S. Deng, Y. Zhang, and J. Kong, "Research on Government Information Sharing Model Using Blockchain Technology," in *10th International Conference on Information Technology in Medicine and Education (ITME)*, Qingdao, China, 2019: IEEE, pp. 726-729, doi: 10.1109/ITME.2019.00166.

[8] C. Sillaber, C. Sauerwein, A. Mussmann, and R. Breu, "Towards a Maturity Model for Inter-Organizational Cyber Threat Intelligence Sharing: A Case Study of Stakeholders' Expectations and Willingness to Share," in *MKWI 2018*, Lüneburg, 2018: Leuphana Universität Lüneburg, pp. 1409-1420.

[9] T. Takahashi, Y. Kadobayashi, and K. Nakao, "Toward global cybersecurity collaboration: Cybersecurity operation activity model," in *Proceedings of ITU Kaleidoscope 2011: The Fully Networked Human? - Innovations for Future Networks and Services (K-2011)*, Cape Town, South Africa, 2011: IEEE, pp. 1-8.

[10] D.-J. van Veen, R. S. Kudesia, and H. R. Heinimann, "An Agent-Based Model of Collective Decision-Making: How Information Sharing Strategies Scale With Information Overload," *IEEE Transactions on Computational Social Systems,* vol. 7, no. 3, pp.

751-767, 2020, doi: 10.1109/tcss.2020.2986161.
[11] L. Zhang, Y. Cui, and Y. Mu, "Improving Security and Privacy Attribute Based Data Sharing in Cloud Computing," *IEEE Systems Journal,* vol. 14, pp. 387-397, 2020, doi: 10.1109/JSYST.2019.2911391.
[12] J. M. de Fuentes, L. González-Manzano, J. Tapiador, and P. Peris-Lopez, "PRACIS: Privacy-preserving and aggregatable cybersecurity information sharing," *computers & security,* vol. 69, pp. 127-141, 2017.
[13] Z. Yang, W. Wang, Y. Huang, and X. Li, "Privacy-preserving public auditing scheme for data confidentiality and accountability in cloud storage," *Chinese Journal of Electronics,* vol. 28, pp. 179-187, 2019, doi: 10.1049/cje.2018.02.017.
[14] Y. Ming and W. Shi, "Efficient Privacy-Preserving Certificateless Provable Data Possession Scheme for Cloud Storage," *IEEE Access,* vol. 7, pp. 122091-122105, 2019, doi: 10.1109/ACCESS.2019.2938528.
[15] W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu, "Enabling Identity-Based Integrity Auditing and Data Sharing with Sensitive Information Hiding for Secure Cloud Storage," *IEEE Transactions on Information Forensics and Security,* vol. 14, pp. 331-346, 2018, doi: 10.1109/TIFS.2018.2850312.
[16] I. Vakilinia, D. K. Tosh, and S. Sengupta, "Attribute based sharing in cybersecurity information exchange framework," presented at the 2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS), Seattle, WA, 2017.
[17] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun, and Y. Xiang, "Block Design-Based Key Agreement for Group Data Sharing in Cloud Computing," *IEEE Transactions on Dependable and Secure Computing,* vol. 16, pp. 996-1010, 2019, doi: 10.1109/TDSC.2017.2725953.
[18] N. Wang, Y. Cai, J. Fu, and X. Chen, "Information privacy protection based on verifiable (t, n)-Threshold multi-secret sharing scheme," *IEEE Access,* vol. 8, pp. 20799-20804, 2020, doi: 10.1109/ACCESS.2020.2968728.
[19] CISECURITY, *MS-ISAC Multi-State Information Sharing & Analysis Center Service Guide*. 2018.
[20] L. Nevill, *Cyber Information Sharing: Lessons for Australia*. ASPI International Cyber Policy Centre (ICPC), 2017.
[21] ENISA, *Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches*. European Union Agency For Network And Information Security (ENISA), 2015.
[22] *Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah*, 2014.
[23] *Peraturan Pemerintah Nomor 18 Tahun 2016 tentang Perangkat Daerah*.
[24] *Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik*, 2021.
[25] *Peraturan Presiden Nomor 95 Tahun 2018 Tentang Sistem Pemerintahan Berbasis Elektronik*.
[26] ENISA, *Information Sharing and Analysis Centres (ISACs) Cooperative models*. 2018.
[27] (Report No. DOT HS 812 076). (2014). *Assessment of the Information Sharing and Analysis Center Model*.
[28] C. O. U. Kingdom, *Public Summary of Sector Security and Resilience Plans*. London: Civil Contingencies Secretariat, 2017.
[29] E. U. A. f. C. (ENISA). "ISAC in a Box." https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing/isacs-toolkit/view# (accessed April 5, 2022).
[30] S. M. Fatihah, "Pemkab Mojokerto Launching Tim CSIRT, Lindungi Sistem Informasi
", ed. Mojokerto: Warta Cakrawala, 2022, pp. https://www.wartacakrawala.com/pemkab-mojokerto-launching-tim-csirt-lindungi-sistem-informasi/2/.
[31] B. J. Bakis and E. D. Wang, *Building a National Cyber Information-Sharing Ecosystem*: MITRE, 2017.
[32] FIRST. "TRAFFIC LIGHT PROTOCOL (TLP) FIRST Standards Definitions and Usage Guidance — Version 1.0." https://www.first.org/tlp/ (accessed 3 January, 2022).
[33] F. A. Putra and F. Aferudin, "Pengembangan Financial Service Information Sharing and Analysis Center (FS-ISAC) di Indonesia dengan Pendekatan ENISA ISAC in a Box," *Infokripto,* vol. 16, 2, 30-09-2022 2022, doi: https://doi.org/10.56706/ik.v16i2.49.