Keamanan Jaringan
(Cyber Security Framework)

Dosen Pembimbing :
Dr. Ferry Astika Saputra, ST., M.Sc.

Disusun Oleh :
Fifin Nur Rahmawati (3122640040)

1 D4 – IT B LJ

PROGRAM STUDI TEKNIK INFORMATIKA
DEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

2023/2024

1. Jelasakan tentang CSF v2 dengan menggunakan referensi :
   https://www.nist.gov/cyberframework

Makalah Konsep Kerangka Kerja Keamanan Siber 2.0 NIST:
Potensi Pembaruan Signifikan pada Kerangka Kerja Keamanan Siber

Konsep CSF 2.0 Paper: Potensi Pembaruan Signifikan pada CSF

Pendahuluan :

Kerangka Kerja Keamanan Siber NIST (CSF atau Kerangka Kerja) memberikan panduan bagi organisasi untuk lebih memahami, mengelola, mengurangi, dan mengomunikasikan risiko keamanan siber. Ini adalah sumber daya dasar dan penting yang digunakan oleh semua sector di seluruh dunia. Meskipun risiko keamanan siber terus berkembang, banyak responden RFI Keamanan Siber NIST melaporkan bahwa CSF tetap efektif dalam menangani risiko keamanan siber dengan memfasilitasi tata kelola dan program manajemen risiko serta meningkatkan komunikasi di dalam dan di seluruh organisasi. CSF telah diadopsi secara sukarela dan dalam kebijakan dan mandat pemerintah di semua tingkatan di seluruh dunia, yang mencerminkan sifatnya yang tahan lama dan fleksibel untuk melampaui risiko, sektor, teknologi, dan batas-batas negara.

Otoritas hukum untuk CSF mengarahkan NIST untuk "memfasilitasi dan mendukung pengembangan" Kerangka Kerja dan "berkoordinasi secara erat dan teratur" dengan organisasi terkait.1 Dengan keterlibatan komunitas yang luas , NIST awalnya membuat Kerangka Kerja pada tahun 2014 dan memperbaruinya pada tahun 2018 dengan CSF 1.1. CSF diperbarui secara terbuka dengan masukan dari pemerintah, akademisi, dan industri, termasuk melalui lokakarya, tinjauan dan komentar publik, dan bentuk keterlibatan lainnya. Dengan pembaruan ini, NIST terbuka untuk melakukan perubahan yang lebih substansial daripada pembaruan sebelumnya. Versi "CSF 2.0" mencerminkan lanskap keamanan siber yang terus berkembang tetapi kebutuhan komunitas akan mendorong tingkat dan konten perubahan. Garis waktuawal CSF 2.0 diusulkan dalam gambar ini:

Potensi Perubahan Signifikan dalam CSF 2.0

1. CSF 2.0 akan secara eksplisit mengakui penggunaan CSF secara luas untuk memperjelas potensi aplikasinya

1.1. Ubah judul dan teks CSF untuk mencerminkan tujuan penggunaannya oleh semua organisasi

CSF 2.0 akan menggunakan nama yang lebih luas dan umum digunakan, "Kerangka Kerja Keamanan Siber", bukan "Kerangka Kerja untuk Meningkatkan Keamanan Siber Infrastruktur Kritis."

1.2. Cakupan CSF untuk memastikan CSF memberikan manfaat bagi organisasi terlepas dari sektor, jenis, atau ukurannya

CSF adalah sumber daya yang diakui untuk organisasi negara bagian dan lokal di bawah Program Hibah Keamanan Siber Negara Bagian dan Lokal dari Departemen Keamanan Dalam Negeri (DHS)4 dan telah dirujuk secara luas oleh banyak asosiasi serta lembaga pemerintah di berbagai tingkatan

1.3. Meningkatkan Kolaborasi dan Keterlibatan Internasional

Untuk memfasilitasi kolaborasi dan keterlibatan internasional, NIST akan memprioritaskan pertukaran dengan pemerintah dan industri asing sebagai bagian dari pengembangan CSF 2.0. NIST akan terus terlibat secara langsung dan melalui kemitraan antarlembaga untuk berbagi manfaat penggunaan CSF, serta meminta masukan mengenai potensi perubahan, sehingga CSF dapat terus diakui sebagai sumber daya internasional.

2. CSF 2.0 akan tetap menjadi kerangka kerja, memberikan konteks dan koneksi kestandar dan sumber daya yang ada

2.1 Mempertahankan tingkat detail CSF saat ini

NIST bertujuan untuk mempertahankan tingkat detail dan kekhususan saat ini dalam CSF 2.0 untuk memastikan bahwa kerangka kerja ini tetap dapat diskalakan dan fleksibel untuk berbagai banyak organisasi. Fungsi dari CSF adalah termasuk memberikan konteks untuk bahasa yang lebih spesifik yang biasa digunakan dalam sebagian besar standar keamanan siber.

2.2. Menghubungkan CSF dengan jelas ke kerangka kerja NIST lainnya

Kerangka kerja terkait keamanan siber dan privasi NIST lainnya - Kerangka Kerja Manajemen Risiko, Kerangka Kerja Privasi, Kerangka Kerja Tenaga Kerja Pendidikan Keamanan Siber, dan Kerangka Kerja Pengembangan Perangkat Lunak yang Aman - akan tetap menjadi kerangka kerja yang terpisah. Masing-masing berfokus pada topik topik spesifik yang layak untuk panduan khusus. Namun, seperti yang ditunjukkan oleh para pemberi komentar, setiap kerangka kerja memiliki hubungan dengan CSF, sehingga akan dirujuk sebagai panduan baik dalam CSF 2.0 atau dalam

materi pendamping, seperti pemetaan. Sebagai contoh, CSF 1.1 diterbitkan sebelum publikasi Kerangka Kerja Privasi; oleh karena itu, Bagian 3.6 CSF, Metodologi untuk Melindungi Privasi dan Kebebasan Sipil dapat diubah dalam CSF 2.0 untuk membahas bagaimana Kerangka Kerja Privasi dapat dimanfaatkan saat menerapkan CSF.

2.3 Memanfaatkan Alat Referensi Keamanan Siber dan Privasi untuk Inti CSF 2.0 online

Selain format PDF dan Excel, CSF 2.0 akan dipamerkan melalui NIST Cybersecurity and Privacy Reference Tool (CPRT) yang baru saja diluncurkan. CPRT menawarkan format yang dapat dibaca oleh mesin dan antarmuka pengguna yang konsisten untuk mengakses data referensi dari standar, pedoman, dan kerangka kerja keamanan siber dan privasi NIST, serta pendekatan yang fleksibel untuk mengkarakterisasi hubungan antara standar, pedoman, dan kerangka kerja, serta berbagai aplikasi dan teknologi.

2.4 Gunakan Referensi Informatif online yang dapat diperbarui

Pada CSF 2.0, NIST akan bergerak ke arah penggunaan referensi online yang dapat diperbarui yang ditampilkan melalui CPRT. Sejak publikasi CSF 1.1, beberapa sumber daya telah dipetakan ke CSF di luar yang termasuk dalam CSF 1.1 Core. Sebagai contoh, Katalog Online Informative References Pro gram (OLIR) berisi sekitar dua lusin sumber daya yang dipetakan ke CSF, termasuk versi terbaru dari Informative References yang termasuk dalam CSF 1.1 Core, serta pemetaan tambahan yang tidak termasuk dalam CSF 1.1 Core. Pemetaan lebih lanjut, terutama untuk standar khusus sektor atau kasus penggunaan tertentu, juga dapat ditemukan di Profil sampel CSF dan publikasi NIST, seperti Panduan Praktik Keamanan Siber (seri SP 1800) yang diterbitkan oleh National Cybersecurity Center of Excellence (NCCoE).

2.5 Gunakan Referensi Informatif untuk memberikan panduan lebih lanjut dalam mengimplementasikan CSF

Ajakan untuk Bertindak - Sediakan Pemetaan: NIST menyambut baik pengiriman pemetaan ke CSF. NIST mendorong penulis/pemilik sumber daya keamanan siber yang relevan untuk terhubung dengan NIST 1) untuk mengembangkan pemetaan ke CSF 1.1 jika pemetaan tidak ada untuk memudahkan pengembangan pemetaan ke CSF 2.0, dan 2)

2.6 Tetap netral terhadap teknologi dan vendor, namun mencerminkan perubahan dalam praktik keamanan siber

CSF 2.0 akan tetap bersifat netral teknologi dan vendor. NIST mengakui bahwa lanskap teknologi telah berubah secara signifikan sejak publikasi awal CSF. Sementara komentar RFI mengusulkan agar Kerangka Kerja membahas topik, teknologi, dan aplikasi tertentu dalam pembaruan CSF, yang lain memperingatkan agar tidak membahayakan penerapan CSF secara luas. Agar tetap netral terhadap teknologi, NIST akan bekerja untuk meninjau CSF sehingga hasilnya yang luas dapat terus dimanfaatkan oleh organisasi terlepas dari teknologi atau layanan yang mereka gunakan, termasuk TI, IoT, OT, dan layanan cloud.

3. **CSF 2.0 (dan sumber daya pendamping) akan mencakup panduan yang diperbarui dan diperluas tentang implementasi Kerangka Kerja**
   Terdapat lebih dari 500 referensi dalam tanggapan RFI yang mendukung perlunya lebih banyak panduan untuk mendukung implementasi CSF, dan banyak pengguna yang menyatakan keinginan untuk mendapatkan detail yang lebih besar dalam CSF sambil mempertahankan pendekatan yang tidak bersifat preskriptif. Permintaan akan panduan tambahan untuk membantu organisasi dalam mempertimbangkan dan menggunakan CSF datang dari berbagai macam organisasi yang memiliki kebutuhan dan risiko yang sangat berbeda. Banyak yang akan mendapatkan manfaat dari deskripsi langsung dan lebih umum tentang komponen utama Kerangka Kerja, sementara yang lain meminta informasi terperinci seperti lambang dan pemetaan untuk panduan keamanan siber tertentu dari NIST dan organisasi lain. Sehubungan dengan pengembangan CSF 2.0, NIST akan memenuhi kedua kebutuhan tersebut dengan menggunakan beberapa pendekatan.

3.1.1 Menambahkan contoh implementasi untuk Subkategori CSF

CSF 2.0 akan menyertakan contoh implementasi nosional dari proses dan aktivitas yang ringkas dan berorientasi pada tindakan untuk membantu mencapai hasil dari Subkategori CSF, di samping panduan yang disediakan dalam Referensi Informatif CSF. Menambahkan contoh-contoh nosional disarankan dalam tanggapan RFI dan telah berhasil dimanfaatkan dalam Kerangka Kerja NIST lainnya seperti Kerangka Kerja Pengembangan Perangkat Lunak yang Aman dan draf Buku Pedoman Kerangka Kerja Manajemen Risiko Kecerdasan Buatan. Untuk memastikan Inti CSF tetap tingkat tinggi dan ringkas, akan ada sejumlah kecil contoh nosional. Daftar kecil contoh ini tidak akan menjadi daftar lengkap dari semua tindakan yang dapat diambil oleh organisasi untuk memenuhi hasil CSF, dan juga tidak akan mewakili garis dasar Tindakan yang diperlukan untuk mengatasi risiko keamanan siber.

3.2 Mengembangkan templat Profil CSF

NIST telah menghasilkan contoh-contoh (dan mengumpulkan contoh-contoh yang dikembangkan oleh pihak lain - termasuk badan-badan dan asosiasi federal lainnya) untuk beberapa Profil khusus sektor dan ancaman yang dapat dimanfaatkan oleh organisasi untuk membangun Profil organisasinya. Contoh Profil ini memudahkan organisasi untuk menerapkan CSF dengan memprioritaskan dan menyelaraskan hasil CSF dengan risiko dan standar sektor dan ancaman tertentu. Contoh-contohnya dapat ditemukan di situs web NIST CSF. Sehubungan dengan pengembangan CSF 2.0, NIST akan membuat template dasar opsional untuk Profil CSF yang menyarankan format dan area yang harus dipertimbangkan dalam Profil. Meskipun organisasi dapat terus menggunakan format yang berbeda untuk Profil berdasarkan kebutuhan spesifik mereka, penggunaan template diharapkan dapat meningkatkan produksi Profil yang spesifik untuk sektor dan organisasi tertentu dan membuat pengembangan Profil lebih mudah bagi pengguna. NIST mencari umpan balik tentang konten apa yang harus dimanfaatkan dalam templat Profil CSF, termasuk konten yang saat ini disertakan oleh organisasi dalam Profil CSF mereka.

3.3 Memperbaiki situs web CSF untuk menyoroti sumber daya implementasi

Situs web CSF NIST berisi banyak informasi dan panduan tambahan tentang penerapan CSF. Ini termasuk berbagai sumber daya yang dikembangkan oleh NIST dan organisasi eksternal, termasuk contoh Profil CSF, pemetaan, panduan, alat bantu, studi kasus, kisah sukses, publikasi terkait (seperti Panduan Memulai Cepat CSF), dan webinar. Pembaruan Kerangka Kerja ini memberikan kesempatan untuk meningkatkan kesadaran akan sumber daya yang ada, serta mengidentifikasi sumber daya baru. Oleh karena itu, NIST akan mengubah situs web CSF untuk menyegarkan konten dan meningkatkan kegunaannya

4. CSF 2.0 akan menekankan pentingnya tata kelola keamanan siber

4.1 Menambahkan Fungsi Pengaturan baru

NIST, CSF 2.0 akan menyertakan Fungsi "Kelola" baru untuk menekankan hasil tata kelola manajemen risiko keamanan siber. Meskipun lima Fungsi CSF telah mendapatkan adopsi luas dalam kebijakan nasional dan internasional, termasuk standar ISO, NIST percaya bahwa ada banyak manfaat untuk memperluas pertimbangan tata kelola dalam CSF 2.0. Fungsi lintas sektoral yang baru ini akan menyoroti bahwa tata kelola keamanan siber sangat penting untuk mengelola dan mengurangi risiko keamanan siber. Tata kelola keamanan siber dapat mencakup penentuan prioritas dan toleransi risiko organisasi, pelanggan, dan masyarakat yang lebih luas; penilaian risiko dan dampak keamanan siber; penetapan kebijakan dan prosedur keamanan siber; serta pemahaman peran dan tanggung jawab keamanan siber. Kegiatan-kegiatan ini sangat penting untuk mengidentifikasi, melindungi, mendeteksi, merespons, dan memulihkan di seluruh organisasi, serta mengawasi pihak-pihak lain yang melakukan kegiatan keamanan siber untuk organisasi, termasuk di dalam rantai pasokan organisasi. Meningkatkan aktivitas tata kelola menjadi sebuah Fungsi juga akan mendorong penyelarasan aktivitas keamanan siber dengan risiko perusahaan dan persyaratan hukum.

4.2 Meningkatkan diskusi mengenai hubungan dengan manajemen risiko

Merevisi CSF menawarkan kesempatan untuk memperjelas hubungan antara tata kelola dan manajemen risiko keamanan siber di seluruh narasi CSF dan Core. CSF 2.0 akan menjelaskan bagaimana proses manajemen risiko yang mendasari sangat penting untuk mengidentifikasi menganalisis, memprioritaskan, merespons, dan memantau risiko, bagaimana hasil CSF mendukung keputusan respons risiko (menerima, memitigasi, memindahkan, menghindari), dan berbagai contoh proses manajemen risiko (mis. Kerangka Kerja Manajemen Risiko, ISO 31000) yang dapat digunakan untuk mendukung implementasi CSF.

5. CSF 2.0 akan menekankan pentingnya manajemen risiko rantai pasokan keamanan siber (C-SCRM)

5.1 Memperluas cakupan rantai pasokan

Responden RFI setuju bahwa risiko keamanan siber dalam rantai pasokan dan pihak ketiga merupakan risiko utama di seluruh organisasi. Meskipun sebagian besar responden setuju bahwa NIST tidak boleh mengembangkan Kerangka Kerja terpisah untuk mengatasi risiko ini,mereka memiliki pendapat yang beragam tentang bagaimana masalah ini harus ditanganidalam pembaruan CSF. Dengan meningkatnya globalisasi, outsourcing, dan perluasan penggunaan layanan teknologi (seperti komputasi awan), CSF 2.0 harus memperjelas pentingnya organisasi untuk mengidentifikasi, menilai, dan mengelola risiko pihak pertama dan ketiga. Namun, risiko pihakketiga mungkin melibatkan penilaian dan pengawasan yang berbeda yang sering kali ditangani oleh tim/organisasi yang terpisah. Oleh karena itu, NIST percaya bahwa CSF 2.0 harus menyertakan hasil spesifik C-SCRM tambahan untuk memberikan panduan tambahan untuk membantu organisasi mengatasi risiko yang berbeda ini. NIST mengundang umpan balik tentang cara terbaik untuk menangani C-SCRM dalam CSF 2.0. Pilihannya bisa meliputi: 1) mengintegrasikan lebih lanjut hasil C-SCRM di seluruh Inti CSF di seluruh Fungsi (integrasi dapat mencakup rantai pasokan secara terpisah atau sebagai pertimbangan sebagai bagian dari hasil yang lebih luas), 2) pembuatan Fungsi baru yang berfokus pada hasil yang terkait dengan pengawasan dan pengelolaan C-SCRM, atau 3) memperluas hasil C-SCRM di dalam Kategori ID.SC saat ini di Fungsi Identifikasi.

6. CSF 2.0 akan memajukan pemahaman tentang pengukuran dan penilaian keamanansiber

6.1 Memperjelas bagaimana memanfaatkan CSF dapat mendukung pengukuran dan penilaian program keamanan siber

CSF 2.0 akan memperjelas bahwa dengan memanfaatkan CSF, organisasi memiliki taksonomi dan leksikon yang sama untuk mengkomunikasikan hasil dari upaya pengukuran dan penilaian mereka, terlepas dari proses manajemen risiko yang mendasarinya. Di semua organisasi, tujuan utama pengukuran dan penilaian keamanan siber adalah untuk menentukan seberapa baik mereka mengelola risiko keamanan siber, dan jika dan bagaimana mereka terus meningkatkannya. Aktivitas yang mendukung pengukuran dan penilaian - dari tingkat system hingga seluruh organisasi - merupakan masukan untuk menentukan kematangan dan mendukung keputusan manajemen risiko.

6.2. Memberikan contoh pengukuran dan penilaian menggunakan CSF

Risiko, prioritas, dan sistem setiap organisasi adalah unik, sehingga metode dan tindakan yang digunakan untuk mencapai hasil yang dijelaskan oleh Kerangka Kerja Inti berbeda-beda.Dengan demikian, pengukuran dan penilaian hasil juga bervariasi tergantung pada konteksnya. Karena tidak ada pendekatan tunggal untuk mengukur dan

menilai CSF, NIST tidak akan mengedepankan pendekatan tunggal untuk penilaian dalam CSF 2.0 untuk melanjutkanfleksibilitas dalam bagaimana organisasi dapat menerapkan Kerangka Kerja

Terminologi Pengukuran: NIST memberikan latar belakang tentang terminologi terkait pengukuran untuk membantu memfasilitasi pemahaman bersama tentang topik-topik ini guna meningkatkan umpan balik pada makalah ini, serta diskusi pada lokakarya yang akan datang. Istilah dan konsep seputar pengukuran keamanan siber sangat bervariasi dan pada akhirnya didorong berdasarkan konteks penggunaannya. Definisi formal dari istilah-istilah ini dapat ditemukan dalam draf Panduan Pengukuran Kinerja untuk Keamanan Informasi, yang terbuka untuk komentar publik.

Penilaian - Tindakan mengevaluasi, memperkirakan, atau menilai berdasarkan kriteria yang ditetapkan. Pendekatan penilaian dapat bersifat kualitatif, kuantitatif, atau semi-kuantitatif. Contoh jenis penilaian termasuk penilaian risiko dan penilaian kontrol. Sebagai contoh, penilaian risiko dapat memanfaatkan matriks risiko dengan skala penilaian berwarna untuk menunjukkan kemungkinan dan dampak (pendekatan penilaian kualitatif), jumlah kerentanan yang diketahui dalam sistem atau organisasi (pendekatan penilaian kuantitatif), atau skala numerik yang representatif (misalnya, 1-10) untuk menunjukkan tingkat keparahan risiko (pendekatan penilaian semi-kuantitatif).

Pengukuran - Proses mendapatkan satu atau lebih nilai kuantitatif. Misalnya, jumlah upaya phishing yang berhasil dicegah melalui pelatihan dan kesadaran keamanan siber.

Metrik - Dirancang untuk i) memfasilitasi pengambilan keputusan; dan ii) meningkatkan kinerja dan akuntabilitas melalui pengumpulan, analisis, dan pelaporan data terkait kinerja yang relevan. Metrik digunakan untuk melacak, membandingkan, dan menilai kinerja atau proses dan terkait dengan tujuan atau persyaratan kinerja. Sebagai contoh, metrik efektivitas pelatihan keamanan siber adalah 80% pengguna melaporkan adanya upaya phishing.

6.3 Memperbarui Panduan Pengukuran Kinerja NIST untuk Keamanan Informasi

NIST memperbarui dokumen panduan pengukuran andalannya, Panduan Pengukuran Kinerja untuk Keamanan Informasi. SP 800-55r2 memberikan panduan kepada organisasi tentang penggunaan ukuran untuk meningkatkan pengambilan keputusan, kinerja, dan akuntabilitas program keamanan siber atau sistem informasi. Panduan ini berlaku untuk pengukuran berbagai aktivitas program keamanan siber, tetapi mengingat minat dalam pengukuran yang terkait dengan CSF 2.0, panduan ini mungkin sangat berguna bagi mereka yang memanfaatkan CSF. Dasar-dasar yang mendasari proses dan implementasi pengukuran keamanan siber tidak akan disertakan dalam CSF, melainkan dalam NIST SP 800-55.

6.4 Memberikan panduan tambahan tentang Tingkatan Implementasi Kerangka Kerja

Tingkatan CSF menyediakan mekanisme bagi organisasi untuk melihat dan memahami pendekatan mereka terhadap risiko keamanan siber serta proses dan program yang ada untukmengelola risiko tersebut. Tingkatan tersebut memiliki tingkat ketelitian dan kecanggihan yang semakin meningkat dalam menggambarkan praktik manajemen risiko keamanan siber secara keseluruhan, termasuk proses manajemen risiko, integrasi program manajemen risiko, dan partisipasi aktif dalam ekosistem keamanan siber yang lebih luas. Umpan balik dari RFI dan lokakarya menunjukkan bahwa organisasi menggunakan Tingkatan dengan berbagai cara dan untuk tujuan yang berbeda untuk memungkinkan fleksibilitas dalam implementasi, seperti yang dirancang pada awalnya. Contoh implementasi berkisar dari membantu menetapkan tujuan internal dan memprioritaskan kemampuan keamanan siber tertentu hingga mengkomunikasikan posisi keamanan siber organisasi dan membantu mengukur kematangan program keamanan siber serta implementasi hasil CSF di tingkat Fungsi, Kategori, dan Subkategori CSF. NIST mengundang umpan balik yang berkelanjutan tentang bagaimana organisasi menggunakan Tingkatan, mencatat permintaan untuk kejelasan yang lebih besar tentang Tingkatan dan untuk memastikan bahwa CSF 2.0 mencerminkan berbagai pendekatan. CSF 2.0 akan memperjelas ruang lingkup dan penerapan Tingkatan untuk menangani ketahanan proses manajemen risiko, program, dan komunikasi eksternal. Pembaruan ini juga akan menjelaskan dengan lebih baik hubungan antara Tingkatan dan konsep model kematangan, tetapi konsisten dengan pendekatan yang dijelaskan secara luas untuk menangani pengukuran keamanan siber (lihat 6.2), CSF 2.0 tidak akan memberikan model kematangan yang berbeda untuk memenuhi hasil CSF di tingkat Fungsi, Kategori, atau Subkategori. Sumber daya tambahan dapat mencakup panduan baru tentang bagaimana Tingkatan dapat digunakan dalam Profil CSF, dan peningkatan fokus pada sumber daya bagi komunitas untuk berbagi pemetaan di antara Tingkatan, proses manajemen risiko, dan model kematangan. NIST mencari umpan balik tambahan untuk menentukan nilai dari pergeseran fokus Jenjang ke tujuan dan sasaran dalam konteks tata kelola, termasuk apakah Jenjang harus terus menyertakan konsep "partisipasi eksternal", atau apakah Jenjang dapat berfungsi sebagai pendekatan penilaian kualitatif yang dapat dimasukkan ke dalam atau berdasarkan hasil dari Fungsi Govern yang baru yang diusulkan