Pengembangan *Financial Service Information Sharing and Analysis Center* (FS-ISAC) di Indonesia dengan Pendekatan ENISA ISAC *in a Box*

Fandi Aditya Putra[1)], Farouq Aferudin [2)]

(1) Badan Siber dan Sandi Negara, fandi.aditya@bssn.go.id

(2) Badan Siber dan Sandi Negara, farouq.aferudin@bssn.go.id

Abstrak

Pembentukan grup *Information Sharing and Anlysis Center* (ISAC) menjadi salah satu *best practice* yang dapat dijalankan dalam menghadapi ancaman siber yang semakin masif pada berbagai sektor infrastruktur informasi vital (IIV) termasuk pada sektor perbankan dan keuangan di Indonesia. Melalui ISAC, setiap organisasi dapat berbagi kapabilitas yang dimiliki untuk secara bersama-sama menciptakan *cybersecurity situational awarenesss*. Pada tahun 2019, Bank Indonesia telah menginisiasi pembentukan *Cyber Security Sharing Platform* - Sistem Pembayaran (CSSP-SP) untuk berbagi informasi keamanan siber khususnya pada industri sistem pembayaran di Indonesia. Pada tahun 2022 telah disahkan payung hukum pelindungan IIV melalui Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital. Pada penelitian ini dilakukan pengembangan *Financial Services*-ISAC di Indonesia melalui pendekatan *The European Union Agency for Network and Information Security* (ENISA) *in A Box* dengan memfokuskan pada satu tahapan yaitu tahap *Build*. Pada tahap ini terdapat beberapa area diantaranya penentuan tujuan, ruang lingkup, keanggotaan, tata kelola, metode pertukaran informasi serta pembiayaan. Hasil penelitian ini berupa rekomendasi pengembangan penyelenggaraan ISAC sektor perbankan dan keuangan di Indonesia guna mengoptimalkan penyelenggaraan *cybersecurity information sharing* khususnya pada ekosistem sistem pembayaran di Indonesia.

Kata kunci: ENISA, FS-ISAC, *Information Sharing and Analysis Center*, Sistem Pembayaran

1. PENDAHULUAN

Peningkatan serangan siber mengharuskan setiap organisasi untuk lebih waspada terhadap segala ancaman siber. Hasil monitoring keamanan siber Badan Siber dan Sandi Negara (BSSN) menyebutkan bahwa sepanjang tahun 2021 terdapat lebih dari 1,6 miliar anomali *traffic* jaringan yang dapat mengindikasikan serangan siber baik pada sektor pemerintahan, swasta hingga infrastruktur informasi vital (IIV) [1]. Serangan siber tersebut harus dihadapi dengan upaya kolaboratif dari setiap pihak dengan upaya yang dapat dilakukan masing-masing [2]. Untuk mengembangkan *cyber security situational awareness* yang lebih baik, diperlukan upaya berbagi informasi antara kelompok kepentingan yang berbeda untuk meningkatkan persiapan dan manajemen insiden [3]. Langkah ini merupakan *best practice* yang disebut dengan *Cybersecurity Information Sharing* (CIS) atau yang lebih dikenal dengan *Information Sharing and Analysis Center* (ISAC).

Dengan ISAC banyak keuntungan yang didapatkan, misalnya organisasi lain yang memiliki karakteristik yang sama dapat belajar dari para korban untuk menghindari serangan serupa. CIS telah diterapkan pada banyak negara dan banyak sektor yang berbeda dan biasanya dibentuk grup-grup CIS sesuai dengan sektor tertentu. CIS sektor IIV akan mempersiapkan semua pemangku kepentingan untuk lebih baik dalam menilai kerentanan, memahami potensi dan konsekuensi insiden, mencegah, melindungi, serta menanggapi dan memulihkan dari berbagai ancaman siber [4].

ISAC pada organisasi sektoral merupakan strategi penting untuk melindungi dari peningkatan pelanggaran data dan serangan siber saat ini [5, 6]. Keamanan siber pada sektor perbankan dan keuangan menjadi hal yang penting mengingat sebagian besar masyarakat memanfaatkan layanan perbankan dan keuangan terutama pada era digitalisasi saat ini. Peningkatan serangan siber pada sektor ini berdampak pada operasional sistem pembayaran yang dijalankan oleh Bank Indonesia. Di samping itu, menguatnya peran dan interkoneksi non-bank di dunia keuangan (termasuk layanan *cloud*) membuat efek domino dari insiden operasional menjadi lebih kompleks [7].

Penelitian sebelumnya membahas mengenai usulan model CIS yang berfokus pada sektor kesehatan [8, 9]. Terdapat penelitian sebelumnya yang juga membahas model berbagi informasi antar pemerintah dengan menggunakan teknologi Blockchain [10]. Selain itu, terdapat penelitian yang berfokus pada kolaborasi keamanan siber dengan model aktivitas operasi keamanan siber dan model kematangan berbagi informasi intelijen ancaman siber antar organisasi sektoral [11-13].

Dalam pertukaran informasi serangan siber antar organisasi, platform ISAC yang berklasifikasi rahasia harus diamankan dengan baik [14, 15]. Penelitian terbaru tentang skema jaminan privasi dalam berbagi informasi atau data telah dilakukan dengan menyembunyikan identitas entitas atau informasi sensitif entitas [16, 17]. Skema audit secara publik untuk memberikan privasi dalam penyimpanan data

diimplementasikan pada penelitian [18]. Isu terkait kebocoran data dengan solusi adalah memberikan perlindungan data yang aman dan terpercaya dapat dicapai dengan menggunakan teknik kriptografi untuk menjaga keamanan dan kerahasiaan berbagi data [17-22].

Saat ini regulasi terkait Pelindungan IIV telah disahkan melalui Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (IIV). Ruang lingkup yang diatur dalam Perpres ini meliputi identifikasi sektor, penyelenggaraan pelindungan, pembinaan dan pengawasan penyelenggaraan dan koordinasi penyelenggaraan. Dalam Pasal 4, didefinisikan sektor IIV yang salah satunya merupakan sektor keuangan. Perpres ini juga mengatur tentang Kementerian atau Lembaga dari masing-masing sektor dengan istilah Instansi Pengatur dan Pengawas Sektor (IPPS). Berkaitan dengan penyelenggaraan ISAC, Perpres ini mengatur bahwa Badan yang menyelenggarakan tugas pemerintahan di bidang Keamanan Siber, Kementerian atau Lembaga, dan/atau Penyelenggara IIV dapat menyelenggarakan forum analisis berbagi informasi keamanan siber sesuai dengan ketentuan peraturan perundang-undangan. Pada tahun 2019 Bank Indonesia selaku otoritas yang mengatur sektor perbankan dan keuangan telah menginisiasi penyelenggaraan ISAC khususnya pada sistem pembayaran di Indonesia melalui *Cyber Security Sharing Platform* - Sistem Pembayaran (CSSP-SP) di Indonesia.

Pada penelitian ini diusulkan pengembangan terhadap penyelenggaraan ISAC sektor perbankan dan keuangan dengan menggunakan pendekatan *The European Union Agency for Network and Information Security* (ENISA) ISAC *in A Box*. Pengembangan yang dilakukan juga didasarkan pada penambahan peran dan tanggung jawab pada entitas terkait dengan keamanan siber di Indonesia. Usulan pengembangan ini diharapkan dapat dijadikan acuan dalam penyelenggaraan FS-ISAC di Indonesia sehingga pelaksanaannya menjadi lebih optimal. Beberapa batasan dalam penelitian ini antara lain, penggambaran kondisi penyelenggaraan ISAC sektor perbankan dan keuangan di Indonesia diperoleh dari sumber terbuka. Untuk pendekatan ENISA ISAC *in A Box* yang digunakan berfokus pada tahapan pertama yaitu tahapan *Build*. Fokus berbagi informasi keamanan siber pada penelitian ini difokuskan pada industri sistem pembayaran di Indonesia sesuai yang telah dijalankan oleh Bank Indonesia.

2. LANDASAN TEORI

2.1. *Information Sharing and Analysis Center*

Berbagi informasi keamanan siber merupakan bagian dari kegiatan yang dilakukan oleh ISAC yang terbagi dalam berbagai sektor [23]. Manfaat penerapan ISAC meliputi kesadaran situasional, kepercayaan dan kemitraan yang kuat antar entitas dalam satu sektor, otomatisasi, hubungan timbal balik, fleksibilitas tata kelola organisasi berbagi informasi, aksesibilitas keanggotaan, pengurangan biaya, peningkatan reputasi publik, penurunan risiko, serta pemberian informasi yang andal dan relevan [9]. Implementasi berbagi informasi keamanan siber salah satunya diterapkan berdasarkan model ISAC yang diterbitkan oleh *The European Union Agency for Network and Information Security* (ENISA) [23].

2.2. FS-ISAC di Negara Lain

Amerika Serikat telah mengimplementasikan berbagai ISAC, salah satunya yaitu *Financial Services* ISAC (FS-ISAC) [24]. FS-ISAC di Amerika Serikat diresmikan menjadi sebuah organisasi non-profit pada 2013 dengan dampak yang lebih luas, yaitu pada Asia, Eropa, dan Amerika Selatan [24]. FS-ISAC memiliki sistem notifikasi yang mempekerjakan tim analis selama 24 jam setiap harinya untuk menghadapi ancaman baru [24]. Industri keuangan di Amerika Serikat menganggap kolaborasi melalui FS-ISAC ini bermanfaat, namun terdapat kendala yang dihadapi seperti menurunnya derajat kepercayaan dan berpotensi merusak ekosistem berbagi informasi di dalam ISAC [24]. Jepang merupakan salah satu negara yang telah mengimplementasikan ISAC dalam ekosistem keamanan sibernya, seperti *Financial* ISAC. Pemerintah Jepang membagi sektor infrastruktur informasi kritis ke dalam 13 sektor, salah satunya sektor keuangan [25].

Negara di Eropa juga menerapkan *Europe ISAC* yang melayani sektor keuangan (EU FI-ISAC) [26]. Anggota grup pada EU FI-ISAC terdiri dari perwakilan negara pada sektor keuangan, CERT Nasional dan CERT pemerintah [26]. Anggota lainnya pada EU FI-ISAC yaitu terdiri dari ENISA, Europol, *the European Central Bank* (ECB), *the European Payment Council* (EPC), dan *the European Commision* dengan pertukaran informasi terkait keamanan siber pada jalur internet hingga topik terkait Teknologi Informasi [26].

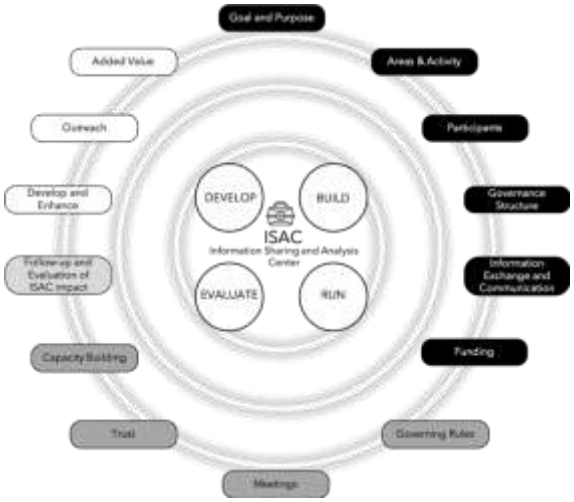
2.3. ISAC *in a Box*

ENISA ISAC *in a Box* merupakan sebuah *toolkit* yang dapat dimanfaatkan untuk membangun dan mengembangkan ISAC yang mencakup aktivitas, dokumen, dan alat yang diperlukan untuk menyiapkan dan menjalankan ISAC [27]. *Toolkit* ini bertujuan untuk memberikan panduan praktis dan sarana untuk memberdayakan industri untuk menciptakan ISAC baru dan mengembangkan ISAC yang sudah ada. *Toolkit* ENISA ISAC *in A Box* dapat dilihat pada Gambar 1.

Toolkit ini dibangun dalam empat fase dan berisi semua aktivitas, dokumen dan alat yang diperlukan untuk memulai, mengembangkan dan mengevaluasi ISAC, antara lain:

- Fase *Build*: Pada fase ini berkaitan dengan menetapkan tujuan, peserta, dan tujuan ISAC; menyepakati anggaran dan mekanisme kerja sama.

- Fase *Run*: Pada fase ini mengenai tata kelola dalam berbagi informasi melalui pertemuan dan mengembangkan kepercayaan serta membangun kapasitas di antara para peserta ISAC.
- Fase *Evaluate*: Pada fase ini mengenai evaluasi untuk membantu menjaga keberlangsungan ISAC tetap dalam jalurnya, mengukur dampaknya serta menimalkan momentum untuk membawa pada fase berikutnya.
- Fase *Develop*: Pada fase ini berfokus pada peningkatan kecanggihan ISAC, pengembangan lebih lanjut serta strategi penjangkauannya.



Gambar 1. *ENISA ISAC in a Box Toolkit* [27]

2.4. Kondisi FS-ISAC di Indonesia

Bank Indonesia (BI) telah memiliki sarana berbagi informasi keamanan siber yang dikemas melalui platform *Cyber Security Sharing Platform - Sistem Pembayaran* (CSSP-SP) yang bertujuan untuk melindungi sistem pembayaran sektor keuangan dari ancaman serangan siber [28]. *Sharing platform* tersebut digunakan sebagai sarana untuk berbagi informasi seputar ancaman siber dan mitigasi insiden siber antar organisasi dan lembaga yang masuk dalam ekosistem keuangan dan sistem pembayaran di Indonesia. Setiap Bank yang mendeteksi ancaman siber atau mengalami insiden siber wajib melaporkannya melalui email CSSP-SP@bi.go.id [28]. Setiap laporan yang masuk akan dianalisis dan dibagikan ke organisasi lainnya lewat CSSP sebagai bahan untuk meningkatkan keamanan siber dan mencegah serangan. Platform tersebut diolah sendiri oleh Bank Indonesia yang di dalamnya mencakup *filtering, formatting* dan setiap analisis serangan akan dibagikan oleh bank lainnya. Setiap informasi yang diberikan oleh organisasi melalui *sharing platform* yang bersifat *vulnerability, threat* dan lainnya dilengkapi dengan aturan TLP yang TLP tersebut mengatur informasi mana saja yang dibagikan kepada publik, sesama organisasi terkait, antara BI dan pengirim informasi saja atau ke antar anggota CSSP saja [28]. CSSP-SP dibentuk pada tahun 2019 yang beranggotakan 60 peserta yang berasal dari industri sistem pembayaran khususnya perbankan [29]. Alur kerja CSSP dapat dilihat pada Gambar 2.

Gambar 2. Alur Kerja *Cyber Security Sharing Platform* - Sistem Pembayaran [28]

Dalam lingkup kerja sama internasional di bidang ISAC, BI menyatakan bahwa negara-negara ASEAN berkomitmen meningkatkan upaya pemulihan dari dampak pandemi Covid-19 dan mendorong pertumbuhan ekonomi jangka panjang melalui dukungan digitalisasi [30]. Salah satu komitmen tersebut berkaitan dengan berbagi informasi keamanan siber yaitu disebutkan bahwa negara-negara ASEAN mengapresiasi dan mendukung operasionalisasi dari ASEAN *Cybersecurity Resilience and Information Sharing Platform* (CRISP) sebagai sarana berbagi informasi di antara bank sentral ASEAN dalam menangani ancaman *cybersecurity* dan mengembangkan langkah-langkah mitigasi bersama [31].

3. METODE PENELITIAN

Objek penelitian ini yaitu ekosistem sistem pembayaran Indonesia yang melibatkan entitas-entitas pada sektor perbankan dan keuangan. Penelitian ini memanfaatkan *toolkit* ENISA *ISAC in a Box* untuk menentukan rekomendasi. Gambar 3 menunjukkan model penelitian yang dilakukan yang dilandaskan pada *toolkit* ENISA *ISAC in a Box* pada tahap *build*, yang terdiri dari tujuan, ruang lingkup dan aktivitas, keanggotaan, tata kelola, metode pertukaran informasi, dan pembiayaan ISAC.

Gambar 3. Model Penelitian

Toolkit ENISA ISAC *in a Box* ini dimanfaatkan dalam penelitian yang berfokus pada tahap *build*

ISAC pada sektor perbankan dan keuangan di Indonesia. Tahapan pada penelitian ini yang memuat ENISA ISAC *in a Box* tahap *Build* yaitu (i) menggambarkan kondisi terkini mengenai implementasi FS-ISAC di Indonesia; (ii) mengembangkan ekosistem FS-ISAC di Indonesia dengan pendekatan ENISA ISAC *in a Box* tahap *Build*, terdiri dari tujuan, ruang lingkup dan aktivitas, keanggotaan, tata kelola, metode pertukaran informasi, dan pembiayaan; (iii) menggambarkan ekosistem FS-ISAC yang diusulkan dengan mengacu pada penyelenggaraan sebelumnya.

4. HASIL PENELITIAN DAN ANALISIS

Dalam Bagian 4, hasil penelitian dan analisis terdiri dari Usulan Ekosistem dan Pengembangan Ekosistem FS-ISAC di Indonesia.

4.1. Usulan Ekosistem FS-ISAC di Indonesia

4.1.1. Tujuan FS-ISAC

Tahap pertama dalam pembangunan FS-ISAC adalah mendefinisikan sasaran dan tujuan. Sasaran dan tujuan tersebut harus dituangkan dalam dokumen tertulis seperti *Term of Reference* (ToR), didiskusikan, dikembangkan serta disepakati oleh seluruh anggota. Beberapa sasaran dan tujuan yang dapat dijadikan rekomendasi dalam pembentukan FS-ISAC di Indonesia antara lain meningkatkan kewaspadaan bersama terkait dengan ancaman siber, mengurangi waktu respons insiden yang diperlukan ketika terjadi insiden, berbagi informasi *best practice* dan *lesson learned* terhadap suatu insiden. Selain itu untuk meningkatkan kapabilitas sumber daya yang dimiliki masing-masing organisasi, meningkatkan budaya keamanan siber, dan kampanye keamanan siber pada sektor lain termasuk pada masyarakat luas.

4.1.2. Ruang Lingkup dan Aktivitas FS-ISAC

Ruang lingkup yang ada pada FS-ISAC berfokus pada pertukaran dan berbagi informasi keamanan siber pada sektor keuangan di Indonesia. Berbagi informasi ini tidak hanya melakukan pertukaran informasi saja, namun juga proses analisis informasi keamanan siber. Selain itu, terdapat beberapa program yang dapat dijalankan seperti:

1. *Cyber Session* merupakan program yang dapat dilakukan oleh entitas di dalam FS-ISAC terkait praktik dan strategi pertahanan siber hingga pertukaran informasi mengenai *cyber threat intelligence* hingga indikator ancaman keamanan siber yang bisa dianalisis lebih lanjut oleh masing-masing anggota di dalam FS-ISAC. *Cyber session* ini dapat dilakukan secara rutin.
2. *Cyber Portal* merupakan program yang dapat diterapkan oleh FS-ISAC dengan melibatkan peran *platform* berupa *portal website* yang diakses oleh ahli dan analis keamanan siber untuk berbagi informasi dan diskusi, seperti informasi intelijen ancaman, profil sumber ancaman, *monitoring* sistem elektronik, hingga kerentanan siber.
3. Kolaborasi penelitian ancaman siber merupakan program yang memanfaatkan *platform* seperti *Cyber Portal* untuk repositori dan analisis lanjutan keamanan siber, baik analisis ancaman, kerentanan, hingga sumber ancaman.
4. C*yber Exchange Forum* adalah program berupa forum yang berisikan antar anggota FS-ISAC terkait diskusi panel, strategi ISAC, hingga sesi berbagi informasi keamanan siber antar entitas.
5. FS-ISAC *Annual Conference* merupakan program kegiatan berupa konferensi terkait berbagi informasi keamanan siber antar anggota, baik entitas di dalam FS-ISAC maupun komunitas dalam lingkup yang lebih luas.

4.1.3. Keanggotaan FS-ISAC

Pada dasarnya keanggotaan FS-ISAC bersifat sukarela. Anggota yang mewakili organisasi dalam FS-ISAC tidak harus merupakan seorang manajer namun setidaknya harus memiliki kapabilitas seperti memiliki kompetensi yang cukup untuk berbagi dan mengambil manfaat dari diskusi, memiliki mandat yang cukup mewakili organisasi agar dapat menyampaikan pendapat dalam rapat, merasa berkomitmen untuk berpartisipasi aktif dan berkontribusi dalam diskusi, dan mampu berkontribusi dengan menerima informasi yang relevan baik yang bersifat strategis maupun teknis.

Dalam desain FS-ISAC di Indonesia, diusulkan bahwa anggota FS-ISAC adalah organisasi yang telah menjadi anggota Asosiasi Sistem Pembayaran Indonesia (ASPI). ASPI merupakan organisasi nirlaba yang didirikan atas prakarsa Bank Indonesia. ASPI memiliki peran, tugas dan fungsi membuat ketentuan dalam industri sistem pembayaran yang bersifat teknis dan mikro guna mendukung fungsi Bank Indonesia sebagai pembuat kebijakan dan peraturan agar terciptanya sistem pembayaran yang efisien, aman dan andal, serta menjadi wadah atas perubahan dan dinamika yang terjadi pada sistem pembayaran untuk memenuhi kebutuhan anggota ASPI dalam rangka meningkatkan peran pelaku sistem pembayaran di Indonesia.

Anggota FS-ISAC merupakan anggota ASPI yang bersedia secara sukarela untuk bergabung dalam FS-ISAC yang anggota ASPI tersebut terdiri dari Bank dan institusi non-Bank antara lain perusahaan *Financial Technology* (*Fintech*), Prinsipal, Lembaga, *Switching*, Perusahaan Telekomunikasi, *Central Depository* serta institusi lain yang terkait dengan sistem pembayaran di Indonesia. Anggota ASPI per Juni 2022 berjumlah 201 anggota yang terdiri dari 122 Anggota Biasa, dan 79 Anggota Afiliasi yang 119 di antaranya adalah Bank dan 82 lembaga selain bank. Kategori anggota biasa terdiri dari Bank, Lembaga selain bank yang memenuhi syarat permodalan minimum yang ditetapkan ASPI serta anggota pendiri

ASPI sedangkan anggota afiliasi terdiri dari Bank Perkreditan Rakyat (BPR), Lembaga Selain Bank (LSB) yang telah memperoleh izin dari Bank Indonesia namun belum memenuhi syarat permodalan minimum yang ditetapkan serta institusi lainnya.

4.1.4. Tata Kelola FS-ISAC

Dalam menjalankan FS-ISAC di Indonesia, peran dari tata kelola berbagi informasi keamanan siber juga perlu diperhatikan. Terdapat peran entitas dalam struktur ISAC yang termuat hingga hubungan entitas pada FS-ISAC. Peran utama yang perlu diperhatikan adalah dari tiga entitas utama, yaitu Bank Indonesia, anggota FS-ISAC, dan BSSN.

Bank Indonesia memiliki peran sangat penting terkait penyelenggaraan FS-ISAC di Indonesia. Bank Indonesia memiliki kewenangan terkait penyelenggaraan berbagi informasi sektor keuangan di Indonesia. Bank Indonesia juga dapat bertindak sebagai penyaring informasi sesuai dengan klasifikasi informasi, seperti *Traffic Light Protocol* sesuai sensitivitas informasi di dalamnya. *Traffic Light Protocol* tersebut memiliki kategori yaitu *red, amber, green,* dan *white.*

Anggota FS-ISAC di Indonesia terdiri dari berbagai entitas yang keseluruhan anggota ini memiliki hubungan sebagai penerima hingga pemilik informasi. Anggota memiliki hak untuk memperoleh informasi hingga membagikan informasi miliknya kepada entitas lain sesuai dengan klasifikasi informasi yang berlaku. Anggota FS-ISAC merupakan entitas utama dan memiliki hubungan dalam pertukaran informasi di dalam ISAC.

BSSN memiliki peran yaitu sebagai pembina jalannya FS-ISAC di Indonesia. BSSN membina dari sisi pelaksanaan tata kelola, manajemen risiko, kepatuhan, hingga pengembangan ekosistem yang berjalan di dalam FS-ISAC. Proses berbagi informasi keamanan siber yang berjalan pada FS-ISAC dapat dimanfaatkan BSSN untuk pengambilan keputusan atau pembuatan regulasi dan kebijakan selanjutnya. Selain itu, BSSN juga memberikan analisis dan informasi seputar keamanan siber di dalam jaringan ISAC untuk memperkaya berbagi informasi keamanan siber di sektor keuangan dan perbankan.

Peran lainnya yaitu dari sisi komunitas eksternal. Komunitas eksternal juga terlibat di dalam FS-ISAC di Indonesia, seperti komunitas dalam lingkup perbankan maupun asosiasi terkait. Komunitas tidak terbatas hanya pada lingkup Indonesia saja, namun bisa berdampak lebih luas yaitu komunitas FS-ISAC antar negara, seperti FS-ISAC di Jepang dan Amerika Serikat. Komunitas ini dapat menyalurkan pertukaran informasi keamanan siber yang berhubungan dengan ancaman hingga kerentanan siber di sektor keuangan.

4.1.5. Metode Pertukaran Informasi FS-ISAC

Proses pertukaran informasi merupakan bagian terpenting dalam ISAC. Pertukaran informasi dapat dilakukan dalam berbagai metode di antaranya melalui pertemuan fisik, email yang terenkripsi, *tele-conference* atau platform kolaborasi. Pada metode pertemuan fisik dilakukan di awal pembentukan grup ISAC yang dilaksanakan oleh ketua penyelenggara dalam hal ini adalah Bank Indonesia. Pertemuan ini akan berkontribusi pada komitmen anggota dan membangun kepercayaan.

Beberapa hal dapat disepakati dalam pertemuan misalnya terkait dengan struktur organisasi, administrasi, operasional dan strategis seperti penentuan visi misi dan ruang lingkup. Selain melalui rapat fisik, penyelenggaraan ISAC juga dapat menginisiasi pertemuan melalui *tele-conference* sesuai dengan kebutuhan. Metode lain yang dapat digunakan adalah melalui email terenkripsi yang telah disepakati dalam grup. Metode ini akan membuat percakapan dan pertukaran informasi menjadi hidup meskipun dilakukan di luar rapat. Anggota dapat mengajukan pertanyaan bila diperlukan, berbagi dokumen dan mendiskusikan topik yang tidak tercakup dalam pertemuan. Metode ini lebih cocok untuk masalah langsung seperti ancaman dan insiden yang memerlukan tindakan segera. Metode lain adalah dengan membuat platform kolaborasi yang dapat dimanfaatkan seluruh anggota ISAC. Dalam platform tersebut dapat diisi seperti daftar kontak anggota yang diperbaharui secara periodik, informasi yang dibagikan oleh anggota, risalah rapat pertemuan, *best practice*, forum diskusi bagi para anggota.

Dalam hal jenis informasi beberapa jenis informasi yang dapat dibagikan antara lain: *threat information; vulnerability information, incident information; mitigation; good practice; situational metrics; compliance topics;* dan *law enforcement and intelligence information.*

4.1.6. Pembiayaan FS-ISAC

Program kegiatan terkait FS-ISAC dapat dilakukan proses kolaborasi keamanan siber antar entitas di sektor keuangan di Indonesia. Program yang berkaitan dengan kegiatan berbagi informasi keamanan siber oleh FS-ISAC ini tidak terlepas dari pembiayaan hingga tanggung jawab keberlangsungan program ISAC. Program ini melibatkan dua entitas utama yang memiliki peran penting keamanan siber di sektor keuangan, yaitu Bank Indonesia dan BSSN.

Bank Indonesia merupakan entitas yang paling layak untuk membangun ekosistem ISAC sesuai dengan kebutuhan di sektor keuangan. Penganggaran FS-ISAC di Indonesia ini bisa disesuaikan dengan kebutuhan kewajiban Bank Indonesia dalam menyediakan sistem berbagi informasi hingga sumber daya. Bank Indonesia bisa bekerja sama dengan BSSN terkait pengembangan ekosistem FS-ISAC. Bank Indonesia dapat menganggarkan sumber daya yang terkait, seperti platform yang dibutuhkan dalam rangka berjalannya program berbagi informasi keamanan siber pada FS-ISAC di Indonesia.

BSSN sebagai pembina juga dapat berperan penting dalam pembiayaan atau anggaran sebagai

pembina komunitas keamanan siber pada sektor keuangan di Indonesia. BSSN dapat menganggarkan setiap kegiatan pembinaan komunitas, pengembangan ekosistem FS-ISAC, manajemen risiko penyelenggaraan ISAC, hingga pengurusan regulasi berbagi informasi keamanan siber di sektor keuangan.

Pembiayaan ini dimaksud untuk berjalannya FS-ISAC di Indonesia. Namun, pada implementasinya, FS-ISAC ini dijalankan berdasarkan sukarela tanpa adanya pungutan biaya keanggotaan. Berbagi informasi keamanan siber ini ditujukan untuk menguatkan ekosistem keamanan siber pada sektor keuangan di Indonesia.

4.2. Rekomendasi Pengembangan Ekosistem FS-ISAC di Indonesia

Pada pengembangan ekosistem FS-ISAC di Indonesia diusulkan modifikasi terhadap proses penyelenggaraan FS-ISAC melalui platform CSSP. Modifikasi dilakukan terhadap beberapa bagian meliputi sumber informasi, metode berbagi informasi, serta klasifikasi informasi. Rekomendasi pengembangan ini didasarkan pada beberapa rujukan ilmiah yang menjadi *best practice* penyelenggaraan ISAC. Best practice ini dikeluarkan oleh beberapa negara dan beberapa organisasi keamanan siber. Beberapa *best practice* penyelenggaraan ISAC yaitu:

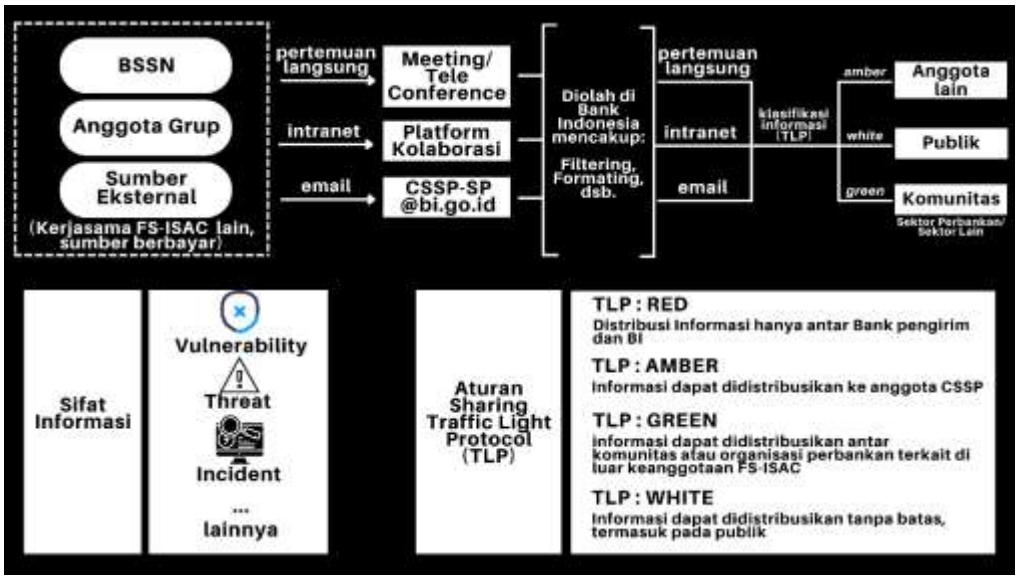
- Fasilitasi mekanisme berbagi informasi dengan sistem elektronik yang mendukung otomatisasi guna meningkatkan efisiensi [32] [33].
- Desain model CIS dengan mempertimbangkan perlindungan privasi [34].
- Lakukan proses berbagi informasi secara dua arah dengan jenis yang melibatkan sektor publik dan swasta (*Public Privat Partnership*) [32].
- Lindungi informasi sensitif dan berklasifikasi [33].
- Peserta berbagi informasi harus mengikuti aturan *Traffic Light Protocol* (TLP) ketika berbagi informasi [35].
- Ketika grup ISAC sudah berjalan, kembangkan sumber informasi sehingga informasi yang dibagikan lebih valid dan beragam [33].
- Kembangkan teknologi sebagai sarana dalam penyelenggaran ISAC [35].

Rekomendasi pengembangan penyelenggaraan ekosistem FS-ISAC di Indonesia dapat dilihat pada Gambar 4. Gambar 4 menunjukkan bahwa sumber informasi dalam FS-ISAC berasal dari tiga sumber utama yaitu anggota FS-ISAC, BSSN, dan sumber eksternal. Pada sumber yang berasal dari anggota, setiap anggota dapat membagikan informasi yang dimiliki kepada anggota lain. BSSN selaku penyelenggara keamanan siber nasional juga dapat memperkaya informasi. Informasi yang diperoleh BSSN merupakan informasi dengan validitas yang tinggi karena telah diolah dan dianalisis sehingga dapat dikonsumsi oleh *stakeholder* terkait termasuk industri sistem pembayaran. Selain kedua sumber di atas FS-ISAC juga dapat memperkaya informasi hasil kerja sama dengan FS-ISAC pada negara lain serta sumber berbayar lainnya.

Pengembangan ekosistem FS-ISAC di Indonesia yang diusulkan ini mengacu pada *toolkit* ISAC *in a Box* yang terdiri dari tahap *build*, meliputi tujuan, ruang lingkup dan aktivitas, keanggotaan, tata kelola, metode pertukaran informasi, dan pembiayaan ISAC. Ekosistem pada *Financial ISAC* ini juga memuat *best practice* dengan fokus kondisi terkait beberapa komponen penting di dalam ekosistem, seperti sifat informasi, aturan berbagi informasi (TLP), pihak pengguna dan pemilik informasi, cara pengolahan dan penyimpanan informasi, hingga program dan kegiatan pelaksanaan FS-ISAC.

Pengembangan ekosistem FS-ISAC memiliki beberapa nilai tambah dalam penyelenggaraannya di antaranya sebagai berikut:

- Informasi yang dibagikan akan lebih beragam dan valid karena didukung dengan sumber eksternal meliputi kerjasama dengan pihak lain, organisasi



Gambar 4. Rekomendasi Pengembangan FS-ISAC di Indonesia

keamanan siber nasional, serta sumber berbayar.

- Informasi yang dibagikan akan lebih efektif dan efisien karena didukung oleh motode berbagi informasi yang lebih beragam meliputi melalui meeting yang dapat meningkatkan kepercayaan, platform kolaborasi maupun melalui email.
- Informasi yang dibagikan akan lebih terjamin keamanannnya karena telah menerapkan TLP, sehingga pemilik informasi akan lebih memiliki kepercayaan untuk berbagi informasi, metode ini juga meningkatkan motivasi berbagi informasi.

5. KESIMPULAN

Kesimpulan dalam penelitian ini yaitu Bank Indonesia telah memiliki sarana berbagi informasi keamanan siber yang dikemas melalui platform *Cyber Security Sharing Platform* (CSSP). Platform tersebut berisi mengenai sifat informasi seperti informasi terkait kerentanan, ancaman, hingga insiden siber. Terdapat pula aturan *Traffic Light Protocol* pada berbagi informasi hingga sistem berbagi informasi keamanan siber yang berfokus pada sistem pembayaran. Usulan ekosistem FS-ISAC di Indonesia terdiri dari tujuan dan sasaran FS-ISAC dengan 6 rekomendasi, ruang lingkup dan aktivitas yang terdiri dari 5 program kegiatan dan berfokus pada berbagi informasi keamanan siber serta analisisnya, keanggotaan dengan organisasi yang menjadi anggota Asosiasi Sistem Pembayaran Indonesia (ASPI), Tata Kelola dengan klasifikasi informasi terkait dan peran entitas pada FS-ISAC, metode pertukaran informasi, serta pembiayaan yang dapat diinisiasi oleh Bank Indonesia dan BSSN pada masing-masing tugas dan fungsi pada ISAC. Pengembangan ekosistem FS-ISAC di Indonesia dilakukan pada beberapa bagian di antaranya sumber informasi yang dibagikan dengan melibatkan peran BSSN dan sumber eksternal, metode pertukaran informasi dengan menambahkan metode pertemuan langsung dan platform kolaborasi, serta pembagian informasi dengan TLP.

Saran dalam penelitian ini yaitu pengembangan ekosistem FS-ISAC yang diusulkan dapat dijadikan pertimbangan dalam mengembangkan penyelenggaraan ISAC yang telah dijalankan oleh Bank Indonesia. Penelitian selanjutnya dapat dikembangkan dengan melakukan implementasi tahapan lain pada *ENISA ISAC in a Box* yaitu tahap *run, evaluate,* dan *improvement.*

REFERENSI

[1] B. S. d. S. N. Direktorat Operasi Keamanan Siber, "Laporan Monitoring Keamanan Siber 2021," BSSN RI, https://bssn.go.id, 2021.

[2] (2015). *Sharing Cyber Security Information - Good Practice from the Dutch Public Private Participation Approach*.

[3] J. Pöyhönen, V. Nuojua, M. Lehto, and J. Rajamäki, "Cyber Situational Awareness and Information Sharing in Critical Infrastructure Organizations," *Information & Security: An International Journal*, vol. 43, pp. 236-256, 01/01 2019, doi: 10.11610/isij.4318.

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

[5] 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.

[6] 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.

[7] B. Indonesia, "Blueprint Sistem Pembayaran Indonesia 2021, Bank Indonesia : Menavigasi Sistem Pembayaran Nasional di Era Digital," Bank Indonesia, Jakarta, 2019. [Online]. Available: https://www.bi.go.id/id/publikasi/kajian/Documents/Blueprint-Sistem-Pembayaran-Indonesia-2025.pdf

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] K. Yan, W. Shen, Q. Jin, and H. Lu, "Emerging Privacy Issues and Solutions in Cyber-Enabled Sharing Services: From Multiple Perspectives," *IEEE Access*, vol. 7, pp. 26031-26059, 2019, doi: 10.1109/ACCESS.2019.2894344.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] ENISA, *Information Sharing and Analysis Centres (ISACs) Cooperative models*. 2018.

[24] N. A. Kollars and A. Sellers, "Trust and information sharing: ISACs and U.S. Policy," *Journal of Cyber Policy*, vol. 1, no. 2, 2016, doi: 10.1080/23738871.2016.1229804.

[25] L. W. II, M. Tsuchiya, and R. Repko, "Improving Cybersecurity Cooperation between the Governments of the United States and Japan," *SASAKAWA USA*, 2020.

[26] (2017). *ENISA Information Sharing and Analysis Center -ISACs- Cooperative models*.

[27] 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).

[28] O. P. Sandy. "BI Bilang Sudah Punya Cyber Security Sharing Platform." cyberthreat.id. https://cyberthreat.id/read/11174/BI-Bilang-Sudah-Punya-Cyber-Security-Sharing-Platform (accessed 12 Juli 2022, 2022).

[29] B. Indonesia, "Laporan Tahunan 2019 "Sinergi, Transformasi, dan Inovasi Menuju Indonesia Maju"," Bank Indonesia, Jakarta, 2019. [Online]. Available: https://www.bi.go.id/id/publikasi/laporan/Documents/LTBI_2019-ID.pdf

[30] T. Suyudi. "Digitalisasi Jadi "Senjata" ASEAN Pulihkan Ekonomi." itworks.id. https://www.itworks.id/38465/digitalisasi-jadi-senjataasean-pulihkan-ekonomi.html (accessed 12 Juli 2022, 2022).

[31] B. Indonesia, "Komitmen Pemulihan, Digitalisasi, dan Keberlanjutan Ekonomi ASEAN," D. Komunikasi, Ed., ed: Bank Indonesia, 2021.

[32] A. G. Zaballos and I. Jeun, "Best Practice for Critical Information Infrastructure Protection (CIIP) - Experiences from Latin America and the Caribbean and Selected Countries," *Inter-American Development Bank*, 2016.

[33] I. B. Tolga, "Whole of Government Cyber Information Sharing," *NATO Cooperative Cyber Defence Center of Excellence (CCDCOE)*, 2019.

[34] C. Goodwin and J. P. Nicholas, "A Framework for Cybersecurity Information Sharing and Risk Reduction," *Microsoft Corporation*, 2015.

[35] e. a. Felix Antonio, "Information Sharing and Analysis Centers (ISACs) Cooperative Models," *The European Union Agency for Network and Information Security*, 2017.