Action List for Developing a CSIRT

1. **Identify stakeholders and participants.**
   a. Tentukan siapa saja yang perlu dilibatkan pada tiap tahap mulai dari perencanaan, implementasi, dan operasional CSIRT.
   b. Tentukan siapa yang akan dilayani atau didukung oleh CSIRT.
   c. Tentukan dengan siapa saja akan berkoordinasi atau berbagi informasi.
   d. Tentukan siapa yang akan melakukan fungsi keamanan atau insiden respon.
   e. Tentukan pihak internal dan eksternal yang mungkin berinteraksi atau berpartisipasi dalam CSIRT.

2. **Obtain management support and sponsorship.**
   a. Tentukan siapa saja dari eksekutif manajer/direktur yang akan mensponsori/mendukung pembentukan CSIRT.

3. **Identify the CSIRT constituency.**
   a. Tentukan initial group baik dari individu atau organisasi yang akan dilayani dan didukung CSIRT.
   b. Tentukan jenis layanan apa saja yang akan disediakan CSIRT kepada segmen yang berbeda dari konstituen yang ada.
   c. Tentukan dan tetapkan mitra strategis, jika ada.
   d. Tentukan bagaimana anggota konstituen bisa mendapatkan layanan dari CSIRT.

4. **Define the CSIRT mission.**
   a. Tentukan misi CSIRT. Pernyataan misi (mission statement) harus memberikan nilai baik untuk konstituensi maupun induk organisasi.
   b. Tentukan *primary goals* dan *objectives* dari CSIRT.

5. **Secure funding for CSIRT operations.**
   a. Tentukan darimana mendapatkan pendanaan baik untuk start-up, operasional jangka pendek dan jangka panjang.
   b. Tentukan model pendanaan yang akan digunakan untuk mendukung CSIRT (fee-for-service, langganan keanggotaan, sponsor pemerintah, atau budget line dari organisasi induk).

6. **Decide on the range and level of services the CSIRT will offer.**
   a. Tentukan layanan yang akan disediakan CSIRT dan kepada bagian mana saja dari konstituen.
   b. Tentukan proses untuk pemberian layanan (jam operasi, metode kontak, metode untuk penyebaran informasi, dan proses terkait).
   c. Tentukan bagaimana CSIRT akan memasarkan/mensosialisasikan layanannya.

7. **Determine the CSIRT reporting structure, authority, and organizational model.**
   a. Tentukan posisi CSIRT yang cocok dalam struktur organisasi.
   b. Buat bagan struktur organisasi.

8. **Identify required resources such as staff, equipment, and infrastructure.**

a. Tentukan bagaimana infrastruktur CSIRT akan disediakan, dilindungi, dijamin, dan dipantau, terutama tempat fisik dan repositori data.
b. Tentukan proses untuk mengumpulkan, menyimpan, melacak, dan mengarsip informasi.
c. Buat job description yang menyebutkan daftar pengetahuan, ketrampilan, dan kemampuan yang diperlukan untuk setiap posisi dalam CSIRT.
d. Tentukan persyaratan untuk background checks, sertifikasi, atau security clearances yang sesuai.

9. Define interactions and interfaces.

a. Identifikasi interaksi dan hubungan dengan bagian-bagian kunci dari konstituen, stakeholder, dan dengan mitra internal atau eksternal, kolaborator, atau kontraktor.
b. Tentukan entitas lain yang akan berkoordinasi dengan CSIRT.
c. Identifikasi bagaimana alur informasi antar entitas.
d. Tentukan dan tetapkan interaksi dan metode kolaborasi dan komunikasi dengan pihak lain secara tepat, termasuk penegak hukum, vendor, komponen critical infrastructure, ISP, kelompok keamanan lainnya, dan CSIRT lainnya.
e. Tentukan metode untuk menyebarkan informasi kepada konstituen dan stakeholder yang relevan.

10. Define roles, responsibilities, and the corresponding authority.

a. Tentukan peran (*role*) dan tanggung jawab untuk setiap fungsi CSIRT.
b. Tenentukan interaksi antar fungsi CSIRT dan fungsi eksternal lainnya.
c. Identifikasi area2 dimana otoritas/kewenangan yang mungkin ambigu atau saling tumpang tindih, dan definisikan fungsi dan peran antar kelompok.

11. Document the workflow.

a. Buat diagram (swimlane chart, flowchart,etc.) untuk mendokumentasikan proses CSIRT dan interaksi yang sesuai, termasuk siapa yang melakukan pekerjaan dan di mana dalam proses interaksi.

12. Develop policies and corresponding procedures.

a. Tentukan kriteria kategori, prioritas, dan eskalasi insiden terkait.
b. Identifikasi kebijakan dan prosedur awal yang perlu diformalkan sebelum operasional, dan apa saja yang akan dibuat setelah CSIRT sudah mulai operasional.
c. Tentukan dan dokumentasikan kriteria/prosedur dalam memberikan layanan CSIRT untuk menjamin proses yang konsisten, reliable, dan repeatable dapat diikuti oleh seluruh staff.

13. Define methods for evaluating the performance of the CSIRT.

a. Tentukan baselines sebagai patokan untuk melakukan pelaporan dan penanganan insiden dalam organisasi sebelum CSIRT diimplementasikan. Gunakan baseline tersebut untuk mengukur performance pada saat CSIRT sudah operasional.
b. Tentukan kriteria pengukuran dan parameter jaminan kualitas sehingga performance CSIRT dapat diukur dengan cara yang konsisten.
c. Tentukan metode untuk memperoleh umpan balik dari konstituen.