LAPORAN TUGAS
NETWORK SECURITY

Cyber Security Framework 2.0

Oleh:

Nama	:	Fisabili Maghfirona Firdaus
NRP	:	3122640051
Kelas	:	LJ D4 IT-B

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

Kampus ITS, Jl. Raya ITS, Keputih, Kec. Sukolilo, Kota SBY,

Jawa Timur 60111

Telepon +62 31 594 7280 Fax. +62 31 594 6114

E-mail: *humas@pens.ac.id* Website: *pens.ac.id*

SURABAYA

2023

CYBER SECURITY FRAMEWORK 2.0

Cyber Security Framework merupakan sebuah framework yang dirilis oleh National Institute of Standards and Technology (NIST) dari Amerika Serikat sebagai benchmark pada organisasi dalam cyber security risk management. Tujuan dibuatnya CSF adalah untuk membantu organisasi dalam pengembangan dan memperkuat kemampuan dalam mengidentifikasi, melindungi, mendeteksi, respon, dan pemulihan dari serangan cyber.

CSF terdiri dari tiga bagian utama, yaitu Framework Core, Implementation Tiers, dan Framework Profiles. Framework Core adalah inti dari CSF yang terdiri dari lima fungsi utama yaitu Identify, Protect, Detect, Respond, dan Recover. Fungsi-fungsi ini mewakili langkah-langkah penting yang harus diambil oleh organisasi dalam mengelola cyber security risks.

Implementation Tiers adalah tingkatan atau level implementasi CSF yang digunakan untuk menentukan sejauh mana organisasi telah mengadopsi dan menerapkan CSF. Ada empat tingkatan implementasi yaitu Partial, Risk Informed, Repeatable, dan Adaptive.

Framework Profiles adalah representasi dari tujuan bisnis, cyber security risk, dan ketersediaan sumber daya organisasi yang digunakan untuk mengembangkan strategi cyber security yang sesuai dengan kebutuhan organisasi.

Secara keseluruhan, CSF adalah sebuah framework yang fleksibel dan dapat disesuaikan dengan kebutuhan dan profil risk dari setiap organisasi. CSF dapat membantu organisasi dalam mengidentifikasi dan mengurangi cyber security risk, meningkatkan kesiapan dan respons terhadap serangan cyber security, serta memperkuat kemampuan organisasi dalam memulihkan diri setelah terjadinya serangan.

CSF telah berkembang sejak lama dan semakin disempurnakan dalam setiap iterasi yang dikembangkan. Pada saat ini, CSF 2.0 sedang dalam konsep pengembangan dan telah merilis sebuah paper yang memuat banyak rancangan dari framework tersebut. Berikut adalah beberapa hal yang dimuat dalam paper "*NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework*"

1. CSF 2.0 akan dengan eksplisit mengklarifikasi penggunaan CSF secara luas.

   Pada hal ini, CSF 2.0 akan mengubah muatan dokumentasi untuk lebih fokus ke arah yang sesuai dengan perencanaan pengguna framework. Di mana scope yang diharapkan oleh pengembang mencakup organisasi pemerintahan, industri, dan pendidikan atau edukasi. Perubahan ini betujuan agar dapat menjadi relevan dengan perkembangan ekosistem.

   Kemudian selain dari scope tersebut, CSF 2.0 juga akan melakukan jangkauan pada sektor, jenis, dan tujuan yang lebih luas lagi. Dengan harapan CSF tidak digunakan oleh perusahaan besar saja, namun oleh banyak pihak sehingga dapat membantu dalam berbagai macam sektor. Selain itu, diharapkan banyak partisipasi yang dapat menghidupkan ekosistemnya.

Dan terakhir adalah dengan menambahkan kolaborasi di tingkat internasional. Hal ini diharapkan untuk dapat menambahkan pengalaman sehingga meningkatkan efisiensi dan efektifitas dalam pengembangan framework. NIST akan terus berpartisipasi dalam kegiatan internasional yang memanfaatkan CSF sebagai bagian dari upaya dan prioritas yang lebih luas untuk terlibat secara strategis dalam pengembangan standar internasional.

2. CSF 2.0 akan tetap menjadi sebuah framework dan menyediakan konteks dan koneksi pada standar dan resource yang ada.

   Mempertahankan tingkat detail dari CSF saat ini, framework ini akan terus menyediakan struktur pengorganisasian umum untuk berbagai cyber security, termasuk dengan pemanfaatan dan penghubungan, tetapi tidak sampai menggantikan, standar dan pedoman yang diakui secara global.

   Penghubungan CSF dengan jelas ke framework NIST lainnya. framework terkait cyber security dan modul NIST lainnya, masing-masing akan tetap menjadi framework terpisah. Masing-masing berfokus pada topik tertentu dan memiliki kebutuhan khusus. Namun, seperti yang ditunjukkan oleh NIST, bahwa setiap framework memiliki hubungan dengan CSF, sehingga akan dirujuk sebagai pedoman baik dalam CSF 2.0 maupun dalam materi pendamping.

   Pemanfaatan cyber security dan tools untuk CSF 2.0 core secara online. Menawarkan format yang dapat dibaca mesin dan interface user yang konsisten untuk mengakses data referensi dari standar, panduan, dan framework cybersecurity dan privasi NIST, serta pendekatan yang fleksibel untuk mengkarakterisasi hubungan antara standar, panduan, dan framework, serta berbagai aplikasi dan teknologi.

   Menggunakan Referensi Informatif online yang dapat diupdate. Meskipun konsep referensi informatif telah diterima dengan baik, beberapa Referensi Informatif CSF menjadi ketinggalan zaman ketika dokumen sumber tersebut diperbarui. Selain itu, kolom Referensi Informatif di CSF 1.1 hanya mewakili sebagian kecil contoh standar yang dapat dimanfaatkan oleh organisasi dalam menggunakan CSF.

   Gunakan Referensi Informatif untuk memberikan lebih banyak panduan dalam mengimplementasikan CSF. NIST akan bekerja sama dengan komunitas untuk mendorong dan memungkinkan produksi pemetaan yang mendukung CSF 2.0. Terdapat minat yang kuat dari komunitas terhadap pemetaan tambahan; responden RFI meminta pemetaan terhadap hampir 50 standar keamanan cyber, pedoman, dan kerangka kerja lainnya, yang banyak di antaranya dibuat oleh organisasi lain.

   Tetap netral terhadap teknologi dan vendor, tetapi mencerminkan perubahan dalam praktik keamanan cyber. CSF 2.0 akan tetap netral terhadap teknologi dan vendor. NIST mengakui bahwa lansekap 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 tanpa memandang teknologi atau layanan yang mereka gunakan, termasuk TI, IoT, OT, dan layanan cloud.

3. CSF 2.0 (dan sebagainya) akan menyediakan update dan perluasan guide pada implementasi Framework.

   Terdapat lebih dari 500 referensi dalam tanggapan RFI yang mendukung perlunya lebih banyak panduan untuk mendukung implementasi CSF, dan banyak pengguna menyatakan keinginan untuk CSF dengan tetap mempertahankan pendekatan yang tidak bersifat preskriptif. Permintaan akan panduan tambahan untuk membantu organisasi ketika mereka mempertimbangkan dan menggunakan CSF berasal dari berbagai macam organisasi yang memiliki kebutuhan dan risiko yang sangat berbeda.

   Menambahkan contoh implementasi untuk Subkategori CSF. CSF 2.0 akan menyertakan contoh implementasi gagasan tentang proses dan kegiatan yang ringkas dan berorientasi pada tindakan dan kegiatan untuk membantu mencapai hasil dari Subkategori CSF, selain panduan yang disediakan dalam Referensi Informatif CSF.

   Pengembangan template Profil CSF. Banyak tanggapan RFI yang meminta panduan tambahan, termasuk template bagi organisasi untuk mengembangkan Profil CSF. Framework Profile adalah cara organisasi mengimplementasikan CSF dengan menyelaraskan Fungsi, Kategori, dan Subkategori CSF dengan persyaratan misi, toleransi risiko, dan sumber daya organisasi. Profile juga menggabungkan dan menyelaraskan referensi informatif yang relevan untuk Subkategori, termasuk standar dan panduan sektoral serta persyaratan hukum dan peraturan.

   Memperbaiki situs web CSF untuk menampilkan referensi implementasi. Situs web NIST CSF berisi banyak informasi dan panduan tambahan tentang mengimplementasikan CSF. Ini termasuk berbagai materi yang dikembangkan oleh NIST dan organisasi eksternal, termasuk contoh CSF Profile, pemetaan, panduan, alat bantu, studi kasus, kisah sukses, publikasi terkait (seperti Panduan Awal 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 pada pentingnya tata kelola cyber security.

   Tata kelola cybersecurity saat ini dibahas dalam CSF 1.1 di Fungsi "Identifikasi", serta di bagian "Cara Menggunakan Framework". CSF 2.0 akan memperluas pertimbangan ini topik-topik ini.

   Menambahkan Fungsi Kelola yang baru. Sebagai cerminan dari masukan substansial kepada NIST, CSF 2.0 akan menyertakan Fungsi " Govern " yang baru untuk menekankan hasil tata kelola manajemen risiko keamanan siber. Meskipun kelima Fungsi CSF telah diadopsi secara 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.

Meningkatkan pembahasan mengenai hubungan dengan manajemen risiko. Merevisi CSF menawarkan kesempatan untuk memperjelas hubungan antara pengelolaan dan manajemen risiko cyber security di seluruh bagian 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, mitigasi, transfer, hindari), dan berbagai contoh proses manajemen risiko (misalnya, Kerangka Kerja Manajemen Risiko, ISO 31000) yang dapat digunakan untuk mendukung implementasi CSF.

5. CSF 2.0 akan menekankan pada pentingnya supply chain risk management (C-SCRM).

   Memperluas cakupan supply chain. Responden RFI setuju bahwa risiko keamanan cyber dalam supply chain 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, namun mereka memiliki pendapat yang beragam tentang bagaimana masalah ini harus ditangani dalam pembaruan CSF. 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.

6. CSF 2.0 akan memberikan pemahaman mengenai pengukuran dan penilaian cyber security.

   Pengukuran dan penilaian program dan strategi manajemen risiko cyber terus menjadi area penting dalam penggunaan CSF. Tanggapan RFI menunjukkan bahwa responden mencari panduan dan sumber daya CSF tambahan untuk mendukung pengukuran dan penilaian penggunaan CSF oleh organisasi. Keinginan terkait adalah agar CSF menjelaskan dengan jelas bagaimana organisasi dapat menggunakan Implementation Tiers, dan bagaimana hubungannya dengan pengukuran.

   Memperjelas bagaimana memanfaatkan CSF dapat mendukung pengukuran dan penilaian program cyber security. CSF 2.0 akan memperjelas bahwa dengan memanfaatkan CSF, organisasi memiliki taxonomy dan lexicon yang sama untuk mengkomunikasikan hasil dari upaya pengukuran dan penilaian, terlepas dari proses manajemen risiko yang mendasarinya. Di semua organisasi, tujuan utama pengukuran dan penilaian cyber security adalah untuk menentukan seberapa baik mereka mengelola risiko keamanan siber, dan jika dan bagaimana mereka terus meningkatkannya.

   Memberikan contoh pengukuran dan penilaian dengan menggunakan CSF. Risiko, prioritas, dan sistem setiap organisasi, sehingga metode dan tindakan yang digunakan untuk mencapai hasil yang dijelaskan oleh Framework Core 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 melanjutkan fleksibilitas dalam bagaimana organisasi dapat mengimplementasikan Framework.

Memperbarui panduan pengukuran kinerja NIST untuk Information Security. NIST memperbarui dokumen panduan pengukuran andalannya, panduan pengukuran kinerja untuk keamanan informasi.

Memberikan panduan tambahan tentang Tingkatan Implementasi Framework. Tingkatan CSF menyediakan mekanisme bagi organisasi untuk melihat dan memahami pendekatan mereka terhadap risiko cyber security serta proses dan program yang ada untuk mengelola risiko tersebut. Tingkatan tersebut memiliki tingkat ketelitian dan kecanggihan yang semakin meningkat dalam menggambarkan praktik manajemen risiko cyber security secara keseluruhan, termasuk proses manajemen risiko, integrasi program manajemen risiko, dan partisipasi aktif dalam ekosistem cyber security yang lebih luas.