Open CSIRT Foundation

SIM3 & MATURE TEAMS

How to use SIM3 with other standards to measure and improve a team's maturity using SIM3

KLAUS-PETER KOSSAKOWSKI

MIROSŁAW MAJ

OLIVIER CALEFF

DON STIKVOORT

ALL ON BEHALF OF OPEN CSIRT FOUNDATION

https.//www.trusted-introducer.org/SIM3-mentoring.pdf

Open CSIRT Foundation

SIM3 & MATURE TEAMS

How to use SIM3 with other standards
to measure and improve a team’s maturity using SIM3

MIROSŁAW MAJ & KLAUS-PETER KOSSAKOWSKI

ALL ON BEHALF OF OPEN CSIRT FOUNDATION

Acknowledgements

Open CSIRT Foundation

CERTIFIED BY TRUSTED INTRODUCER TI

CYBER4Dev

FIRST™ Improving Security Together

Why using SIM3?

SIM3 can – because it is a maturity model – help you to assess the maturity of your – or other – teams! Good to know and handy if you want to improve ...

SIM3 can be used as monitoring tool to increase the team‘s maturity including performance and service quality over time!

SIM3 works in the context of various profiles including acquiring FIRST membership – and ensures interoperability which cannot be reached by membership / accreditation

Maturity

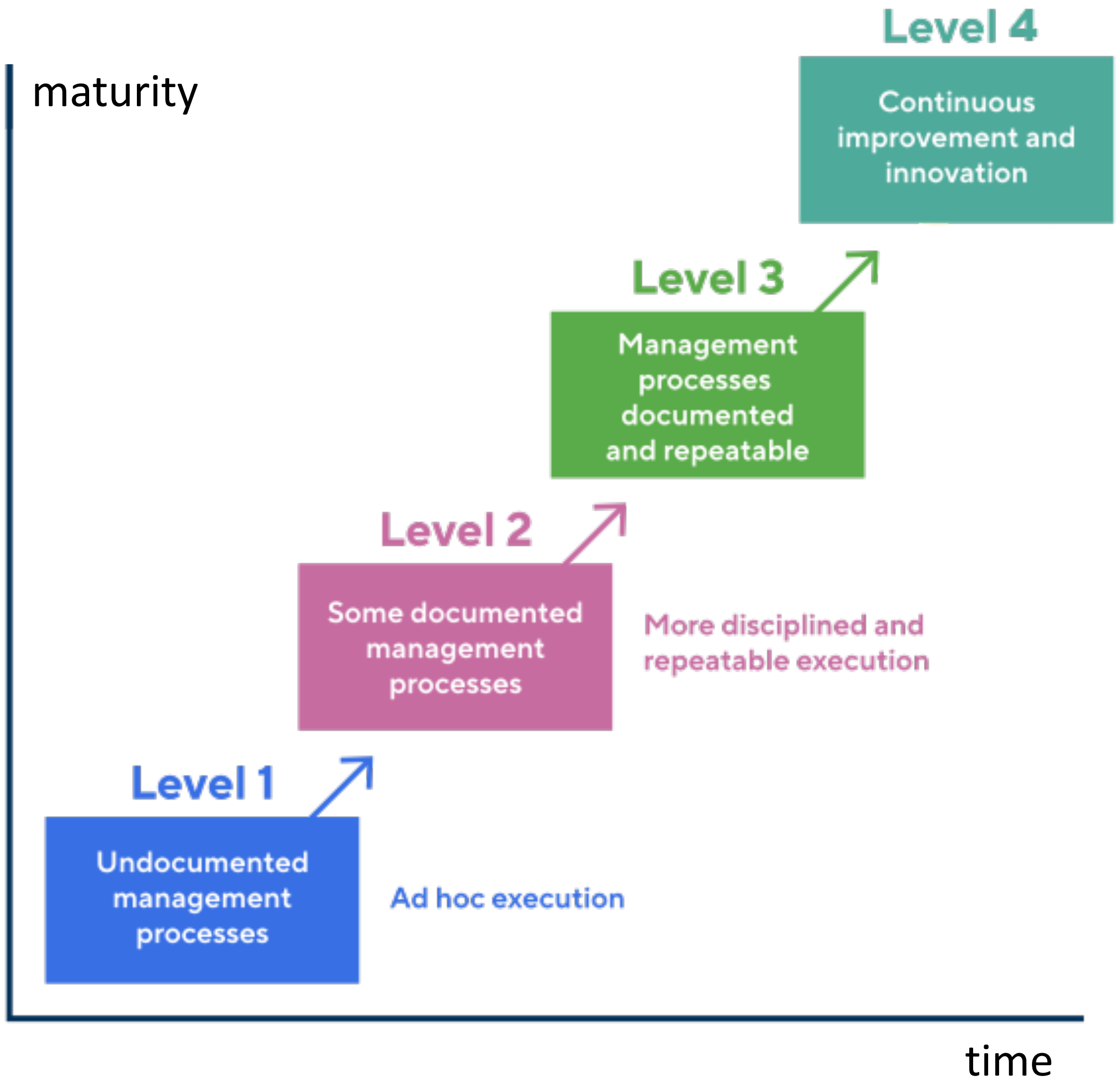
How effectively an organization executes a particular capability within the mission and authorities of the organization. It is a level of proficiency attained either in executing specific functions or in an aggregate of functions or services.

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.

Source:
https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1#ANNEX-2-Terms-and-Definitions

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.


maturity
Level 4
Continuous improvement and innovation
Level 3
Management processes documented and repeatable
Level 2
Some documented management processes
More disciplined and repeatable execution
Level 1
Undocumented management processes
Ad hoc execution
time

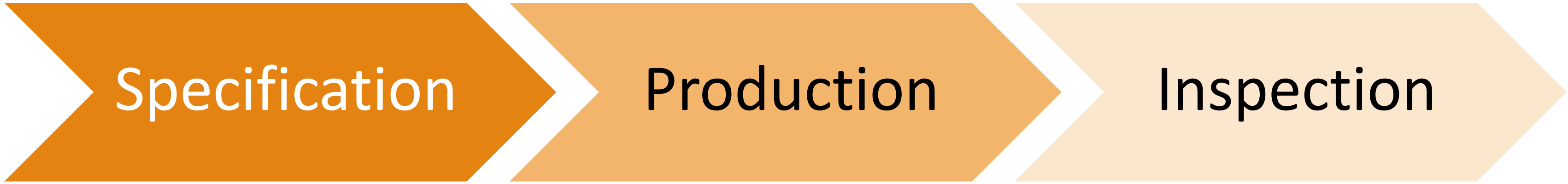
Maturity Levels are nothing new ...

Level	Description
0	not available / undefined / unaware
1	implicit (known/considered but not written down, “between the ears”)
2	explicit internal (written down but not formalised in any way)
3	explicit formalised (published or rubberstamped)
4	subject to control process / audited / enforced

… but those Levels need to be clearly defined!

Only if „we“ learn, we will be able to improve!

- In order to improve „something“, it needs some kind of learning process
  - and the ability to observe a specific behaviour (service delivery) and
  - reasoning on the observed outcome.
- Today this is strongly related to the concept of „organisational“ learning even for organisations and not only individuals ...
- Originally introduced in 1939 by Walter Andrew Shewhart on the topic of quality improvement in engineering ...



Specification

Production

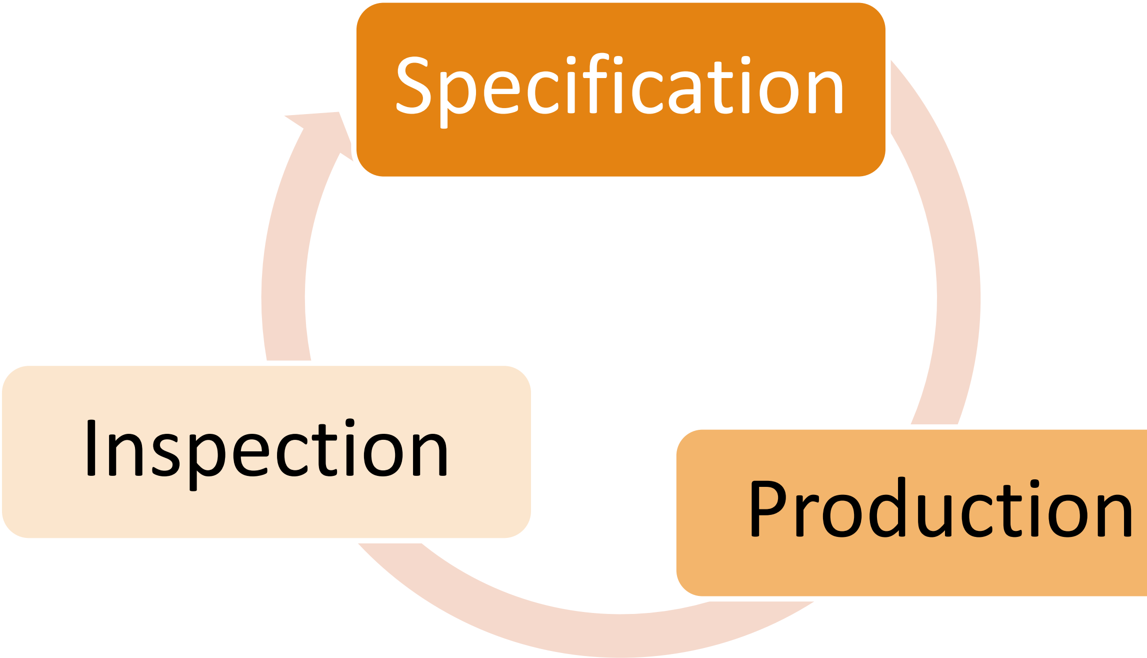
Inspection

Shewart: These steps must go into a Circle!

He was realy into a rather academic perspective:

- First of all you need to have a hypothesis
- then you need to test it and
- only after (many) such tests you
- you will be able to determine
  if the hypothesis is right ...
- if not, better start over again ;)

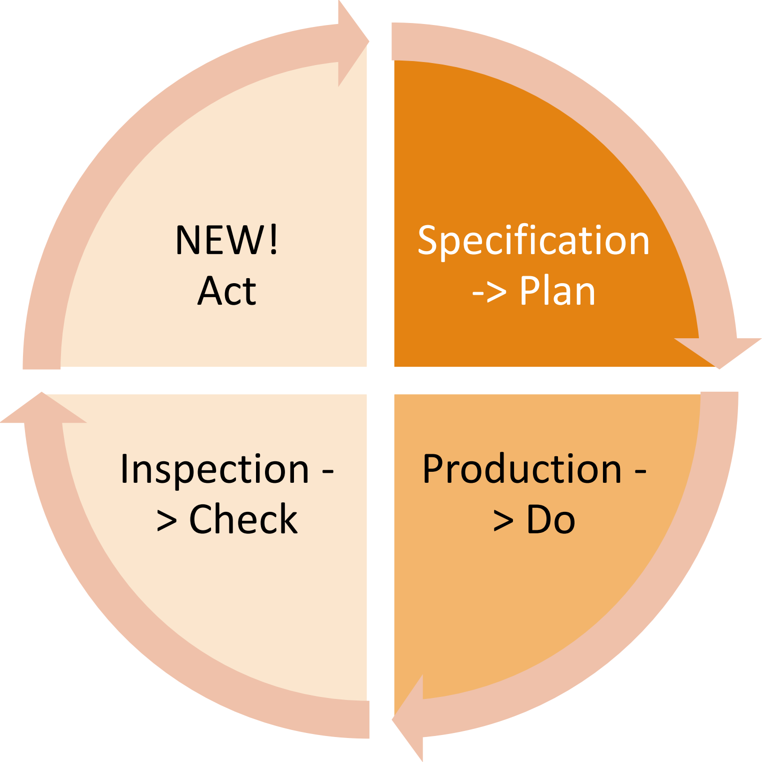
W. Edwards Deming was the person to build on the concepts of his teacher and trained > 35.000 ingenieurs to think differently!



Deming introduced an evolutionary Approach

He is actually the creater of what we know today as PDCA cycle

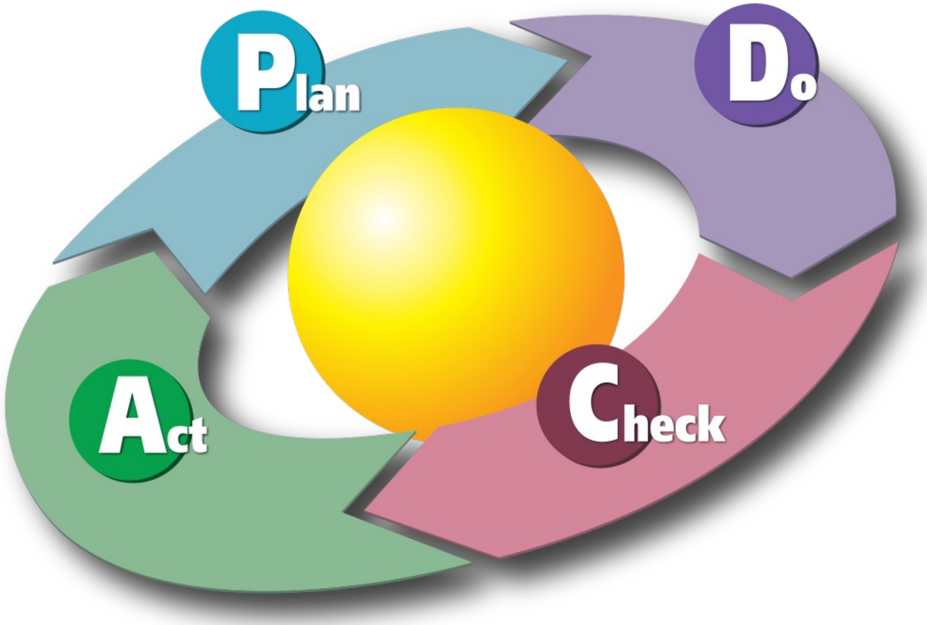
- **Plan** including the analysis of potentials and current status
- Next phase is limited to **do** a test in a very practical setting if it works
- Only after **checking** (with a limited scope) and good results those improvements should be applied
- This requires to **act**, as any new procedure or workflow needs to be defined as new best practice, changing the way the organisation works!



Genba (現場)

In business, *genba* refers to the place where value is created, could be the factory floor. But it can be any "site" such as a construction site, sales floor or where the service provider interacts directly with the customer.

1. If something happens, go there
2. Check all people and circumstances
3. Execute ad-hoc measures
4. Identify the root causes
5. Mitigate any such root causes
6. Improve to avoid further instances

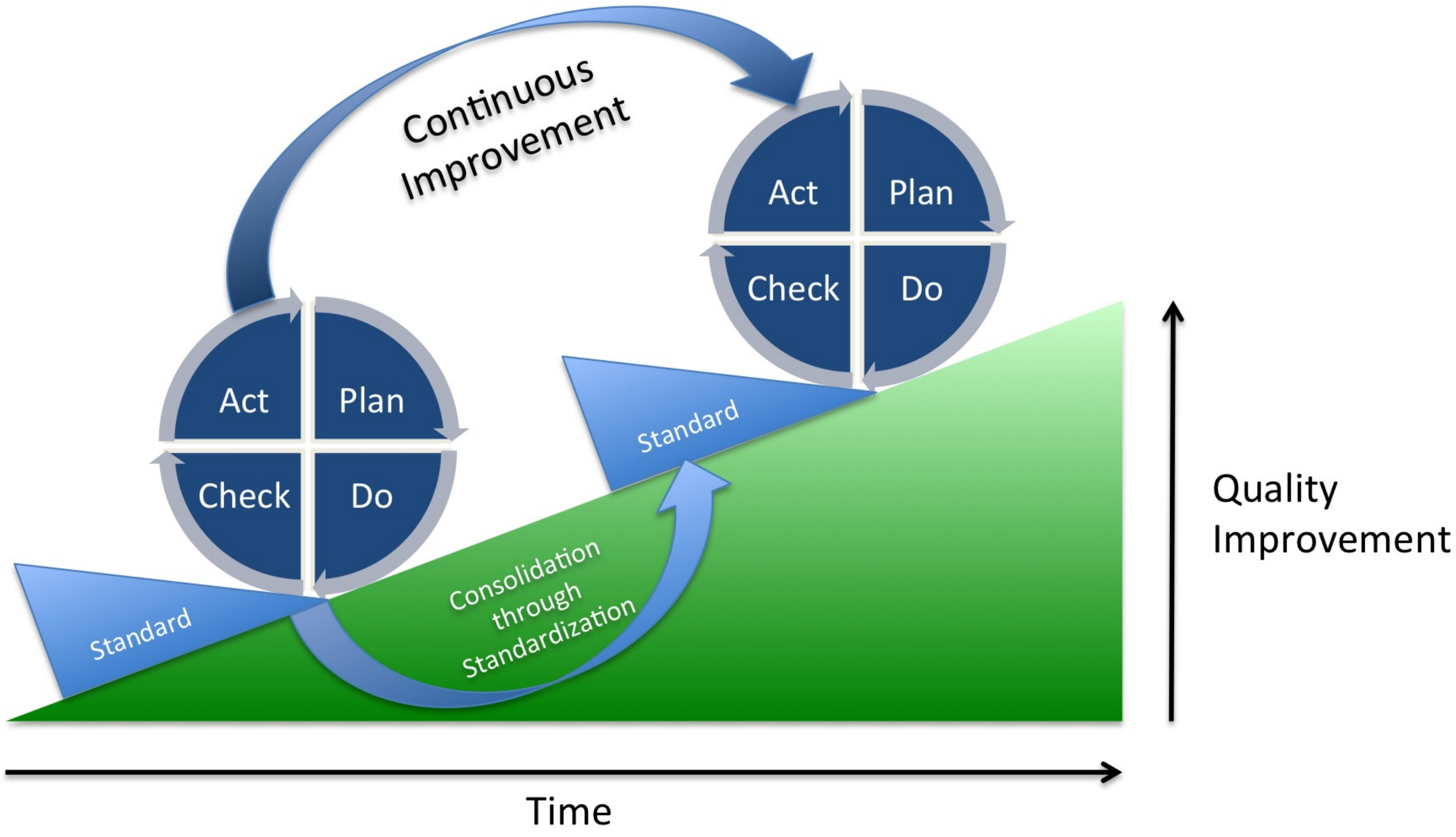


https://www.bulsuk.com/2009/02/taking-first-step-with-pdca.html Taking the First Step with the PDCA Cycle / K.G. Bulsuk (including diagram)

Continuous Improvement Process

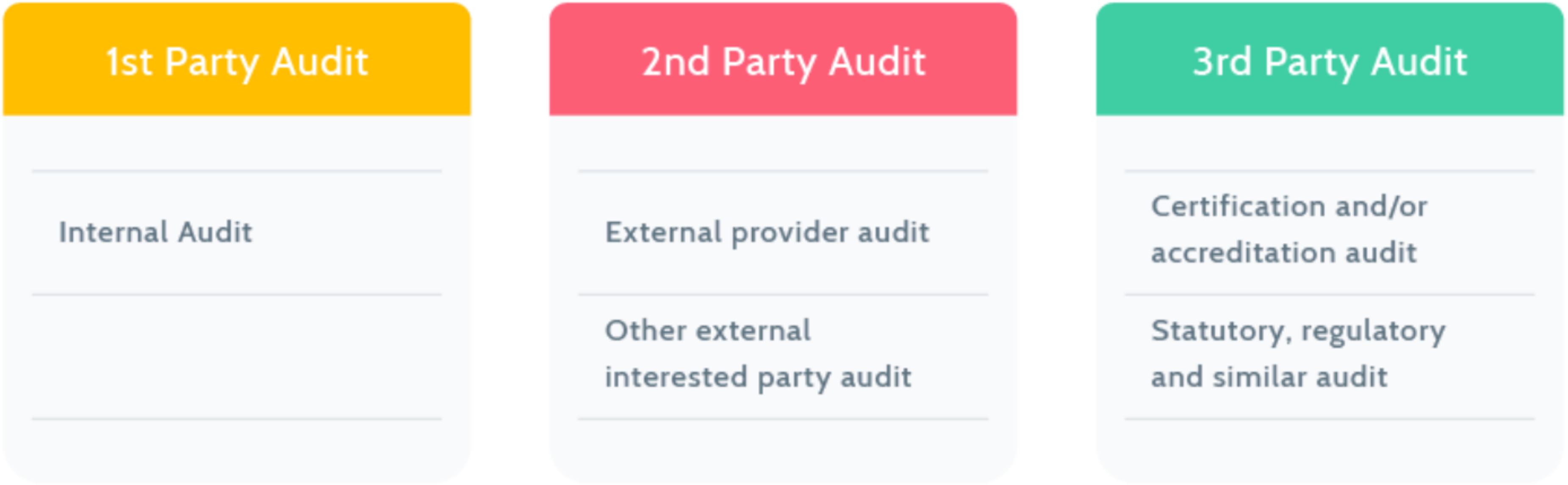
In any case the PDCA cycle became the „de-facto“ standard for all quality management approaches!

改 善



https://de.wikipedia.org/wiki/Demingkreis#/media/Datei:PDCA_Process.png

SIM3
as baseline for Assessments / Audits



1st Party Audit	2nd Party Audit	3rd Party Audit
Internal Audit	External provider audit	Certification and/or accreditation audit
	Other external interested party audit	Statutory, regulatory and similar audit

SIM3 as Third-Party Assessments

Third party assessments are done by independent organizations that have no vested or conflict of interest in the organization being audited, like those that provide certification, or government agencies.

Independence of the assessment organization and auditors is one of the defining factors of a third-party audit.

Not yet relevant in CSIRT context: In some settings stake holders can also request third-party audits, and this will usually be in order to verify you conform to some specific requirements.

Open CSIRT Foundation

Kaizen:
Change for the Better!

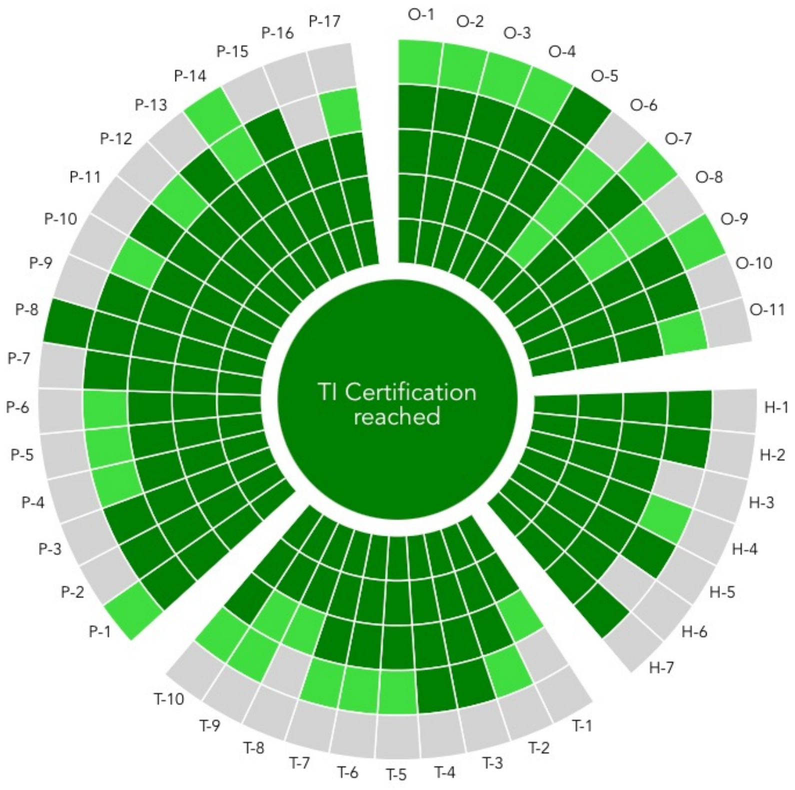
Certainly we can focus on the economic perspectives, like quality improvements or decrease of costs only.

But to realy improve the quality of anything, you must be prepared to question (nearly) everything and test your assumptions!

This is also true for any third-party assessment, which should result in a win/win situation focusing on

1. Constituents
2. Processes
3. Quality
4. Weaknesses
5. Standardisation

→ Baseline of any quality management system!



SIM3-CHECK.opencsirt.org

- **A simple to use tool for any (quick) self assessment**
- **Improved tooling for SIM3 auditors**
- **Includes the most actual „manual“ on SIM3 v2interim https://sim3-check.opencsirt.org/**
- **Additional features available for SIM3 Auditors**
  - **Export of all views (still CSV, working on Excel)**
  - **Comparison and visualization of two different assessments**
- **Previous SIM3 v1 still available https://sim3-check.opencsirt.org/sim3v1/**

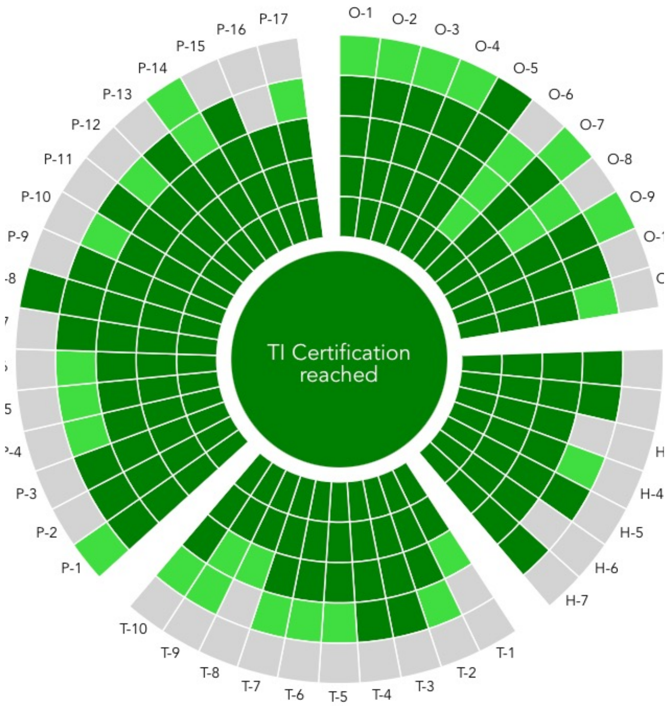
Why do we need different Profiles?

- **Defining a minimum threshold**
  → FIRST membership criteria (define minimum oriented levels)
  → TI certification criteria (define a specific minimum level with high assurance applicable for all kind of teams, not only CSIRTs Network)

- **Defining a growth Path**
  → ENISA Maturity levels
  an approach to reach a desired outcome in several phases for a set of teams that operate in the same legal framework

SIM3-CHECK.opencsirt.org

- FIRST Membership (v2i - O-6 set to level „0“)
  https://sim3-check.opencsirt.org/#/v1/66C1nXDVm-4AwLRcfsq-4CNCdxjOQ
- ENISA Basic (v2i)
  https://sim3-check.opencsirt.org/#/v1/66C3VaNye-55Nw6kf3O-5DTYOkC4a
- ENISA Intermediate (v2i)
  https://sim3-check.opencsirt.org/#/v1/6CaeFNgPF-5BIGQX5L1-69s9yXvmv
- ENISA Advanced (v2i)
  https://sim3-check.opencsirt.org/#/v1/6CafLtd90-66CfWhJ03-6cBKCPKIY
- TI Certification (v2i - O-6 set to level „0“)
  https://sim3-check.opencsirt.org/#/v1/66CcDU1PI-63Ikl6zRL-66iJpajOu



Open CSIRT Foundation

CSIRT Services

Standards used in conjunction with SIM3

KLAUS-PETER KOSSAKOWSKI

OLIVIER CALEFF

MIROSŁAW MAJ

DON STIKVOORT

ALL ON BEHALF OF OPEN CSIRT FOUNDATION

Just wonder what is already out there in regard to standards?

-- 1998: RFC 2350 / IETF (co-chaired by CERT/CC and DFN-CERT)

-- 2002: CSIRT Services List (published by CERT/CC)

-- 2004: Code of Practice (developed by TF-CSIRT)

-- 2009: TLP (adapted from GB and now maintained by FIRST, co-chaired by US-CERT and OCF)

-- 2009: SIM3 (developed/maintained by OCF and adopted by TF-CSIRT, NCA, ENISA and FIRST)

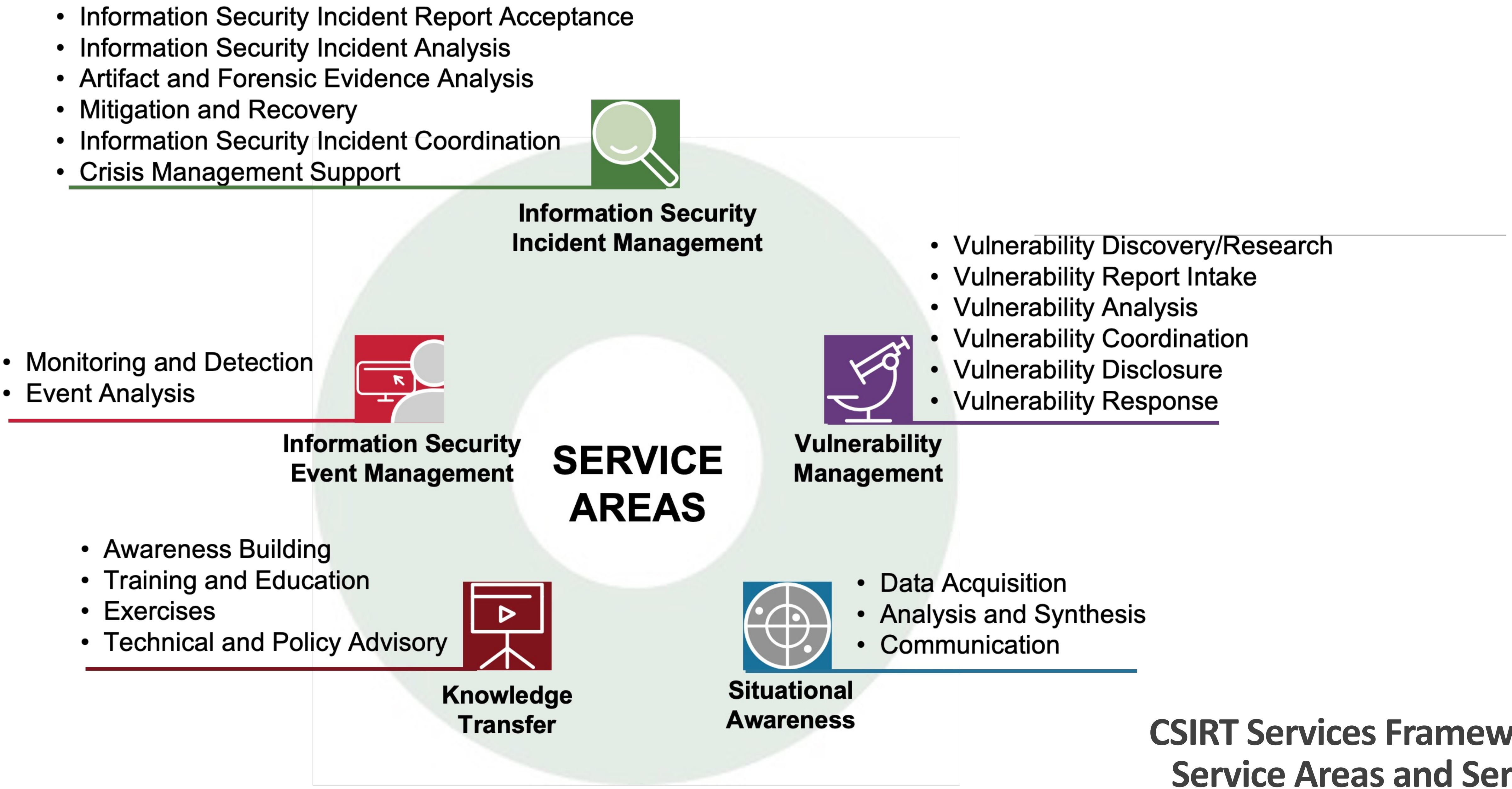
-- 2003 / 2017: Incident Taxonomy (adopted from eCSIRT.net and now maintained by TF-CSIRT)

-- 2017: CSIRT Services Framework (v1.1)

-- 2019: CSIRT Services Framework (v2.1 re-write, maintained by FIRST, chaired by OCF)

-- 2021: CSIRT Roles and Competencies (v0.9 review, maintained by FIRST, chaired by OCF)

CSIRT Services Framework / Service Areas and Services



SERVICE AREAS

Information Security Incident Management

- 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 Management

- Vulnerability Discovery/Research
- Vulnerability Report Intake
- Vulnerability Analysis
- Vulnerability Coordination
- Vulnerability Disclosure
- Vulnerability Response

Situational Awareness

- Data Acquisition
- Analysis and Synthesis
- Communication

Knowledge Transfer

- Awareness Building
- Training and Education
- Exercises
- Technical and Policy Advisory

Information Security Event Management

- Monitoring and Detection
- Event Analysis

Services Frameworks apply to different team types

- **No attempt to build specific team types into it:**
  Service offerings however can be described using the same service names (but different service levels or attributes)
- **No attempt to synchronize (yet) with other services frameworks:**
  If multiple frameworks describe „vulnerability management“, separate / overlapping / contradicting descriptions (based on a rather not aligned context) are possible and should be ignored (for now).

Understanding the leading principle

The framework for CSIRT services is based on the relationships of four key elements:

SERVICE AREAS

→ **SERVICES**

→ **FUNCTIONS**

→ **SUB-FUNCTIONS**

SERVICE AREA
Information Security Event Management

SERVICE AREA
Information Security Incident Management

SERVICE AREA
Vulnerability Management

SERVICE AREA
Situational Awareness

SERVICE AREA
Knowledge Transfer

SERVICE AREA Information Security Event Management

Monitoring and Detection
- Log and Sensor Management
- Detection Use Case Management
- Contextual Data Management

Event Analysis
- Correlation
- Qualification

SERVICE AREA Information Security Incident Management

Information Security Incident Report Acceptance
- Information Security Incident Report Receipt
- Information Security Incident Triage and Processing

Information Security Incident Analysis
- Information Security Incident Triage (Prioritization and Categorization)
- Information Collection
- Detailed Analysis Coordination
- Information Security Incident Root Cause Analysis
- Cross-Incident Correlation

Artifact and Forensic Evidence Analysis
- Media or Surface Analysis
- Reverse Engineering
- Runtime or Dynamic Analysis
- Comparative Analysis

Mitigation and Recovery
- Response Plan Establishment
- Ad Hoc Measures and Containment
- System Restoration
- Other Information Security Entities Support

Information Security Incident Coordination
- Communication
- Notification Distribution
- Relevant Information Distribution
- Activities Coordination
- Reporting
- Media Communication

Crisis Management Support
- Information Distribution to Constituents
- Information Security Status Reporting
- Strategic Decisions Communication

SERVICE AREA Vulnerability Management

Vulnerability Discovery/Research
- Incident Response Vulnerability Discovery
- Public Source Vulnerability Discovery
- Vulnerability Research

Vulnerability Report Intake
- Vulnerability Report Receipt
- Vulnerability Report Triage and Processing

Vulnerability Analysis
- Vulnerability Triage (Validation and Categorization)
- Vulnerability Root Cause Analysis
- Vulnerability Remediation Development

Vulnerability Coordination
- Vulnerability Notification/Reporting
- Vulnerability Stakeholder Coordination

Vulnerability Disclosure
- Vulnerability Disclosure Policy and Infrastructure Maintenance
- Vulnerability Announcement/ Communication/Dissemination
- Post-Vulnerability Disclosure Feedback

Vulnerability Response
- Vulnerability Detection/Scanning
- Vulnerability Remediation

SERVICE AREA Situational Awareness

Data Acquisition
- Policy Aggregation, Distillation, and Guidance
- Asset Mapping to Functions, Roles, Actions, and Key Risks
- Collection
- Data Processing and Preparation

Analysis and Synthesis
- Projection and Inference
- Event Detection (through Alerting and/or Hunting)
- Information Security Incident Management Decision Support
- Situational Impact

Communication
- Internal and External Communication
- Reporting and Recommendations
- Implementation
- Dissemination/Integration/Information Sharing
- Management of Information Sharing
- Feedback

SERVICE AREA Knowledge Transfer

Awareness Building
- Research and Information Aggregation
- Report and Awareness Materials Development
- Information Dissemination
- Outreach

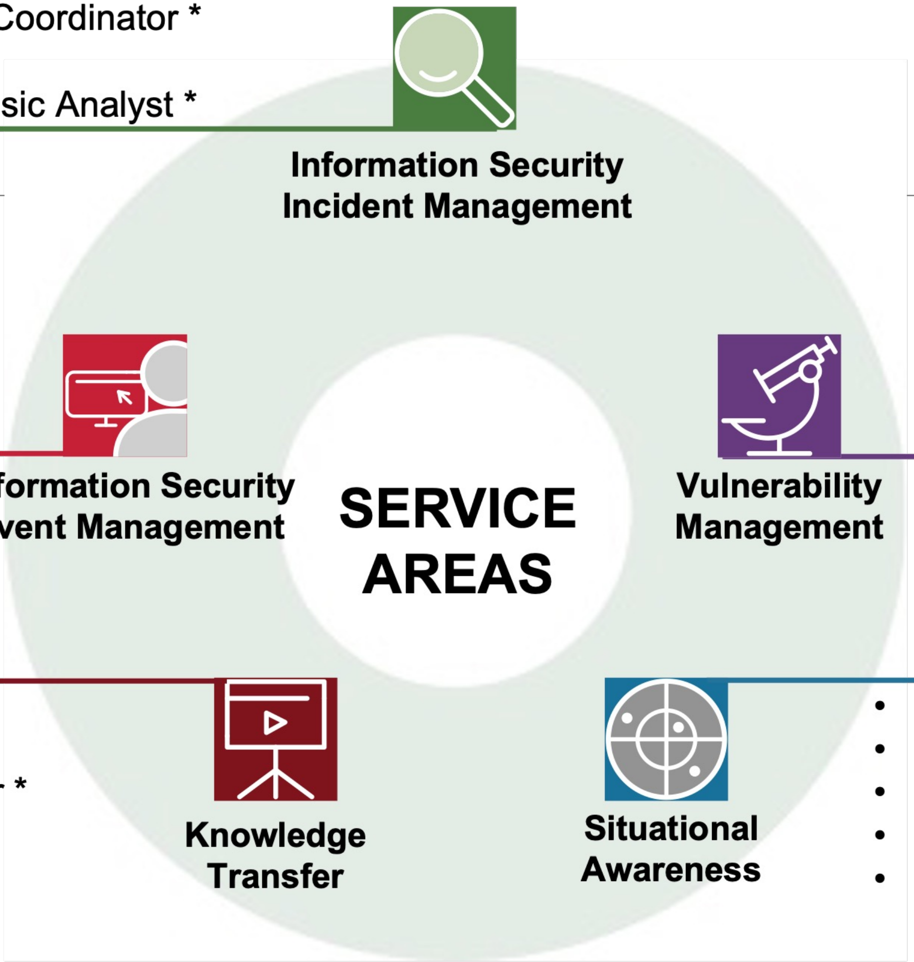
Training and Education
- Knowledge, Skill, and Ability Requirements Gathering
- Educational and Training Materials Development
- Content Delivery
- Mentoring
- CSIRT Staff Professional Development

Exercises
- Requirements Analysis
- Format and Environment Development
- Scenario Development
- Exercise Execution
- Exercise Outcome Review

Technical and Policy Advisory
- Risk Management Support
- Business Continuity and Disaster Recovery Planning Support
- Policy Support
- Technical Advice

CSIRT Services Framework / Services and Functions

CSIRT Services Framework / Service Areas and Roles



SERVICE AREAS

Information Security Incident Management

- Communication Liaison *
- Incident Analyst *
- Incident Responder
- Incident Triage Coordinator *
- IT Administrator
- Malware / Forensic Analyst *

Information Security Event Management

- Data Manager
- Incident Analyst *
- Incident Triage Coordinator *
- System and Sensor Administrator
- Use Case Manager

Vulnerability Management

- Incident Analyst *
- IT Security Administrator
- Malware/Forensic Analyst *
- Vulnerability Analyst
- Vulnerability Assessment Analyst
- Vulnerability Coordinator
- Vulnerability Disclosure Coordinator
- Vulnerability Researcher
- Vulnerability Triage Coordinator

Knowledge Transfer

- Awareness Coordinator
- Policy Advisor
- Risk & Continuity Advisor *
- Staff Developer
- Technical Policy Advisor
- Training Developer
- Training Instructor

Situational Awareness

- Communication Liaison *
- Risk Analyst / Risk & Continuity Advisor *
- Situational Awareness Data Analyst
- Situational Awareness Manager
- Threat Warning Analyst

* role defined for multiple service areas

Apply the CSIRT Services Framework here!

O-5 Service Description

Description: Describes what the CSIRT service is and how to reach it.

Question: Whereas 'responsibility' is usually formulated as a high level form of expectations of your CSIRT, the description of your team's services are the way you further shape that into a concise list of services that you offer to your constituency, which will most likely include incident management/response, but also possibly vulnerability handling, malware analysis, awareness raising and potentially others.

[...] It is important to make a clear selection of those services you must or should offer based on your mandate, authority and responsibility - and taking into account the resources you have available.

All of this leads to a list of services, and it is important to consider that at least your constituency needs to have access to this list, including your team's contact information and service windows. It is strongly advised to use RFC2350 as a standardised way to publish a high-level list of their services, contact info and service windows even to the Internet at large, as for any CSIRT it is important that it is known how to reach them.

... and here also!

O-7 Service Level Description

Description: Describes the level of service to be expected from the CSIRT.

Minimum requirement: Specifies the speed of reaction to incoming incident reports and reports from constituents and from peer CSIRTs. For the latter a human reaction within two working days is the minimum expected.

Question: Have service levels been defined for the services that your CSIRT offers? This can range from something as simple as the requirement to send a first (human) reaction to incident reports within a set amount of time, to more extensive "SLA" type requirements.

Open CSIRT Foundation

CSIRT Services & Roles

Standards used in conjunction with SIM3

KLAUS-PETER KOSSAKOWSKI

OLIVIER CALEFF

MIROSŁAW MAJ

DON STIKVOORT

ALL ON BEHALF OF OPEN CSIRT FOUNDATION

Defining Roles for all Functions

The new document currently written for CSIRTs (final draft expected for begin IV/2023) is based on competencies for those carrying out the specific (service) functions!

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

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

SERVICE AREA
Information Security
Incident Management

Defining Roles for all Functions

The new document currently written for CSIRTs is based on competencies for those carrying out the specific (service) functions!

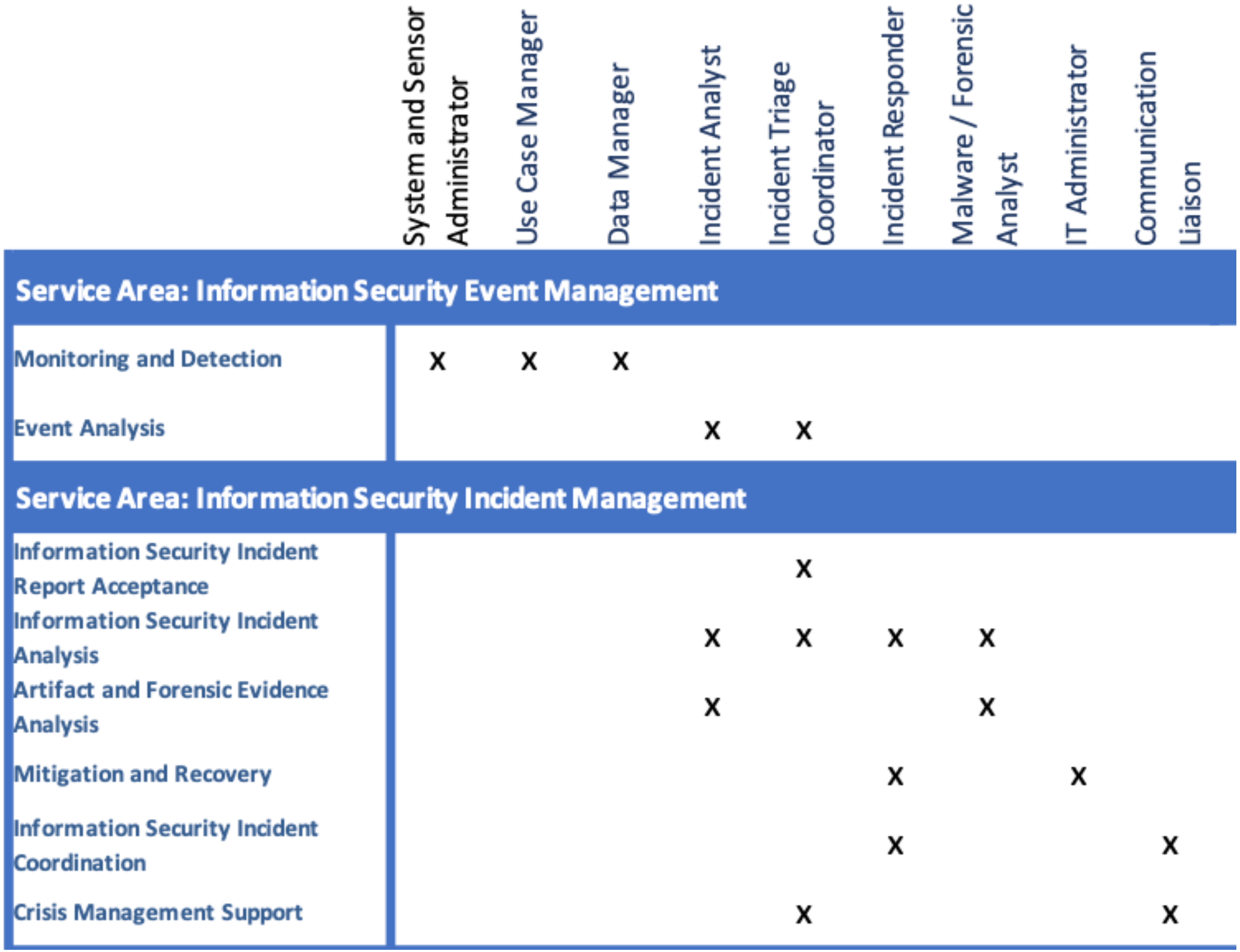
- **Use Case Manager**
- **Data Manager**

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

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

SERVICE AREA
Information Security
Event Management

SERVICE AREA
Information Security
Incident Management



	System and Sensor Administrator	Use Case Manager	Data Manager	Incident Analyst	Incident Triage Coordinator	Incident Responder	Malware / Forensic Analyst	IT Administrator	Communication Liaison
Service Area: Information Security Event Management									
Monitoring and Detection	X	X	X						
Event Analysis				X	X				
Service Area: Information Security Incident Management									
Information Security Incident Report Acceptance					X				
Information Security Incident Analysis				X	X	X	X		
Artifact and Forensic Evidence Analysis				X			X		
Mitigation and Recovery						X		X	
Information Security Incident Coordination						X			X
Crisis Management Support					X				X

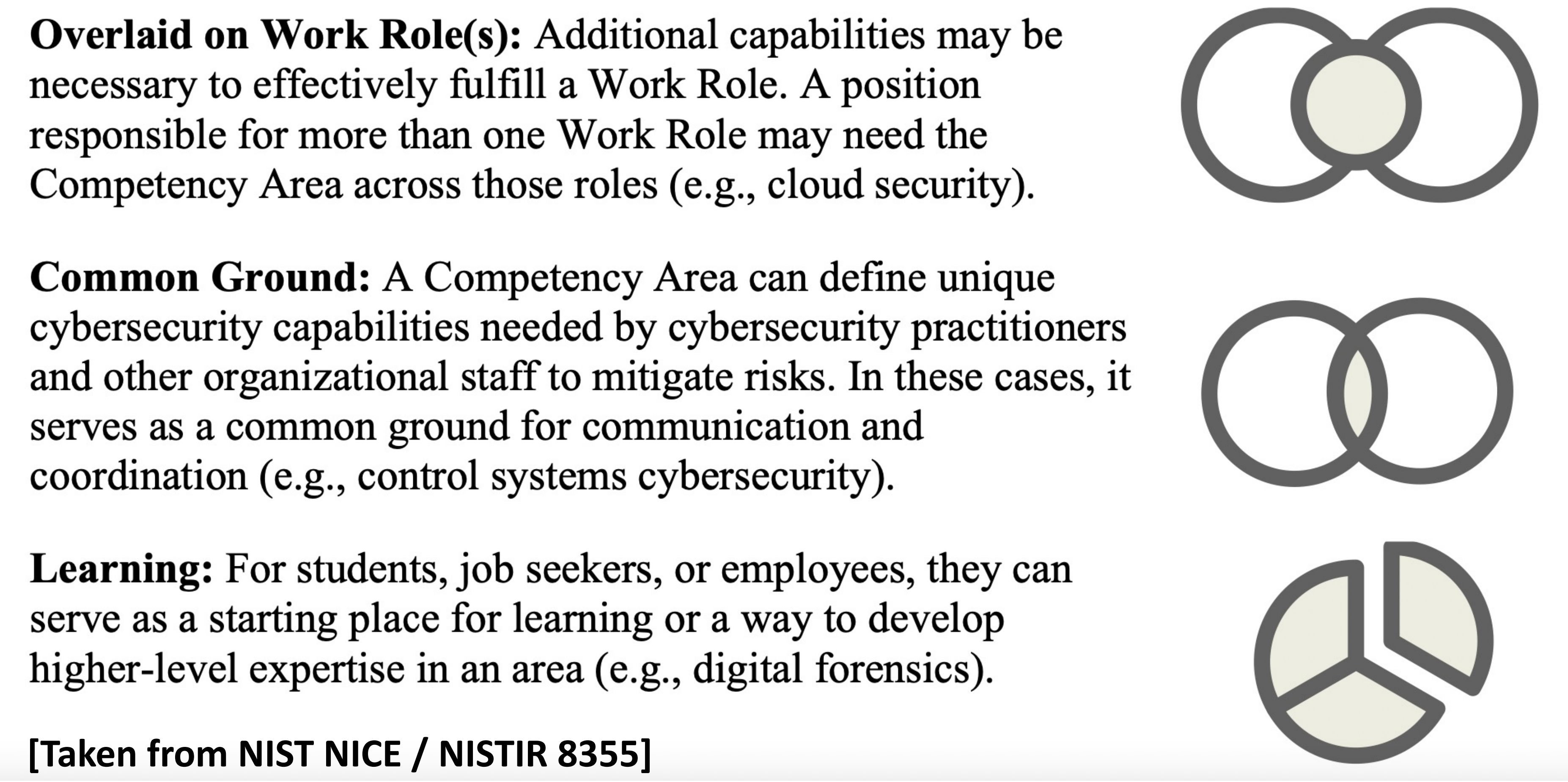
CSIRT Services Framework / Services and Roles

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.

How to use COMPETENCIES within a CSIRT?



Overlaid on Work Role(s): Additional capabilities may be necessary to effectively fulfill a Work Role. A position responsible for more than one Work Role may need the Competency Area across those roles (e.g., cloud security).

Common Ground: A Competency Area can define unique cybersecurity capabilities needed by cybersecurity practitioners and other organizational staff to mitigate risks. In these cases, it serves as a common ground for communication and coordination (e.g., control systems cybersecurity).

Learning: For students, job seekers, or employees, they can serve as a starting place for learning or a way to develop higher-level expertise in an area (e.g., digital forensics).

[Taken from NIST NICE / NISTIR 8355]

Role: Incident Responder / Generic Competencies

Professional

- Conflict Management(C009)
- Critical Thinking(C011)
- Oral Communication(C036)
- Presenting Effectively(C039)
- Written Communication(C060)

Operational

- Client Relationship Management(C003)

Technical

- Problem Solving(C040)

National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

https://www.nist.gov/system/files/documents/2019/11/08/nist.sp_.800-181.pdf

Role: Incident Responder / Role-Specific Competencies

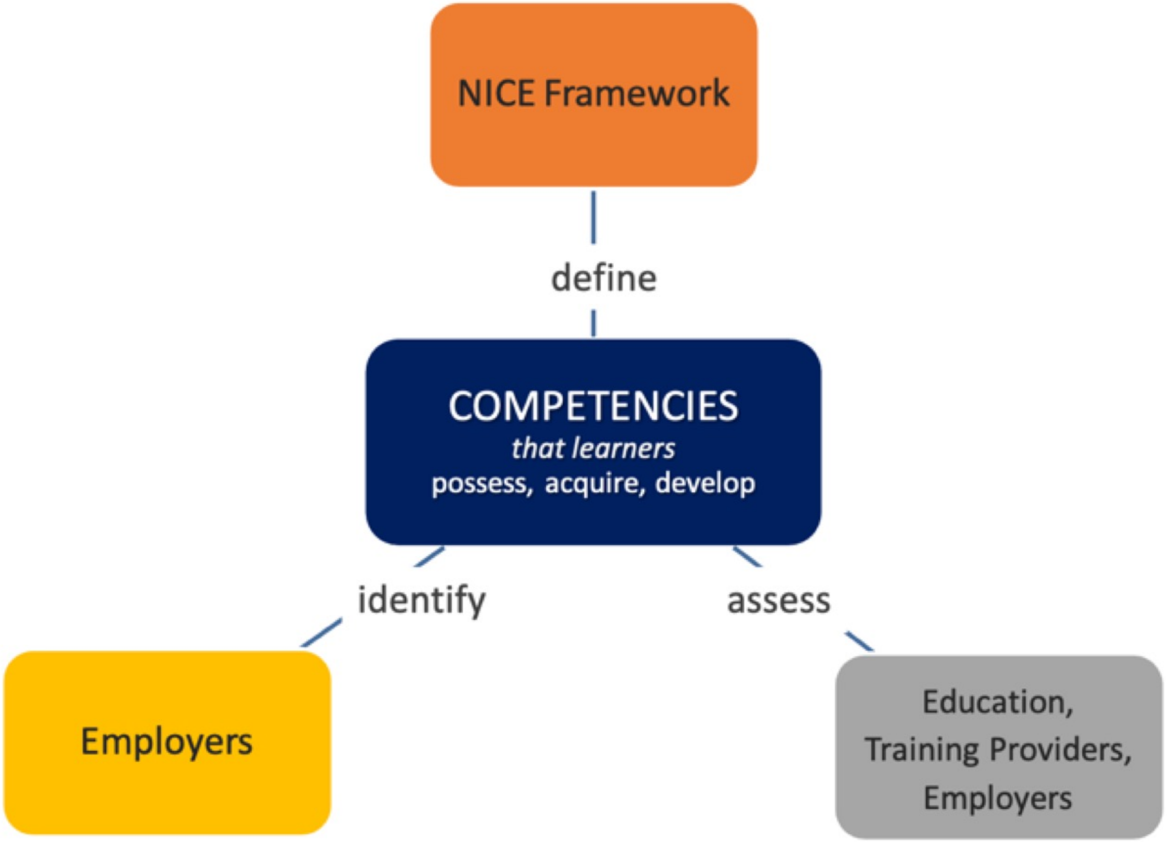
Operational

- Business Continuity (C002)
- Data Privacy and Protection (C014)
- External Awareness(C019)
- Legal, Government, and Jurisprudence (C030)
- Organizational Awareness (C037)
- Risk Management (C044)

Technical

- Computer Forensics (C005)
- Computer NetworkDefense (C007)
- Data Analysis (C012)
- Incident Management (C021)
- InformationSystems / Network Security (C024)
- Information Technology Assessment (C025)
- Intelligence Analysis (C027)
- Knowledge Management (C029)
- Technology Awareness (C053)
- Threat Analysis (C055)
- Vulnerabilities Assessment (C057)

How to get from COMPETENCIES to SKILLS?



NICE Framework

define

COMPETENCIES

that learners

possess, acquire, develop

identify

assess

Employers

Education, Training Providers, Employers

Role: Incident Responder / From Competencies to KSAs Competency: **(C031) Incident Management**

KSA ID	Knowledge, Skills, Abilities
K0041	Knowledge of incident categories, incident responses, and timelines for responses.
K0042	Knowledge of incident response and handling methodologies.
K0150	Knowledge of enterprise incident response program, roles, and responsibilities.
K0231	Knowledge of crisis management protocols, processes, and techniques.
K0292	Knowledge of the operations and processes for incident, problem, and event management.
K0317	Knowledge of procedures used for documenting and querying reported incidents, problems, and events.
K0343	Knowledge of root cause analysis techniques.
K0381	Knowledge of collateral damage and estimating impact(s).
K0399	Knowledge of crisis action planning and time sensitive planning procedures.
K0519	Knowledge of planning timelines adaptive, crisis action, and time-sensitive planning.
K0543	Knowledge of target estimated repair and recuperation times.
K0586	Knowledge of the outputs of course of action and exercise analysis.
S0054	Skill in using incident handling methodologies.
S0080	Skill in performing damage assessments.
S0175	Skill in performing root cause analysis.
S0365	Skill to design incident response for cloud service models.
A0025	Ability to accurately define incidents, problems, and events in the trouble ticketing system.
A0113	Ability to determine whether it violates a privacy principle or legal standard requiring specific legal action.
A0121	Ability to design incident response for cloud service models.
A0166	Ability to identify types of Communications Security (COMSEC) Incidents and how they're reported.

Open CSIRT Foundation

SIM3 does only apply to CSIRTs?

Parameters and Levels are for SIM capabilities, not CSIRTs only! But …

KLAUS-PETER KOSSAKOWSKI

OLIVIER CALEFF

MIROSŁAW MAJ

DON STIKVOORT

ALL ON BEHALF OF OPEN CSIRT FOUNDATIO

Services Frameworks apply to different team types

From „above“

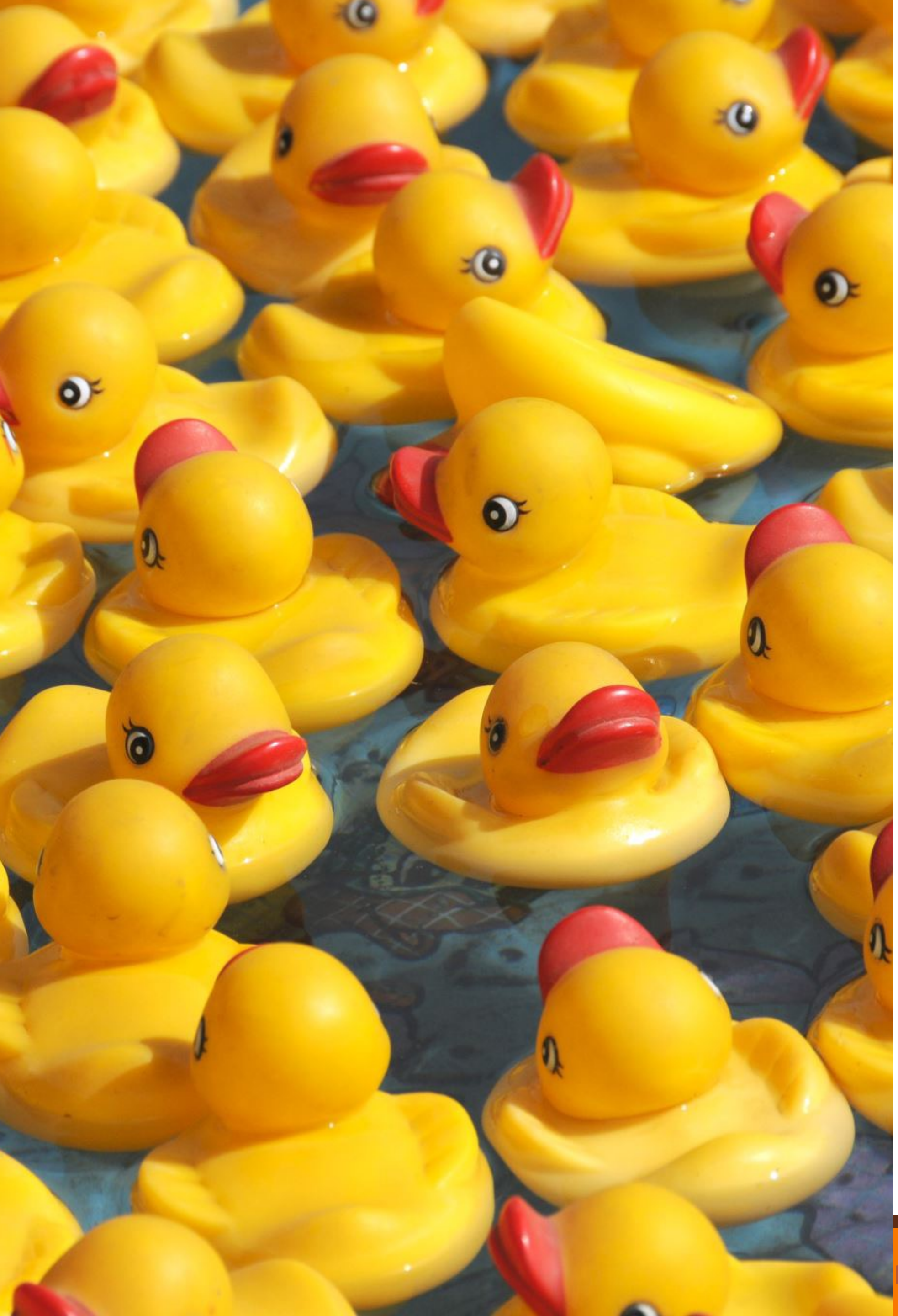
- **No attempt to build specific team types into it:** Service offerings however can be described using the same service names (but different service levels or attributes)
- **No attempt to synchronize (yet) with other services frameworks:** If multiple frameworks describe „vulnerability management“, separate / overlapping / contradicting descriptions (based on a rather not aligned context) are possible and should be ignored (for now).

What team types do we need then?

These are the four types of incident management and security teams:

- Computer Security Incident Response Teams (CSIRTs)
- Product Security Incident Response Teams (PSIRTs)
- Security Operations Centers (SOCs)
- Information Sharing and Analysis Centers (ISACs)

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

wants (and pays for)
ims like a duck and

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

Not everything from Services Frameworks might be mandatory to have!

- **Training and Awareness – as this is what „Knowledge Transfer“ is all about – is important! But it is not considered a MUST!**

  However, providing development of such materials and delivering related services is resource intensive if done by an incident management capability

  Therefore it is not always possible to provide. These activities are often also done by other parts of a capability's parent organization such as a training group or department, but with input from the incident management capability.

Open CSIRT Foundation

Contacts

INFO@OPENCSIRT.ORG

ALL ON BEHALF OF OPEN CSIRT FOUNDATION