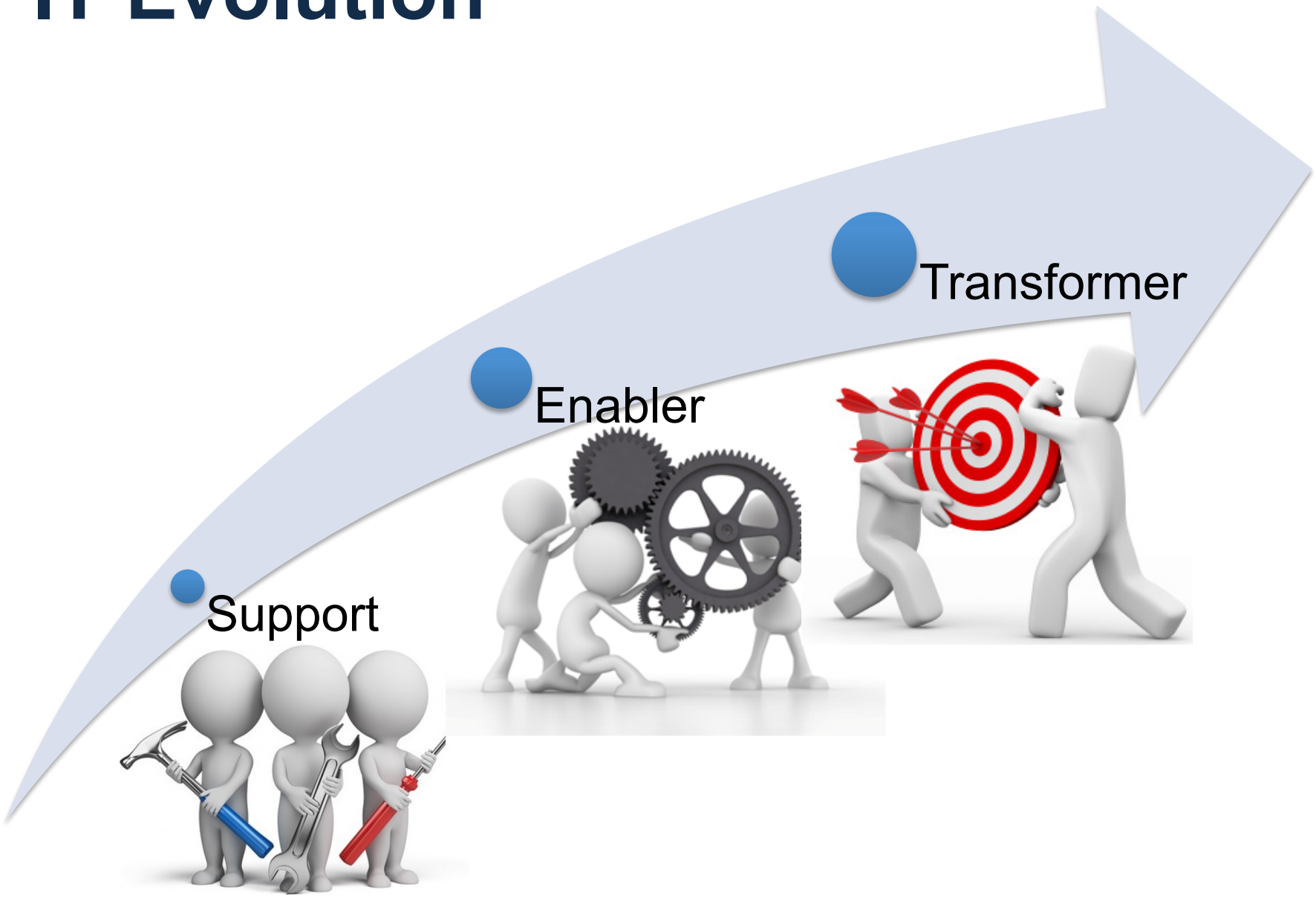
PEMBENTUKAN CSIRT

BADAN SIBER &
SANDI NEGARA

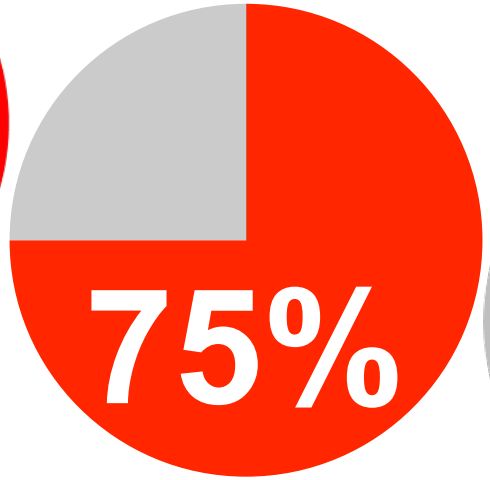
IT Evolution



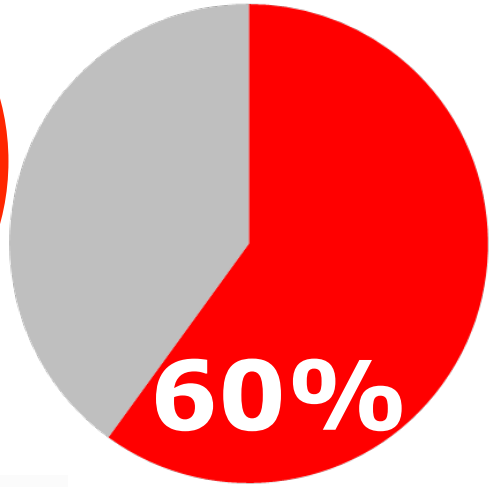
Security Incidents

Target of all successful APT attacks is a user (Mandiant)

Exploits need a user interaction (Symantec)



Human factor



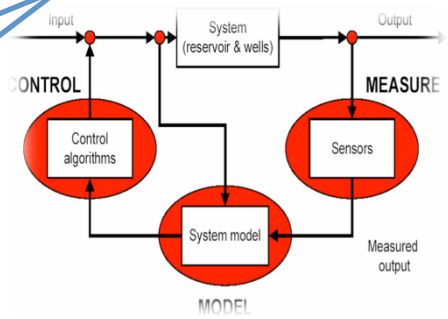
Accidental mistakes (InfoWatch)

The weakest link in security is human!

Who use or interact with the Information

People

Process



The repeatable steps to accomplish business objectives

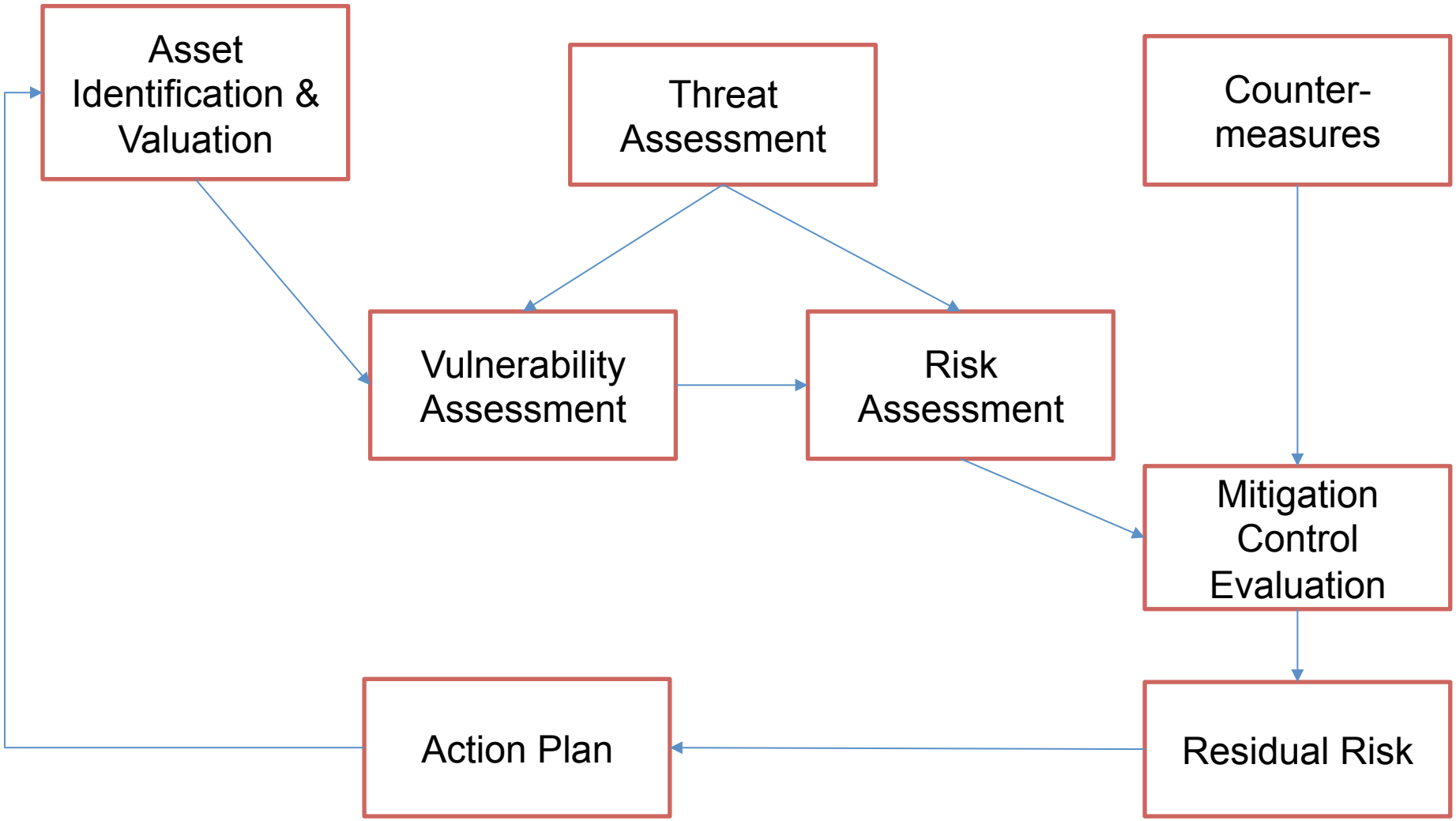
Technology

what we use to improve what we do

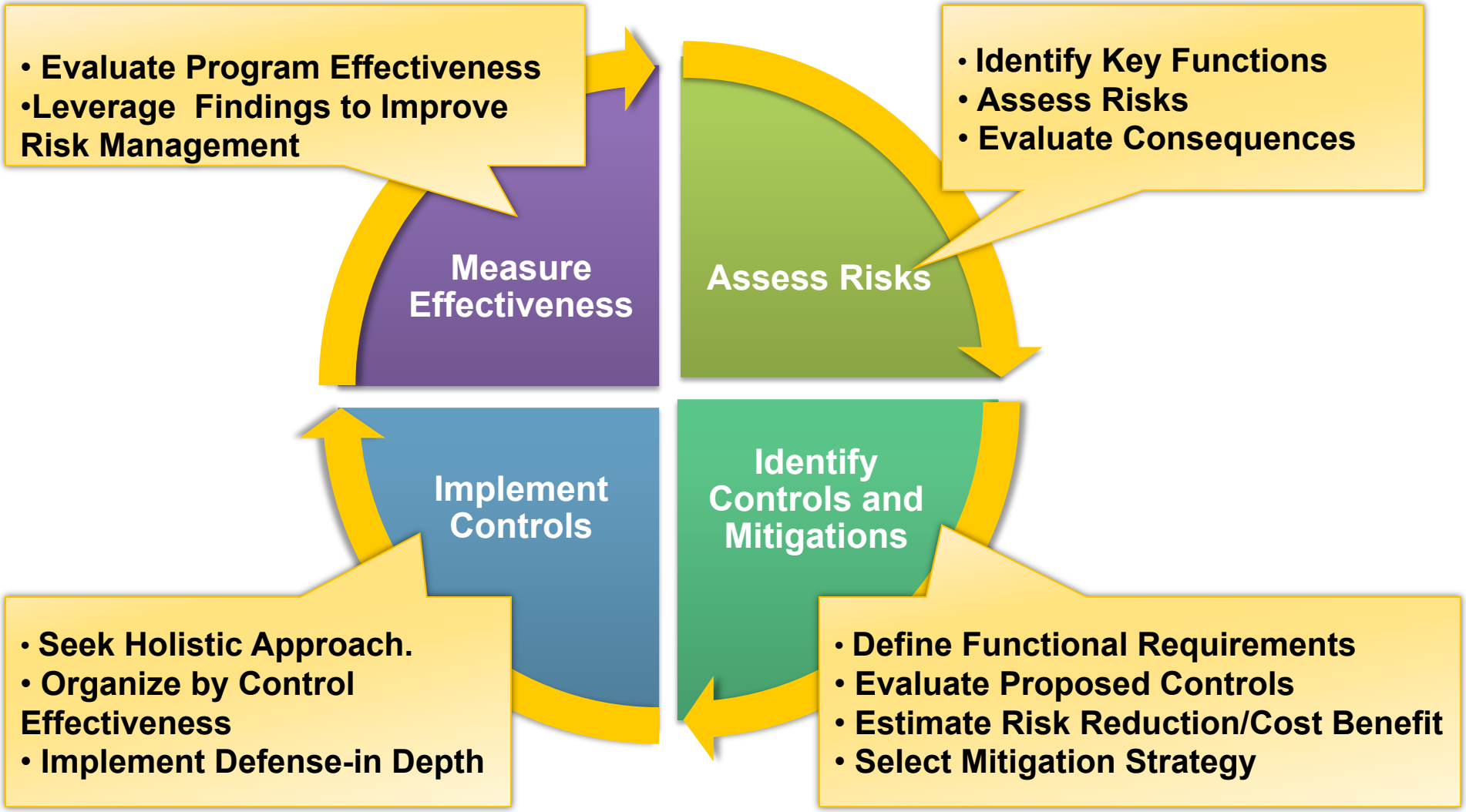

Technology
We can't deploy technology without competent people and support processes
Process
* Management
* Governance
* Best Practice
* Audit & Control
People
* Staff Training & Awareness
* Professional Skills & Qualifications
* Competent Resources


RISK
RISK

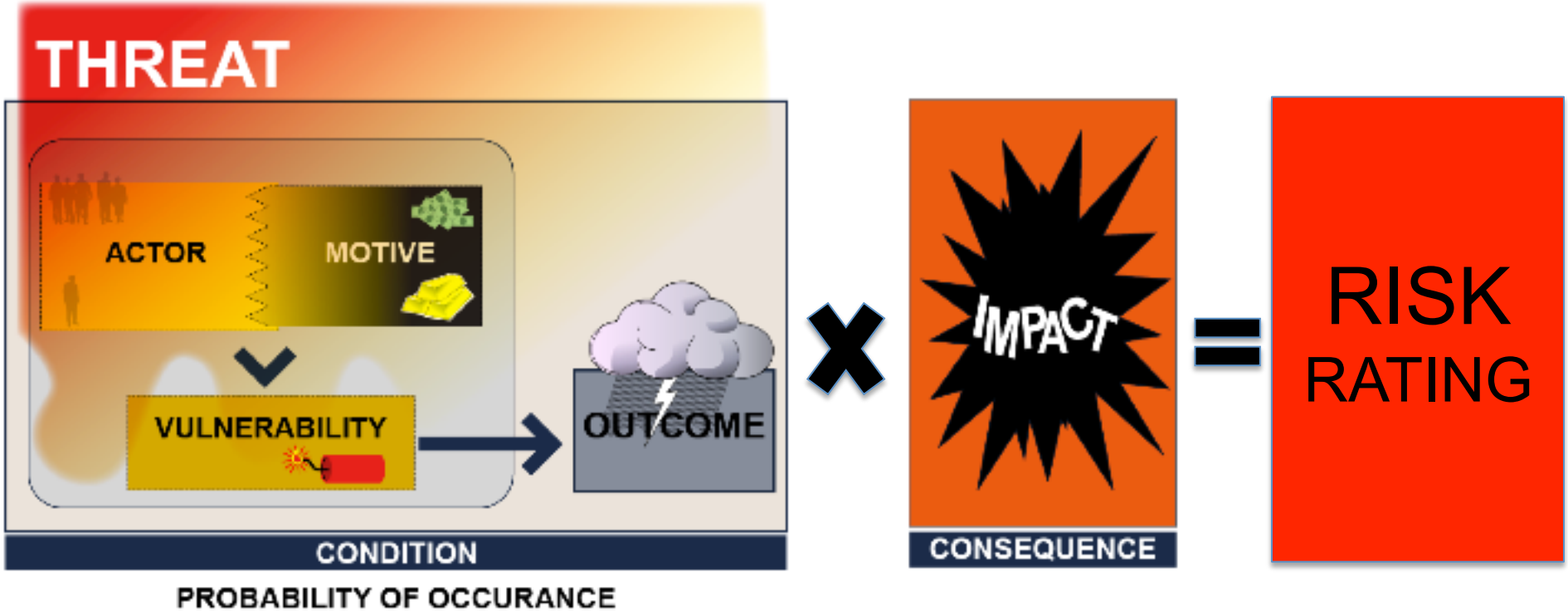
Risk Management Framework



Continuously Assess and Manage Risks



RISK RATING


THREAT
ACTOR
MOTIVE
VULNERABILITY
OUTCOME
CONDITION
PROBABILITY OF OCCURANCE
IMPACT
CONSEQUENCE
RISK
RATING

RISK RATING MATRIX

RISK LIKELIHOOD	RISK IMPACT		
	LOW (10)	MODERATE (50)	HIGH (100)
HIGH (1,0)	Low 10 x 1,0 = 10	Moderate 50 x 1,0 = 50	High 100 x 1,0 = 100
MODERATE (0,5)	Low 10 x 0,5 = 5	Moderate 50 x 0,5 = 25	Moderate 100 x 0,5 = 50
LOW (0,1)	Low 10 x 0,1 = 1	Low 50 x 0,1 = 5	Low 100 x 0,1 = 10

Risk Scale: Low (1 to 10); Moderate (>10 to 50); High (>50 to 100)

Qualitative Risk Assessment

For a given scope of assets, identify:

- Vulnerabilities
- Threats
- Threat probability (Low / medium / high)
- Impact (Low / medium / high)
- Countermeasures

Quantitative Risk

	Formula	Description
Asset value (AV)	AV	Value of the asset
Exposure factor (EF)	EF	Percentage of asset value lost
Single-loss expectancy (SLE)	AV × EF	Cost of one loss
Annual rate of occurrence (ARO)	ARO	Number of losses per year
Annualized loss expectancy (ALE)	SLE × ARO	Cost of losses per year


CSIRT

RENCANA STRATEGIS

- Definisi CSIRT
  - Role/Responsible
  - Menentukan Stakeholder
- Establishment
  - Dokumentasi
- Scope
- Organisasi dan Sumberdaya

1. Stakeholder

Semua stakeholder akan memainkan peran yang berbeda dalam pembentukan, pengembangan, dan pengoperasian CSIRT. Dapat dikelompokkan secara berdasarkan kontribusinya:

Sponsors or promoters

Orang atau organisasi yang mempromosikan keberadaan CSIRT, dan akan mendukungnya baik secara politik maupun finansial.

Clients

Organisasi yang akan menggunakan layanan CSIRT.

Providers

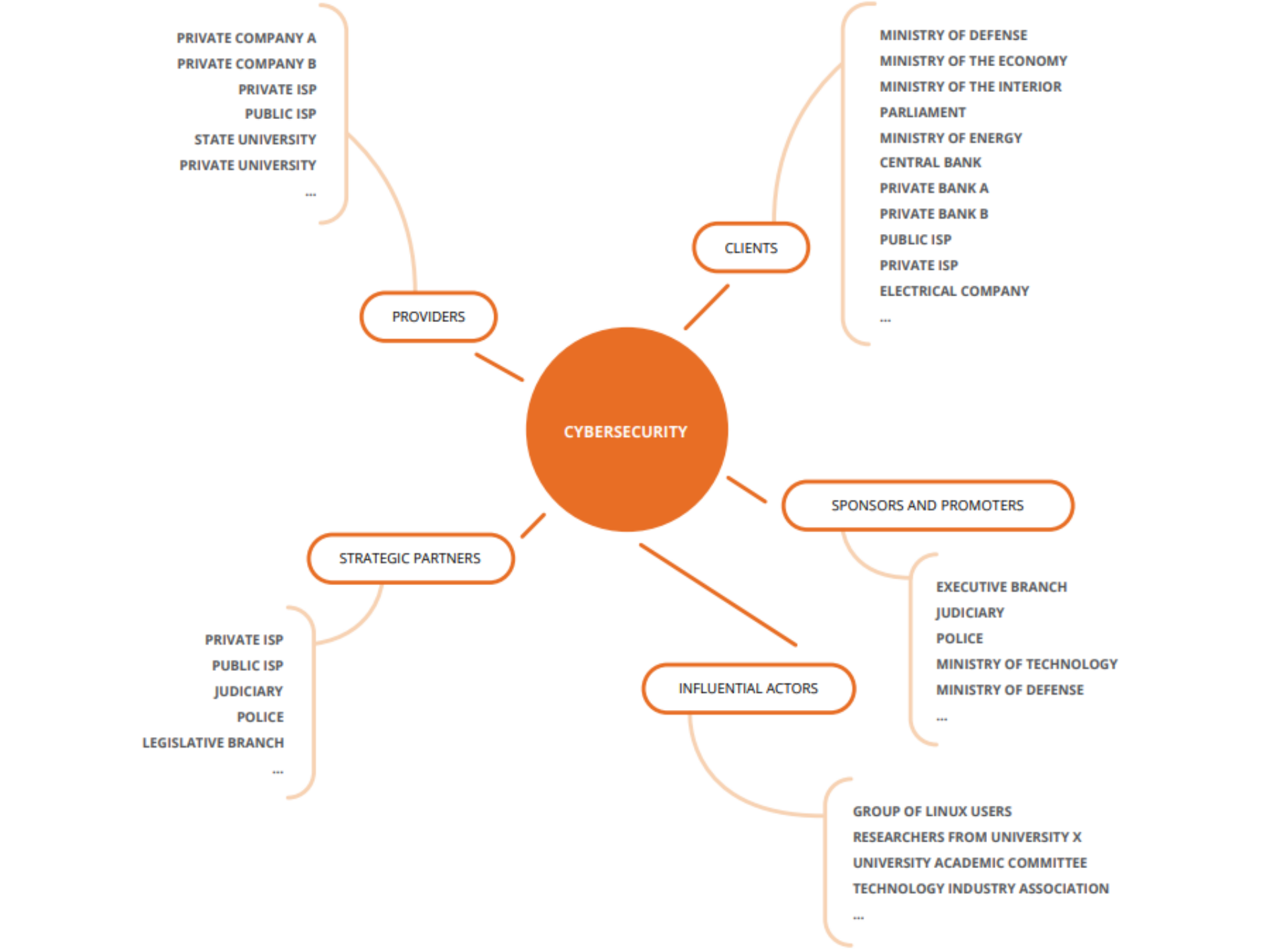
Organisasi yang menyediakan produk dan / atau layanan kepada CSIRT, seperti alat, layanan profesional, pelatihan, dll.

Strategic Partners

Individu atau organisasi yang strategis untuk pengembangan CSIRT. Secara umum, mitra ini menjalankan aktivitas yang menarik bagi CSIRT yang tidak dapat dilakukannya sendiri. Contohnya mungkin akademisi atau regulator khusus sektor.

Influential

Individu atau organisasi yang secara informal memengaruhi berbagai sektor.


CYBERSECURITY
PROVIDERS
PRIVATE COMPANY A
PRIVATE COMPANY B
PRIVATE ISP
PUBLIC ISP
STATE UNIVERSITY
PRIVATE UNIVERSITY
...
CLIENTS
MINISTRY OF DEFENSE
MINISTRY OF THE ECONOMY
MINISTRY OF THE INTERIOR
PARLIAMENT
MINISTRY OF ENERGY
CENTRAL BANK
PRIVATE BANK A
PRIVATE BANK B
PUBLIC ISP
PRIVATE ISP
ELECTRICAL COMPANY
...
SPONSORS AND PROMOTERS
EXECUTIVE BRANCH
JUDICIARY
POLICE
MINISTRY OF TECHNOLOGY
MINISTRY OF DEFENSE
...
STRATEGIC PARTNERS
PRIVATE ISP
PUBLIC ISP
JUDICIARY
POLICE
LEGISLATIVE BRANCH
...
INFLUENTIAL ACTORS
GROUP OF LINUX USERS
RESEARCHERS FROM UNIVERSITY X
UNIVERSITY ACADEMIC COMMITTEE
TECHNOLOGY INDUSTRY ASSOCIATION
...

Interview Stakeholder

- Apakah Anda merasa perlu membuat CSIRT? Mengapa?
- Bagaimana seharusnya peran CSIRT?
- Layanan apa yang harus disediakan CSIRT?
- Apakah ada bagian tertentu dari pemerintah di mana CSIRT harus ditempatkan?
- Apa manfaat CSIRT bagi organisasi Anda?
- Bagaimana mungkin bekerja dengan CSIRT sulit bagi organisasi Anda?
- Apakah hubungan tersebut diatur oleh kontrak, NDA, SLA, atau cara lain?
- Apakah organisasi Anda bersedia bekerja sama secara aktif dengan CSIRT?
- Apa batasan untuk kerja sama?
- Menurut Anda, organisasi atau individu apa yang harus


INFLUENCE
HIGH INFLUENCE
LOW INFLUENCE
Keep them satisfied
Stakeholders must simply be kept satisfied. As they don't have much interest in the project, they can become easily overburdened if given too much information or tasks to complete. The CSIRT project team cannot demand too much of this group.
Manage them closely
Stakeholders with high levels of both interest and influence need to be kept abreast of all developments and must be continuously engaged. Even if this stakeholder has a negative view of the project, it should be managed closely owing to its ability to impede the work of the CSIRT.
Only monitor them
Stakeholders who have little interest and little influence on the project must only be monitored. There is not a lot to gain or lose from this group, whether positive or negative.
Keep them informed
Stakeholders who have high interest in the project but low capacity to influence must be kept informed. At the same time, avoid giving them critical responsibilities because they have no power to influence materially. Nevertheless, they are reliable allies.
INTEREST
LOW INTEREST
HIGH INTEREST

2. Establishment

- Visi Misi
- Institutional Framework
- Legal Framework

Visi Misi

- WHAT

Menggambarkan apa yang dilakukan tim, biasanya menggunakan istilah seperti mengoordinasikan, mempromosikan regulasi, memimpin upaya, melindungi, mencegah, atau mengartikulasikan kegiatan seperti respon insiden, keamanan cyber, sistem informasi atau aset, dll.

- WHOM

Menggambarkan untuk siapa kegiatan dilakukan, istilah yang sering digunakan adalah negara, pemerintah, sektor, masyarakat, atau lainnya.

- VALUES

Mengenai nilai-nilai yang menggerakkan misi, motifnya harus dinyatakan dengan jelas, misalnya dengan menggunakan istilah : pengembangan, kesejahteraan, keselamatan, atau manajemen risiko, keamanan, kepercayaan, atau tanggung

Institutional Framework

Framework kelembagaan CSIRT adalah kunci untuk pembentukan dan fungsinya di sepanjang siklus hidupnya. Framework kelembagaan menjadi pedoman untuk pertimbangan berikut :

- Tanggung jawab
- Wewenang
- Interaksi dengan para pemangku kepentingan
- Sumber keuangan
- Sumber daya manusia
- Infrastruktur
- Resillience

Legal Framework

Sangat penting untuk mendefinisikan otoritas hukum di mana CSIRT akan dibentuk. Sangat penting bahwa misi, visi, dan kerangka kerja kelembagaan dinilai oleh para ahli hukum, baik dari pemerintah atau akademisi atau praktisi, secara khusus untuk menjawab pertanyaan-pertanyaan berikut:

- Apakah CSIRT dapat diterima dari sudut pandang hukum?
- Apakah ini bertentangan dengan hukum apa pun, atau mengizinkan celah apa pun yang eksploitasinya mungkin berdampak negatif pada tim respons dan tugasnya?
- Instrumen apa yang akan digunakan untuk kerangka kelembagaan?
- Legislasi, keputusan, atau resolusi?
- Bisakah CSIRT menggunakan tindakan hukum apa pun untuk menjamin pendanaan?

3. Scope

- Target Komunitas
- Lingkup Service

Full Authority

The CSIRT has authority to carry out all necessary actions relating to the management of an incident, and community members are required to implement the measures proposed by the CSIRT or, at most, allow members of the CSIRT to implement them.

Shared Authority

The decision regarding an incident is made jointly between members of the affected community and the CSIRT. The CSIRT supports the actors involved in an incident and collaborates with equipment and expertise.

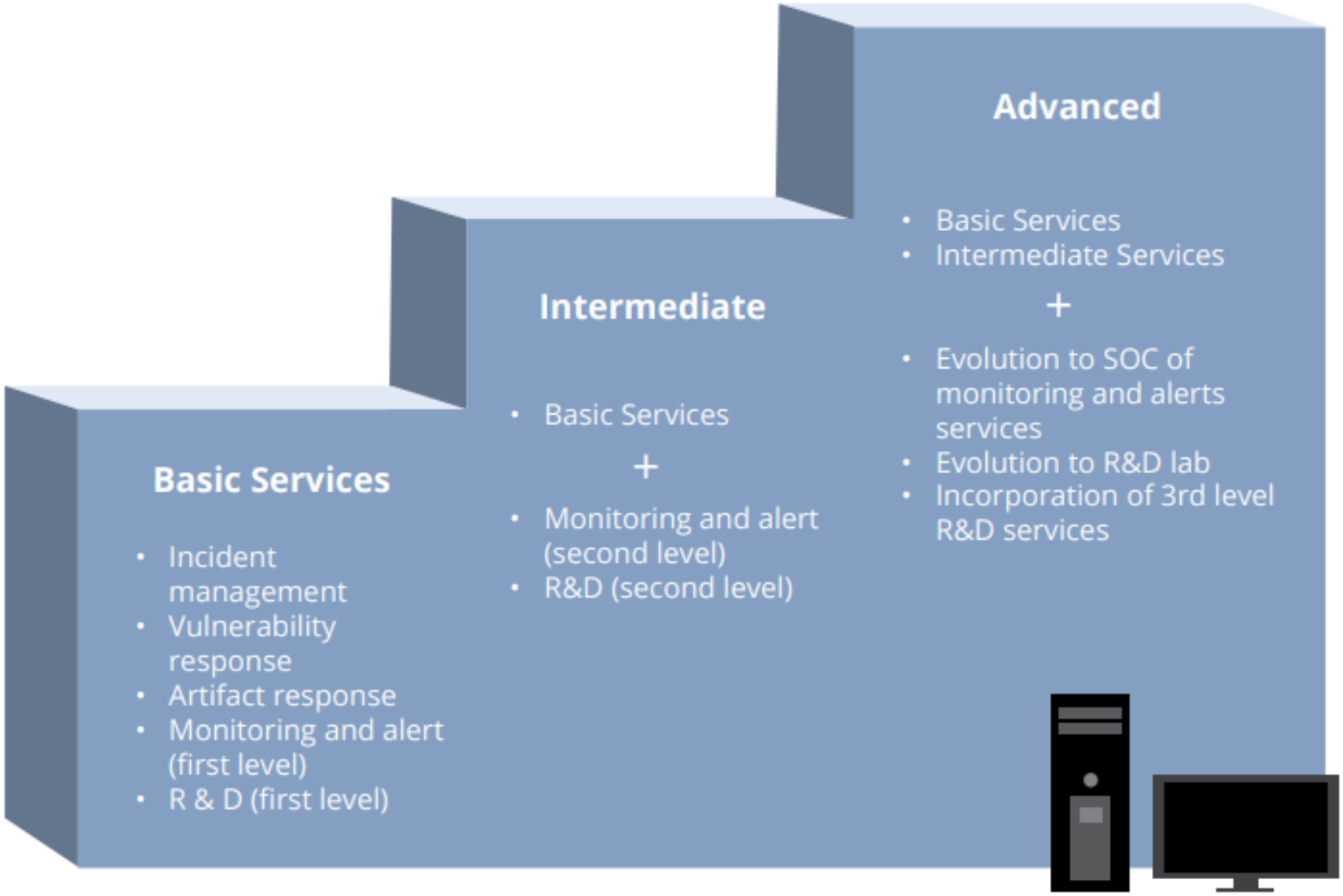
Null Authority

The CSIRT has no authority over decisions regarding incidents. It provides advice, information and experience, but decisions are taken by those affected.

Indirect Authority

The CSIRT has no authority over the community, however it can exert indirect pressure on it-- for example, through regulators or other organizations with which the CSIRT has established bonds of trust.

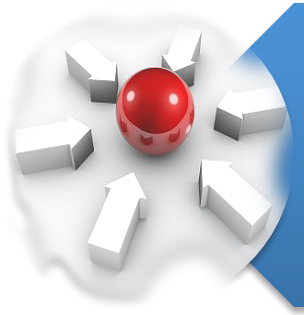
Lingkup Service



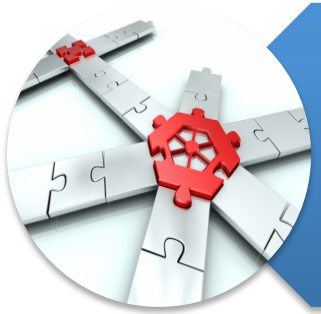
Organisasi dan Sumberdaya

- Organizational Structure
- Organization Size
- Roles and Responsibilities
- Kebutuhan Sumberdaya

Team Structure Model



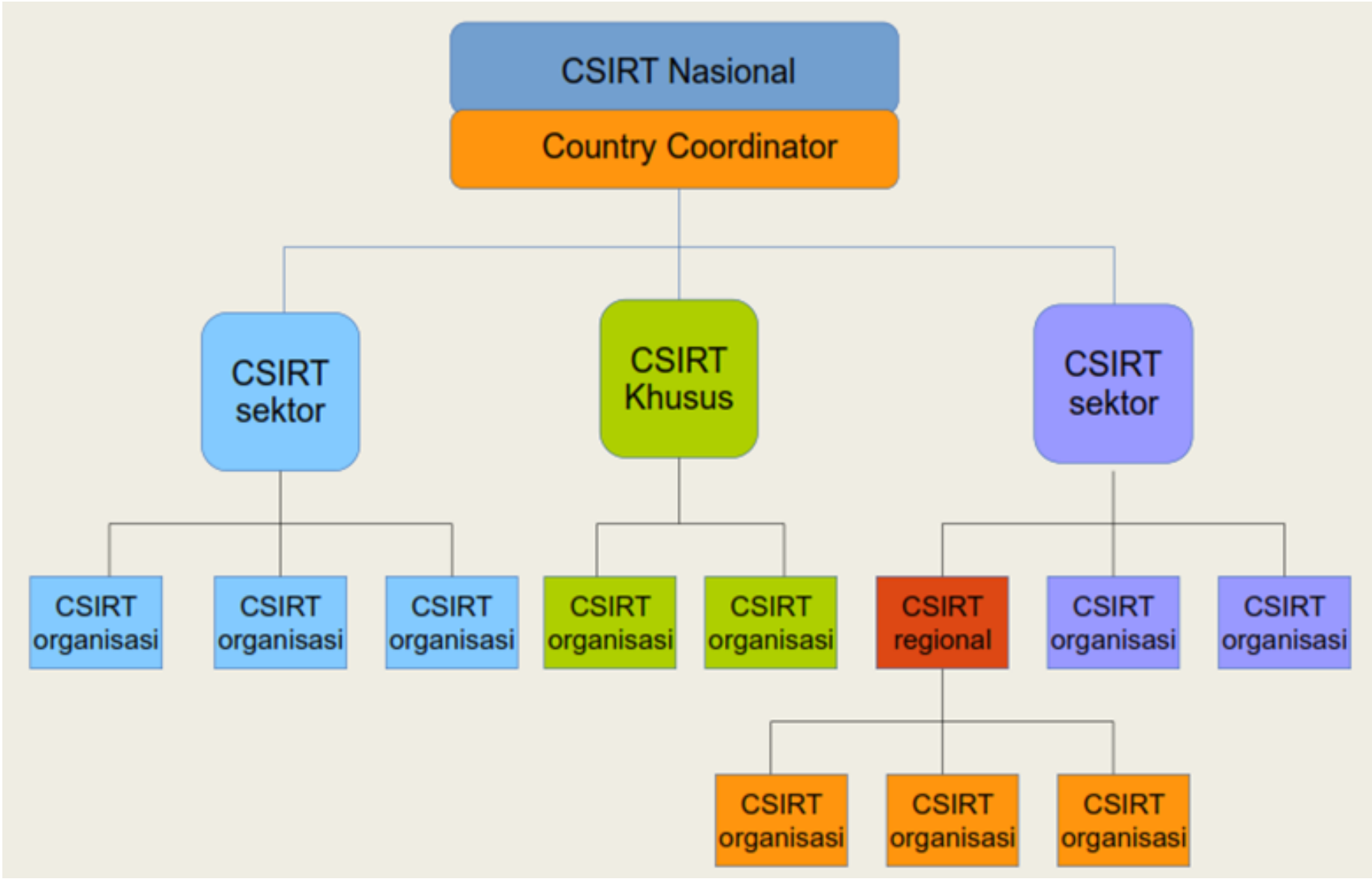
Central Incident Response Team



Distributed Incident Response Team

Coordinating Team

Struktur CSIRT



IMPLEMENTASI

- SDM
- Training
- Fasilitas dan Infrastruktur
- Operational Policies and Procedures

Incident Response Policy

- Dukungan Pimpinan/Manajemen
- Ruang lingkup dan tujuan dari Respons Insiden
- Mengarahkan Organisasi tim, metode komunikasi, dan bagaimana tim berinteraksi dengan organisasi internal dan eksternal
- Menetapkan apa insiden, dan bagaimana Incident Response Plan and Procedures digunakan
- Persyaratan validasi untuk memastikan kepatuhan dengan semua persyaratan organisasi dan regulasi

Incident Response Procedure

- Menjabarkan proses teknis selama investigasi
- Bagian yang paling rinci dan komprehensif dari program Respon Insiden dengan tujuan untuk membangun pendekatan yang sistematis dan konsisten untuk setiap insiden.
- Bisa dalam bentuk check list, atau formulir atau menguraikan rincian tentang cara memeriksa ancaman tertentu dan mengumpulkan data log atau bukti untuk keperluan analisis

Typical IR Procedures

- Komunikasi - baik internal maupun eksternal
- Pemberitahuan Eskalasi
- Formulir Pelacakan Insiden
- Pelaporan dan Dokumentasi Insiden
- Daftar Pemeriksaan Investigasi
- Daftar Periksa Remediasi berdasarkan klasifikasi Risiko dan Ancaman
- Koleksi Bukti dan Penanganan “Chain of Custody”
- Investigasi dan Dokumentasi Forensik
- Retensi dan Penghancuran Data
- Perjanjian Non-Disclosure


Incident
Handling
Checklist

	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

Tugas POC

- Menerima dan menanggapi laporan insiden keamanan siber
- Menerima dukungan dan saran dalam menanggapi dan memitigasi insiden siber
- Memonitor insiden keamanan atau serangan siber
- Memberikan saran dan peringatan kepada stakeholder dan konstituen untuk meningkatkan ketahanan keamanan siber
- Sebagai kontak terpercaya (*trusted*) untuk *sharing information*