FIRST CSIRT Framework Development SIG:

The CSIRT Services Framework

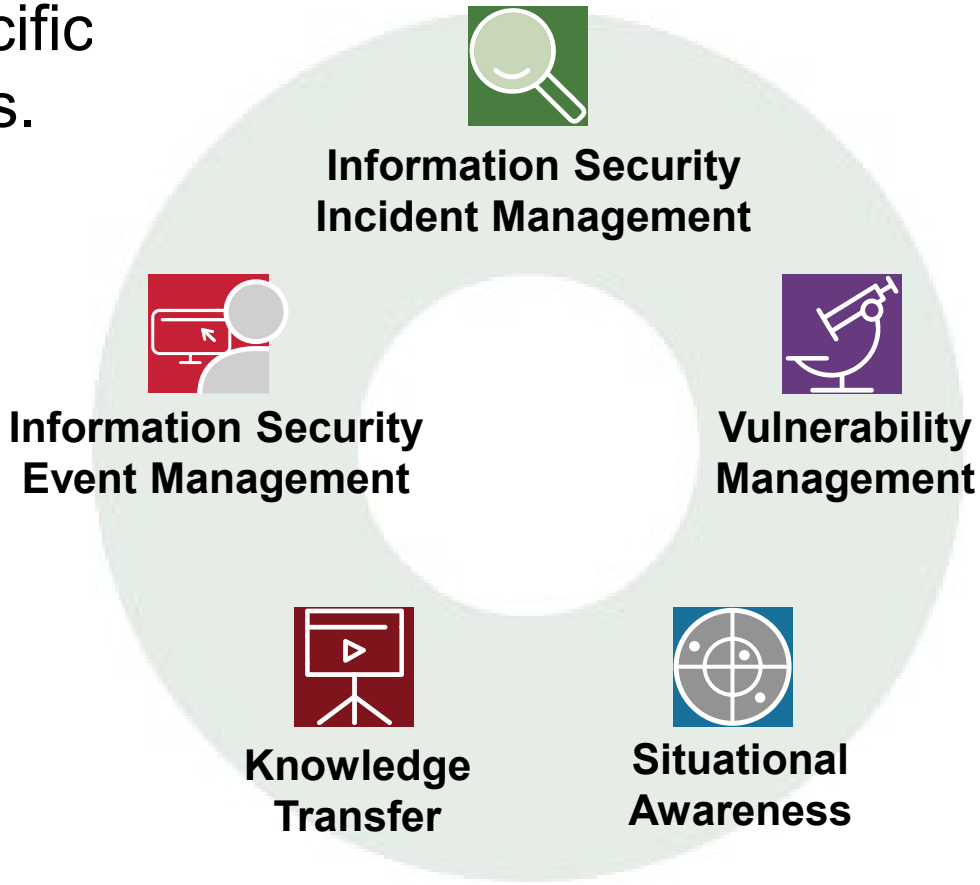
Prof. Dr. Klaus-Peter Kossakowski (Chair)
HAW Hamburg, Germany

Maturity

How effectively an organization executes a particular capability within the mission and authorities of the organization. It is a level of proficiency attained either in executing specific functions or in an aggregate of functions or services.

The ability of an organization will be determined by the extent and quality of established policies and documentation and the ability to execute a set process.

Service Frameworks allow us to improve each team‘s maturity!



FIRST CSIRT Framework Development SIG:

The CSIRT Services Framework ... and defining CSIRT Roles

Prof. Dr. Klaus-Peter Kossakowski (Chair)
HAW Hamburg, Germany

Maturity, but Capacity and Capabilities first

Capability - A measurable activity that may be performed as part of an organization's roles and responsibilities. For the purposes of the FIRST services framework, the capabilities can either be defined as the broader services or as the requisite functions.

Capacity - The number of simultaneous process-occurrences of a particular capability that an organization can execute before they achieve some form of resource exhaustion.

Each Role is defined as ...

A combination of references to mostly other documents. By referencing the content we can deliver a „lean“ document taking advantage of other resources (instead of reinventing the wheel!)

- **Description –** setting the context of the role within the service
- **General Tasks –** list general tasks to be carried out by it
- **Associated Functions** from the CSIRT Services Framework (v2.1)
- **Generic Competencies –** like „communication“ or „problem solving“
- **Role-specific Competencies –** like „threat analysis“ etc.

→ https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Roles_and_Competencies_v_0.9.0.pdf

Defining Roles for all Functions

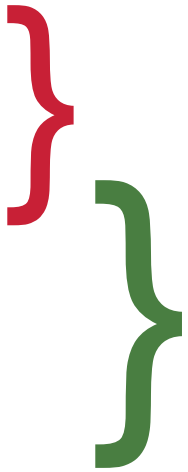
An addendum for CSIRTs (version 0.9 for review is out, final draft expected for IV/2023) is based on competencies for those carrying out the specific (service) functions!

Multiple roles are required, which can be mapped on the available staff members in various ways, which are beyond this addendum!

- **Use Case Manager**
- **Data Manager**

- **Incident Analyst**
- **Incident Triage Coordinator**

- **Incident Responder**
- **Malware / Forensic Analyst**



SERVICE AREA
Information Security
Event Management

SERVICE AREA
Information Security Incident
Management

FIRST CSIRT Framework Development SIG:

The CSIRT Services Framework
... and defining CSIRT Roles
... and defining SIM Team Types

Prof. Dr. Klaus-Peter Kossakowski (Chair)
HAW Hamburg, Germany

Services Framework apply to different team types

- **No attempt to build specific team types into it:**
  Service offerings can be described using the same service names!
  But teams might choose different service levels or attributes, and indeed package those services in – even unusual – ways.
- **No attempt to synchronize (yet) with other services frameworks:**
  The existing frameworks indeed both describe „vulnerability management“ from rather different perspectives!
  Alignments are left as an exercise to the observing user (for now).

What team types do we need then?

And what is a SOC / CSIRT / PSIRT / ISAC now exactly?

	Monitoring and Detection	Event Analysis	Information Security Incident Report Acceptance	Information Security Incident Analysis	Artifact and Forensic Evidence Analysis	Mitigation and Recovery	Information Security Incident Coordination	Crisis Management Support	Vulnerability Discovery/Research	Vulnerability Report Intake	Vulnerability Analysis	Vulnerability Coordination	Vulnerability Disclosure	Vulnerability Response	Data Acquisition	Analysis and Synthesis	Service Communication	Awareness Building	Training and Education	Exercises	Technical and Policy Advisory
SOC	MUST	MUST																			
CSIRT			MUST	MUST		MUST	MUST														
PSIRT										MUST	MUST	MUST	MUST	MUST							
ISAC															MUST	MUST	MUST				

You can name your team whatever you like ...

But keep in mind:

- **We (all) need to agree on capabilities – and consistent naming thereof: FORGET ABOUT MARKETING – at least for a moment!**

  You know the „duck“ test, do you?
  If it swim like a duck, and quacks like a duck, ...

- **And yes, your „duck“ might be different!**
  But much more important is, whether you still have a “duck“!
  We (the SIG) knows we need to agree on sub-types for teams

- **Service providers offer what the customer wants (and pays for)**
  But again, if a „duck“ is offered, it better swims like a duck and quacks like it, ...

You can name your team whatever you like ...

But keep in mind:

- **We (all) need to agree on capabilities – and consistent naming thereof: FORGET ABOUT MARKETING – at least for a moment!**

  You know the „duck“ test, do you?
  If it swim like a duck, and quacks like a duck, ...

- **And yes, your**
  But much
  We (the S

- **S**
  But
  like

Wait for announcement of review draft before October 2023! Then: Provide feedback and input (as you see fit ;)

... And maybe make the „duck“ test ;)

Contact:

CSIRT Framework Development SIG

Prof. Dr. Klaus-Peter Kossakowski (Chair)
klaus-peter.kossakowski@haw-hamburg.de