ITU-T X.1060 CDC FOR AFRICA

SG17 Q3

ITU-T SG17 Question 3 Rapporteur
X.1060 Editors

Our Journey Today

A very simplified story – Few words about me just for context + I am colorblind

What is ITU-T X.1060 and Cyber Defence Center (CDC)?

Where does it come from?

Why and why now?

What is it?

How will African nations/countries implement?

The ”German” way!

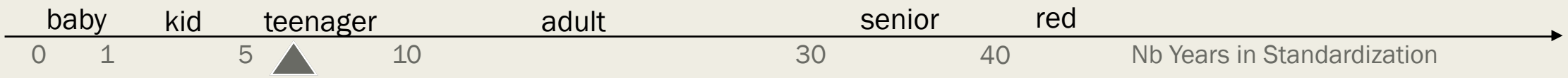
Key outcomes from SG17?

A VERY good meeting!

Arnaud Taddei – Broadcom Software Group – Symantec Enterprise Division

- ~~Global Security Strategist~~
- Techno-Diplomat on the UK Delegation
- Leadership positions in Standard Organizations
  - SG17 Vice Chairman, TSAG associate Rapporteur RG-IEM for Emerging tech
- Standardization Maturity level: “teenager”

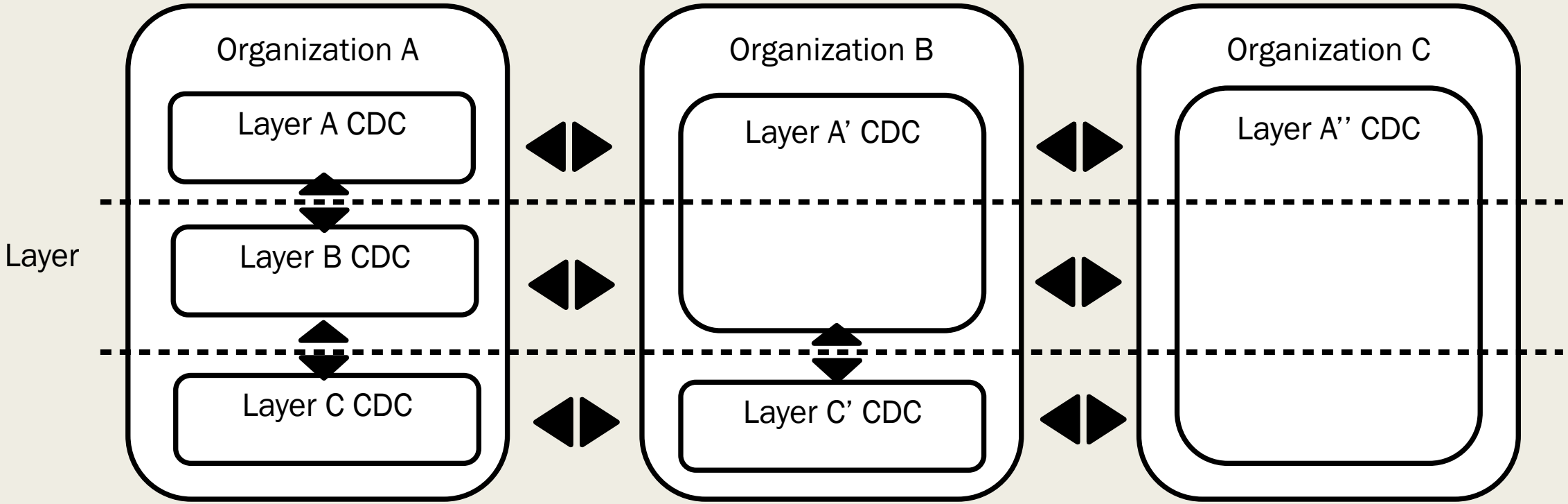
I am not here for that today



WHY USING X.1060?

Common language

- Widely common language for cybersecurity and available to everyone.
- Codifying the services and listing whole security services as best practices.



CDC = Broader concept that embraces the existing organizations

- CDC implies new concept
- But it does not mean a new organization - it may be performed by the existing functions
- A CDC is existing, if the services in X.1060 are provided and the related organizations works together
- CDC is rather broader concept than CSIRTs or SOCs - CDC includes them as a part of the services
- The concept of CDC become so important as an organization to counter broader impacts that are not limited to information systems, caused by cyber incidents

Process to the CDC

1. Risk management process (include cybersecurity)

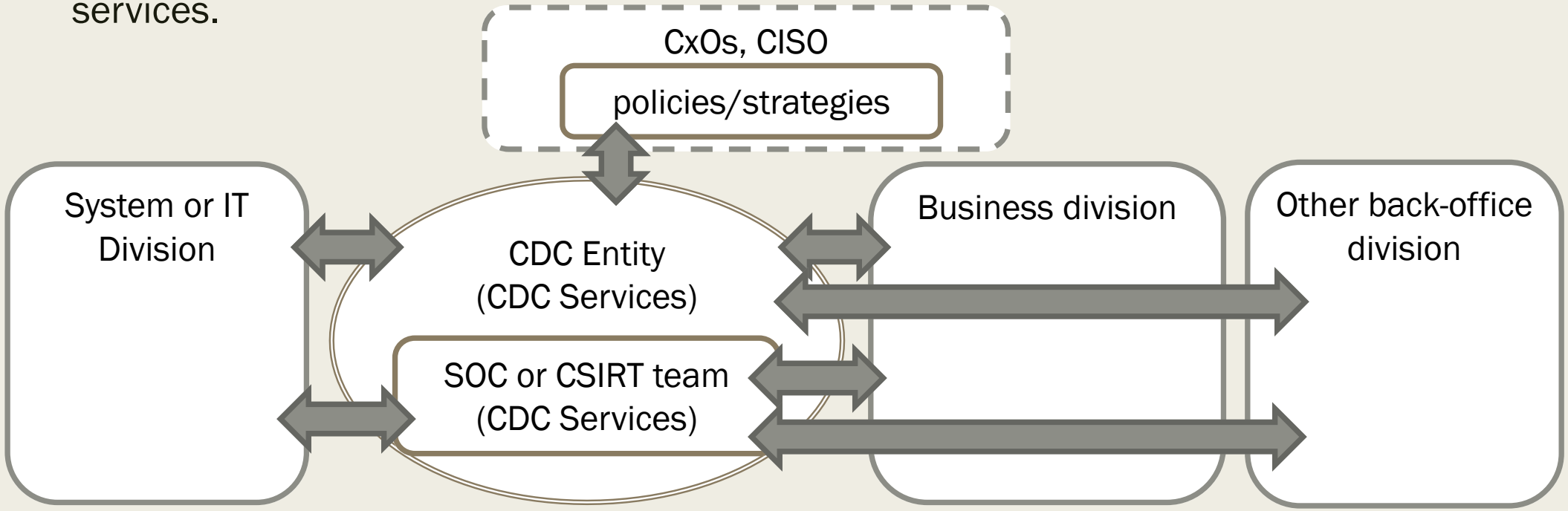
2. Prioritize those risks (include cybersecurity)

3. CISO decide to organize the CDC

4. Reference the X.1060 as a framework

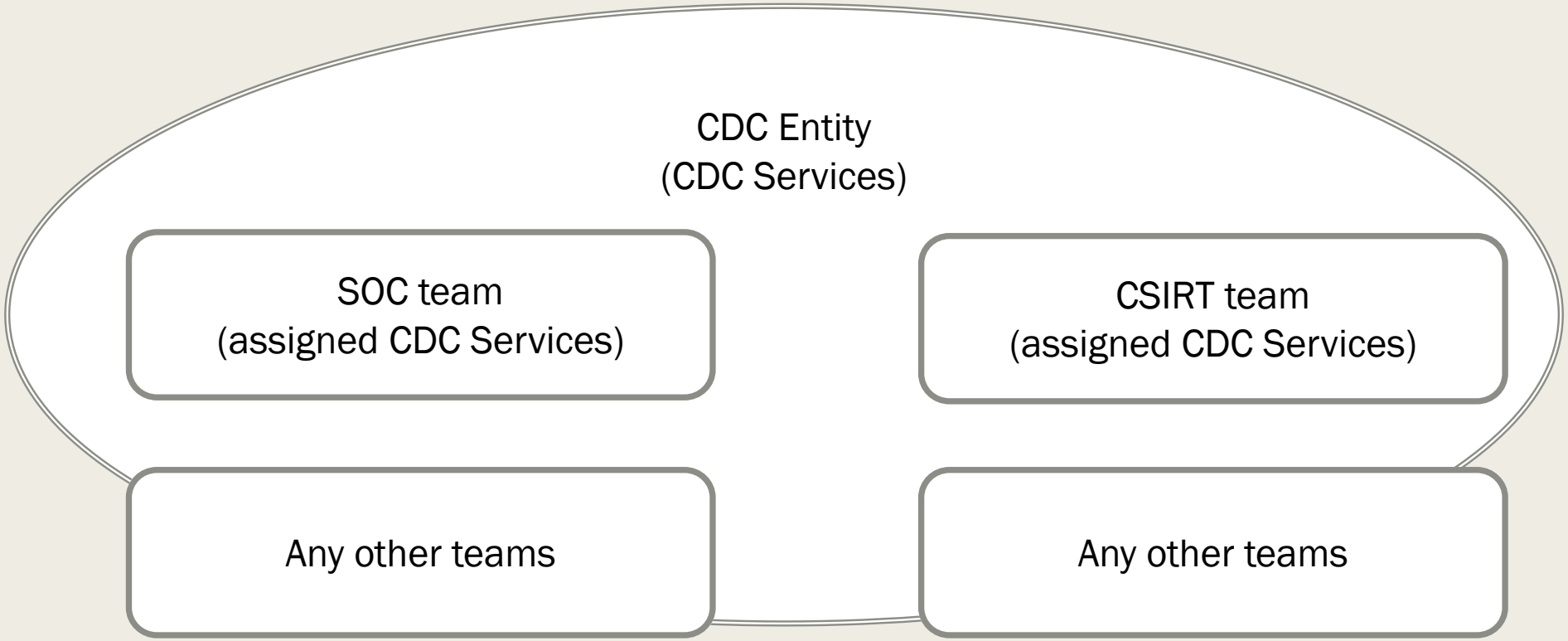
CDC provides security services which counter business risks.

- Cybersecurity is considered as a one of the important business risk.
- In order to deal with the risk of cybersecurity, it is necessary to provide not only the existing SOC and CSIRT/CERT/CIRT services but also a wide range of security services.



Teams assigned security services are sometimes called “SOC” or “CSIRT”.

- If the organization already has a ”SOC” or “CISRT” and implements CDC services, we can think of it as implementing part of CDC.



ITU-T X.1060 OVERVIEW
WHAT IS CDC?

X.1060

- Title
  - ***Framework for the creation and operation of a cyber defence centre***
- Scope
  - *X.1060 provides a framework for organizations to build and manage a Cyber Defence Centre (CDC), and to evaluate its effectiveness. The framework indicates how the CDC should define and implement security services to enable an organization's security.*
  - *This Recommendation is intended for those who is responsible for security at the top management level of an organization, such as Chief Security Officer (CSO) and/or Chief Information Security Officer (CISO), and security supervisors who assist the CSO and/or CISO.*

What is “Cyber Defence Centre (CDC)” ?

- Definition
  - *CDC is an entity within an organization that offers security services to manage the cybersecurity risks of its business activities*

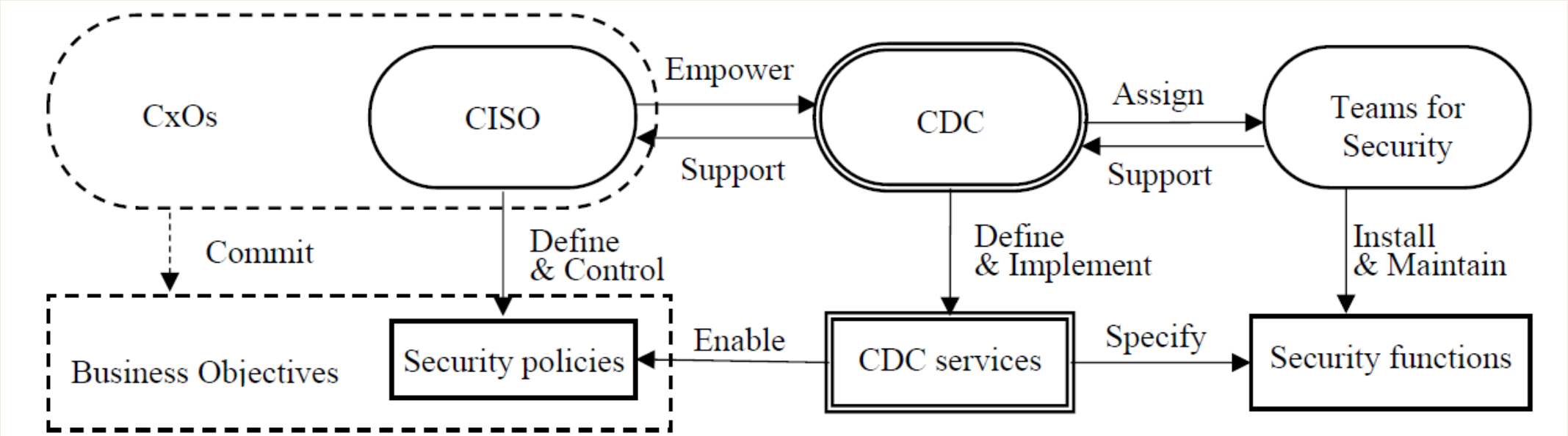


Figure 1 – Stakeholders and their roles for CDC operation

CDC in the organization

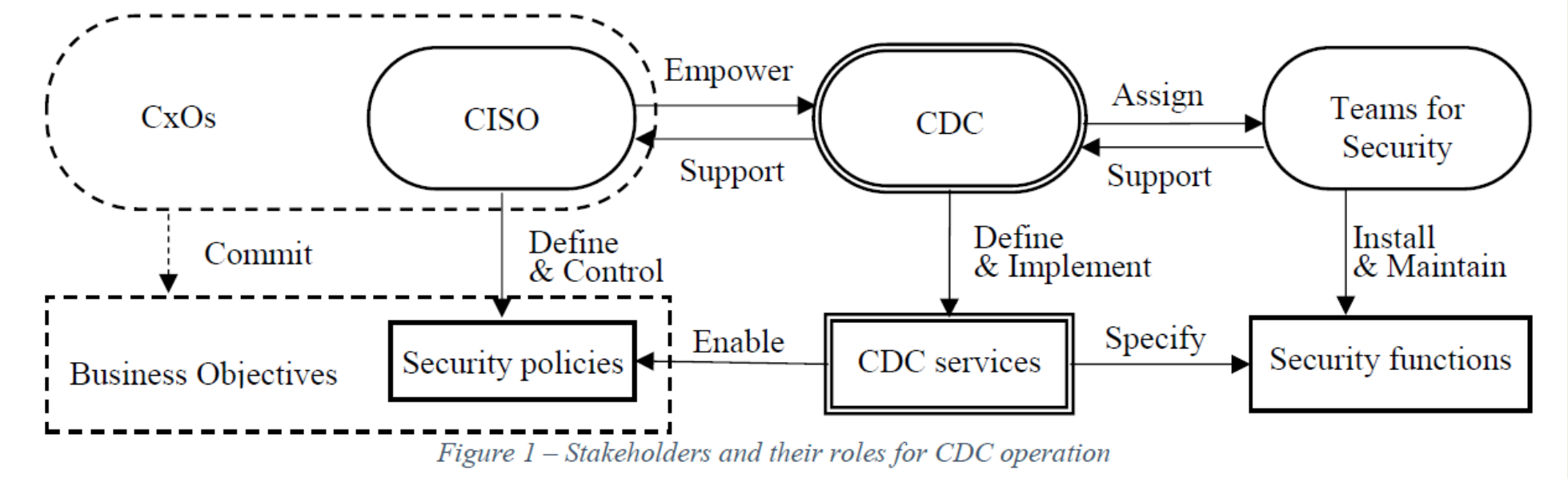


Figure 1 – Stakeholders and their roles for CDC operation

CxOs commit their business objectives.

CISO defines and controls security policies to manage cyber risks.

CDC is empowered by CISO to define and implement CDC services for enabling security policies.

CDC assigns resources to activate security functions which compose CDC services.

CDC is an entity, and the structures and names of organizations vary.

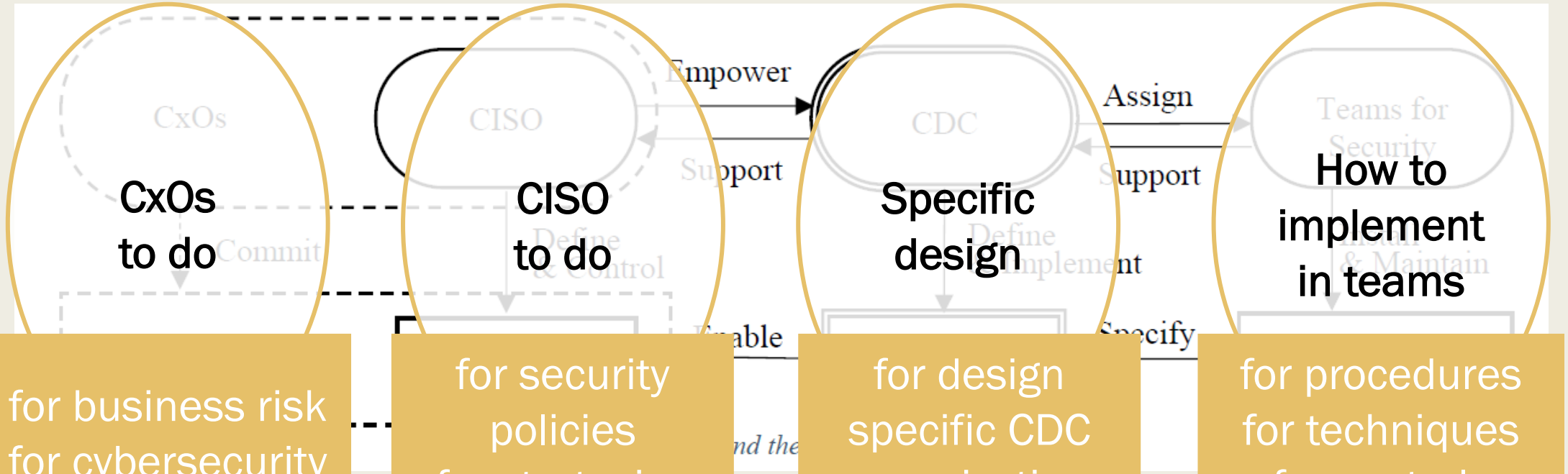
- It is not the purpose to build a division or unit with the name “CDC”. It is up to each organization to name the entity.
- Depending on how security services have been implemented, the form and name of the CDC is vary among organizations.

X.1060 provides only a framework.

- X.1060 is only framework for the creation and operation of the CDC.
- It is necessary to utilize various existing documents in order to implement CDC services which is actually implemented in the organization.

Out of scope of X.1060

- Using any guidelines and documents for complement and specify X.1060.



FRAMEWORK FOR THE CREATION AND OPERATION OF A CYBER DEFENCE CENTRE

The framework

- Three processes to maintain security activities
- **Build – Management - Evaluation**

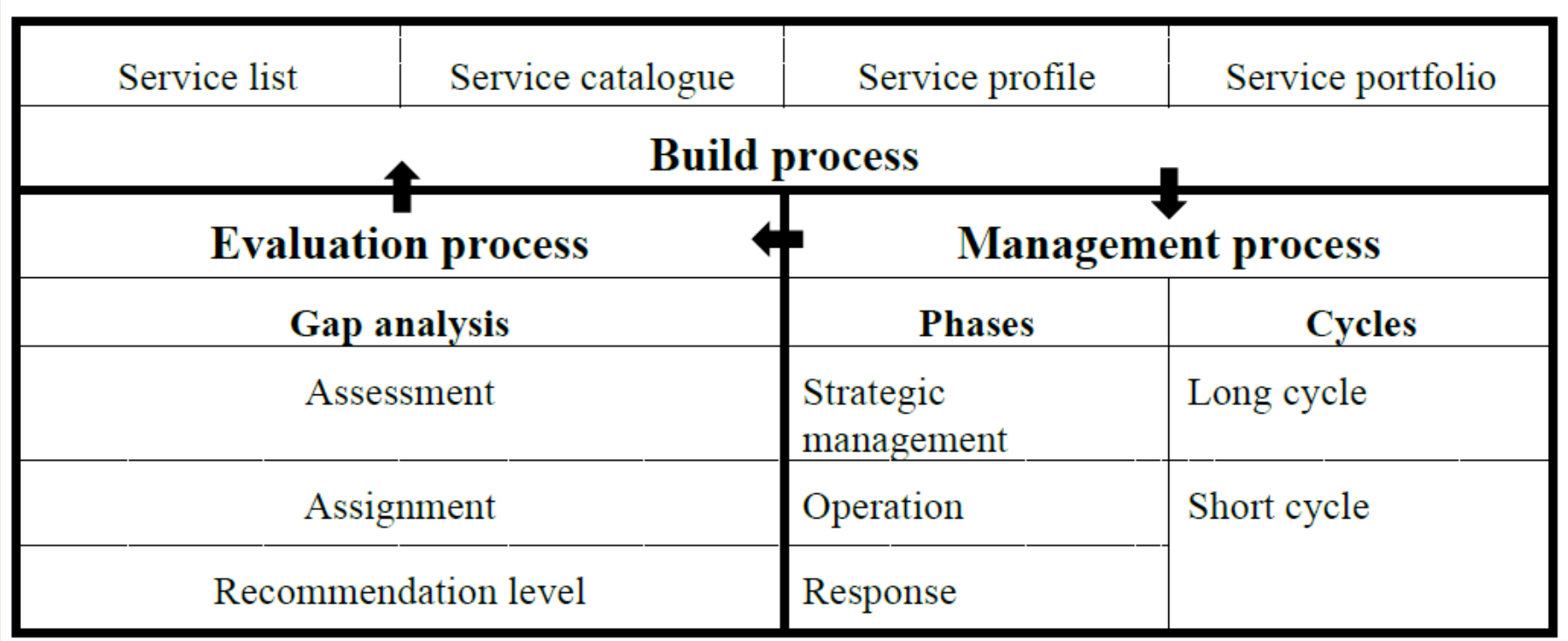


Figure 2 - Framework for the creation and operation of CDC

Build Process

Process

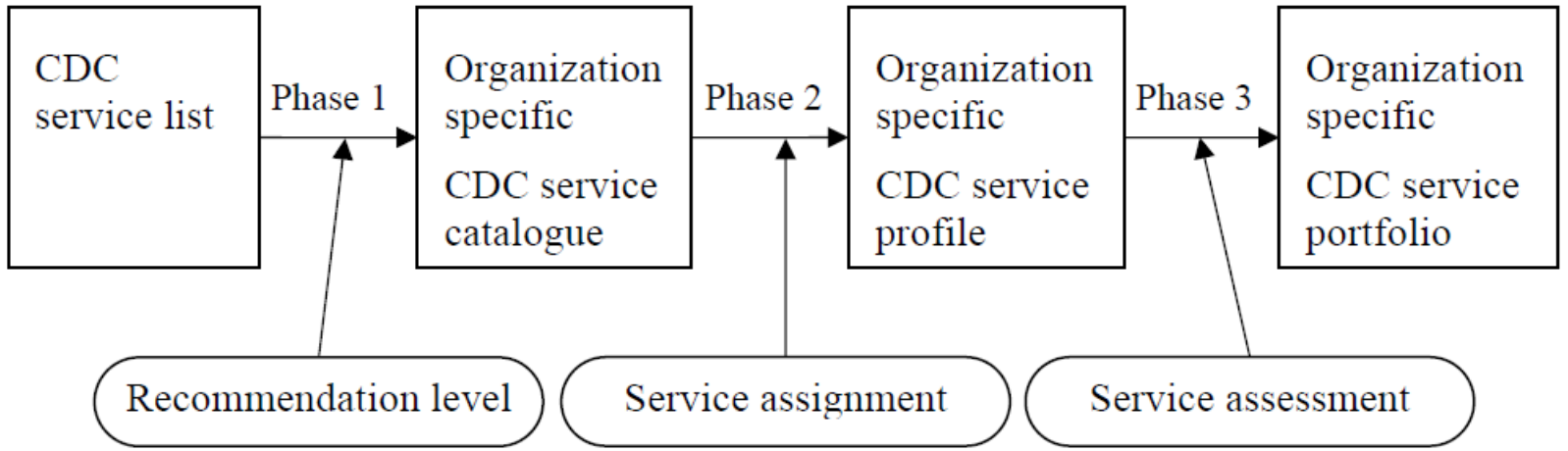
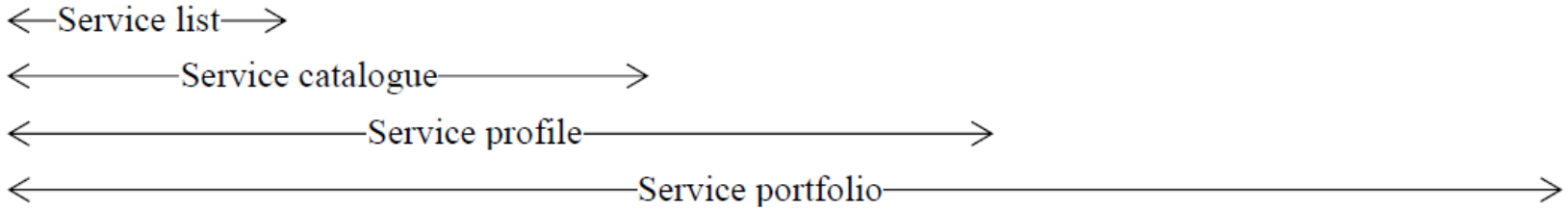


Figure 3 - Phases to build services for CDC

Output

Service	Recommendation level	Service assignment	Service score	
			As-is	To-be
Service ex.1	Basic	Insourcing (AB dept.)	3	5
Service ex.2	Standard	Outsourcing (Z-MSSP)	2	4
Service ex.3	Advanced	Unassignable	1	2



CDC service category

Service category		Number of services
A	Strategic management of CDC	13
B	Real-time analysis	4
C	Deep analysis	4
D	Incident response	7
E	Check and evaluate	9
F	Collection, analyzing and evaluating threat intelligence	5
G	Development and maintenance of CDC platforms	13
H	Supporting internal fraud response	2
I	Active relationship with external parties	7

CDC service list

A	**Strategic management of CDC**
A-1	Risk management
A-2	Risk assessment
A-3	Policy planning
A-4	Policy management
A-5	Business continuity
A-6	Business impact analysis
A-7	Resource management
A-8	Security architecture design
A-9	Triage criteria management
A-10	Counter measures selection
A-11	Quality management
A-12	Security audit
A-13	Certification
B	**Real-time analysis**
B-1	Real-time asset monitoring
B-2	Event data retention
B-3	Alerting & warning
B-4	Handling inquiry on report
C	**Deep analysis**
C-1	Forensic analysis
C-2	Malware sample analysis
C-3	Tracking & tracing
C-4	Forensic evidence collection
D	**Incident response**
D-1	Incident report acceptation
D-2	Incident handling
D-3	Incident classification
D-4	Incident response & containment
D-5	Incident recovery
D-6	Incident notification
D-7	Incident response report
E	**Check and evaluate**
E-1	Network information collection
E-2	Asset inventory
E-3	Vulnerability assessment
E-4	Patch management
E-5	Penetration test
E-6	Defence capability against APT attack evaluation
E-7	Handling capability on cyber attack evaluation
E-8	Policy compliance
E-9	Hardening

F	**Collecting, analyzing and evaluating threat intelligence**
F-1	Post mortem analysis
F-2	Internal threat intelligence collection and analysis
F-3	External threat intelligence collection and evaluation
F-4	Threat intelligence report
F-5	Threat intelligence utilization
G	**Development and maintenance of CDC platforms**
G-1	Security architecture implementation
G-2	Basic operation for network security asset
G-3	Advanced operation for network security asset
G-4	Basic operation for endpoint security asset
G-5	Advanced operation for endpoint security asset
G-6	Basic operation for cloud security products
G-7	Advanced operation for cloud security products
G-8	Deep analysis tool operation
G-9	Basic operation for analysis platform
G-10	Advanced operation for analysis platform
G-11	Operates CDC systems
G-12	Existing security tools evaluation
G-13	New security tools evaluation
H	**Supporting internal fraud response**
H-1	Internal fraud response and analysis support
H-2	Internal fraud detection and reoccurrence prevention support
I	**Active relationship with external parties**
I-1	Awareness
I-2	Education & training
I-3	Security consulting
I-4	Security vendor collaboration
I-5	Collaboration service with external security communities
I-6	Technical reporting
I-7	Executive security reporting

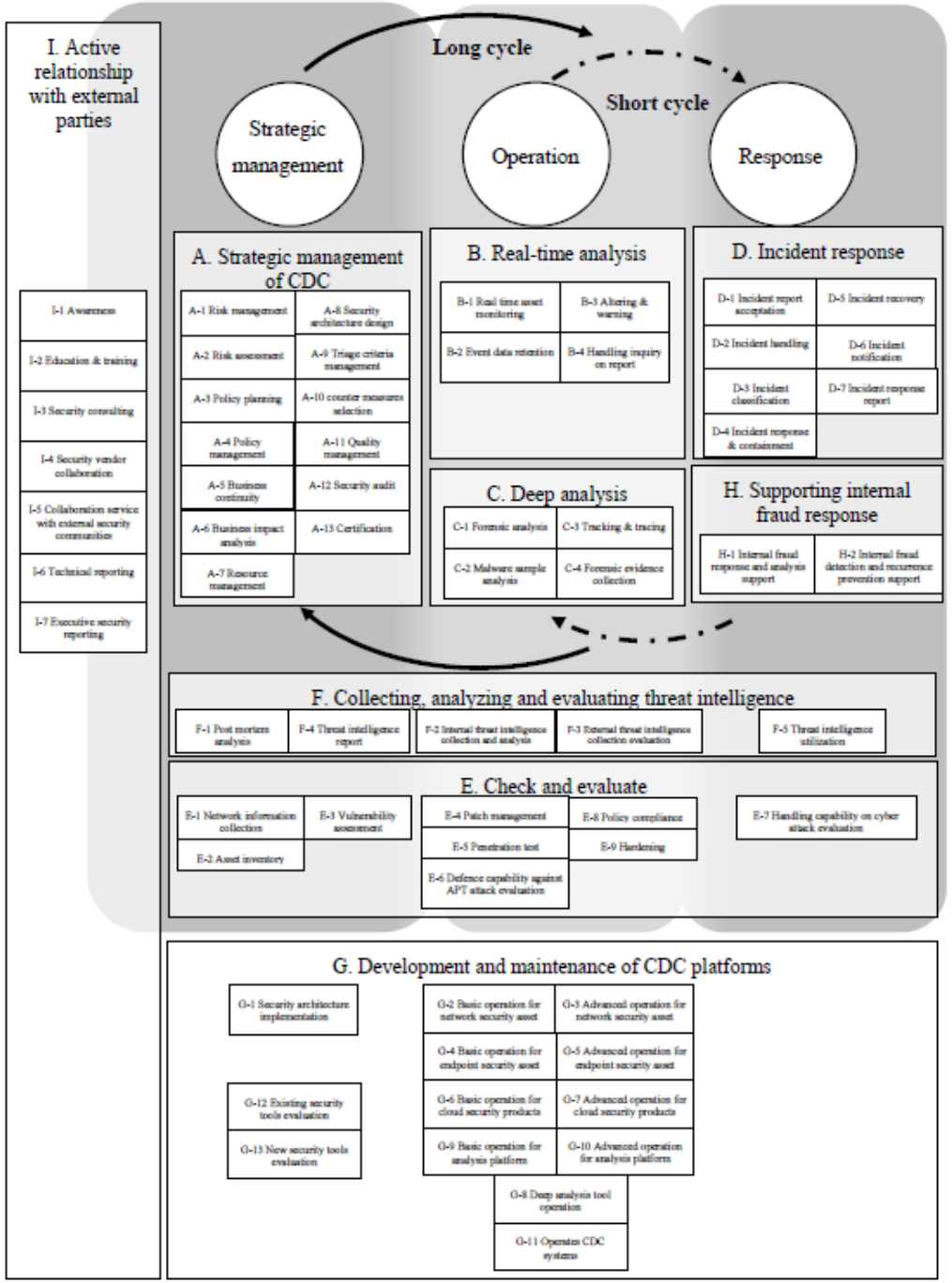


Figure 8 - CDC service categories

HOW CAN AFRICAN NATIONS IMPLEMENT CDC

Before anything!
“Leadership The German Way”

- You build the story for the decision makers!
- And it doesn’t start by the word assessment!
- This is a LEADERSHIP ACT
- And it starts with the Story
- STORY =

NARRATIVE

+

BACK TO BACK AGREEMENTS WITH THE CONSTITUENCIES THAT CAN CONTRIBUTE TO THE NARRATIVE!

What is at stake at organizations level?

- Organizations = not only government! Think your private sector!
- The intention of the CDC framework is to provide a common language to elevate the bar of the security services organization
- This is an answer to several issues
  - *Lack of a formal normative common language*
  - *Lack of executive understanding and engagement*
  - *SOC and others are too operational and not enough business level*
  - *Fractalization of organizations*

The Narrative is a TRANSFORMATION Narrative
“CDC is about elevating and harmonizing our security services portfolio to better answer our business needs”

The ‘astuce’ is that X.1060 is ‘external’ to the organization so it blocks internal politicking

What is at stake at regional level: AFRICA

- If tomorrow a new Wannacry explodes
  - *and the world got VERY LUCKY with Wannacry it could have been MUCH worse*
- Today what are the chances that all African countries are able to engage ALL the services capabilities of ALL their constituencies across the continent?
  - *National entities, private sector, foreign private sector, service providers, etc.*
  - *?*
- Like in any place in the world probably very complicated
- CDC for Africa is a common language to give a minimal first condition to allow one aspect of a truly joint regional answer

The narrative is a REGIONAL HARMONISATION narrative
“CDC sets a common foundation and language at the right level of all our organization to improve collaboration, cooperation and the continent resiliency”

How to create? Build Process

Making the catalogue

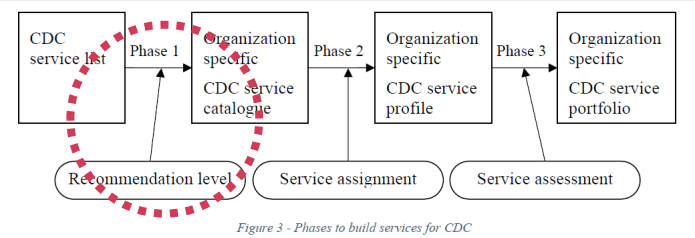


Figure 3 - Phases to build services for CDC

Weight	Description
Unnecessary	Services deemed unnecessary
Basic	Minimum services to be implemented
Standard	Services that are generally recommended for implementation
Advanced	Services required to achieve a higher-level CDC cycle
Optional	Services arbitrarily selected according to the expected form of CDC

Making the profiles

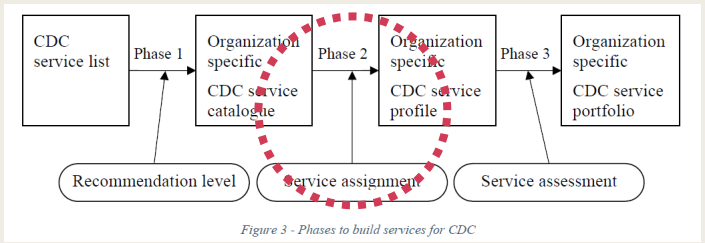


Figure 3 - Phases to build services for CDC

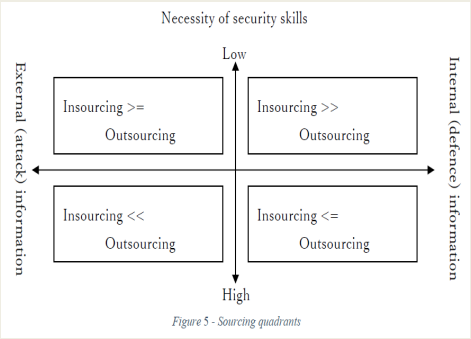


Figure 5 - Sourcing quadrants

Making the portfolio

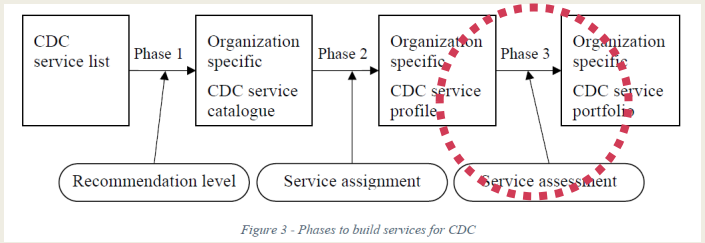


Figure 3 - Phases to build services for CDC

For insource:

Documented operation is authorized by CISO or other organizational director who has proper responsibilities	+5 points
Operation is documented and others can play the role of existing operator	+4 points
Operation isn't documented and others can play the partial role of existing operator temporarily	+3 points
Operation isn't documented and the existing operator can play role	+2 points
Operation isn't working	+1 point
Decided not to implement by insourcing	N/A

How to manage? Management Process

3 Phases
- Strategic management
- Operations
- Response

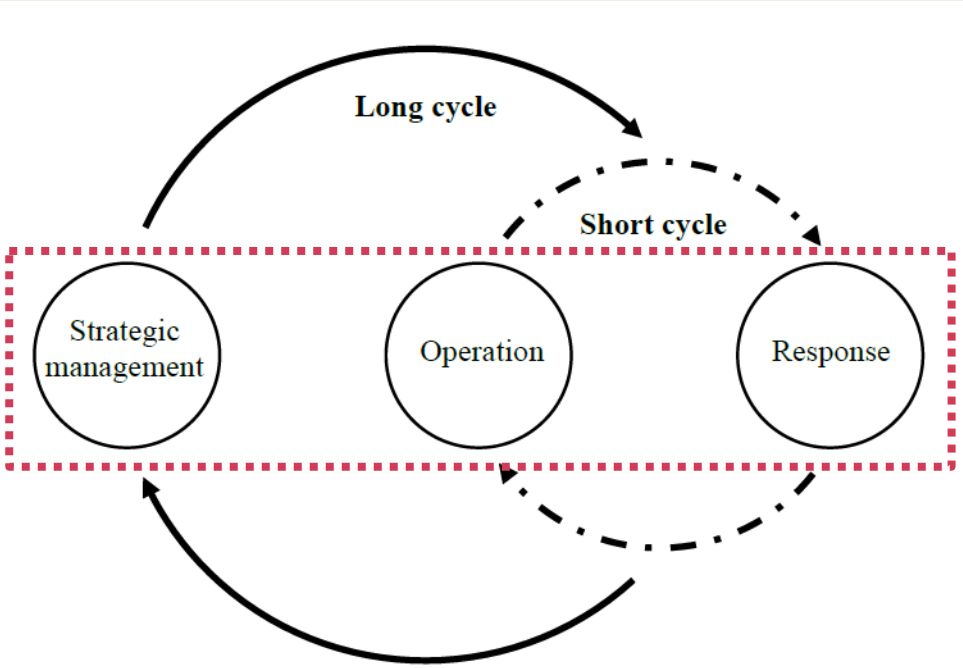
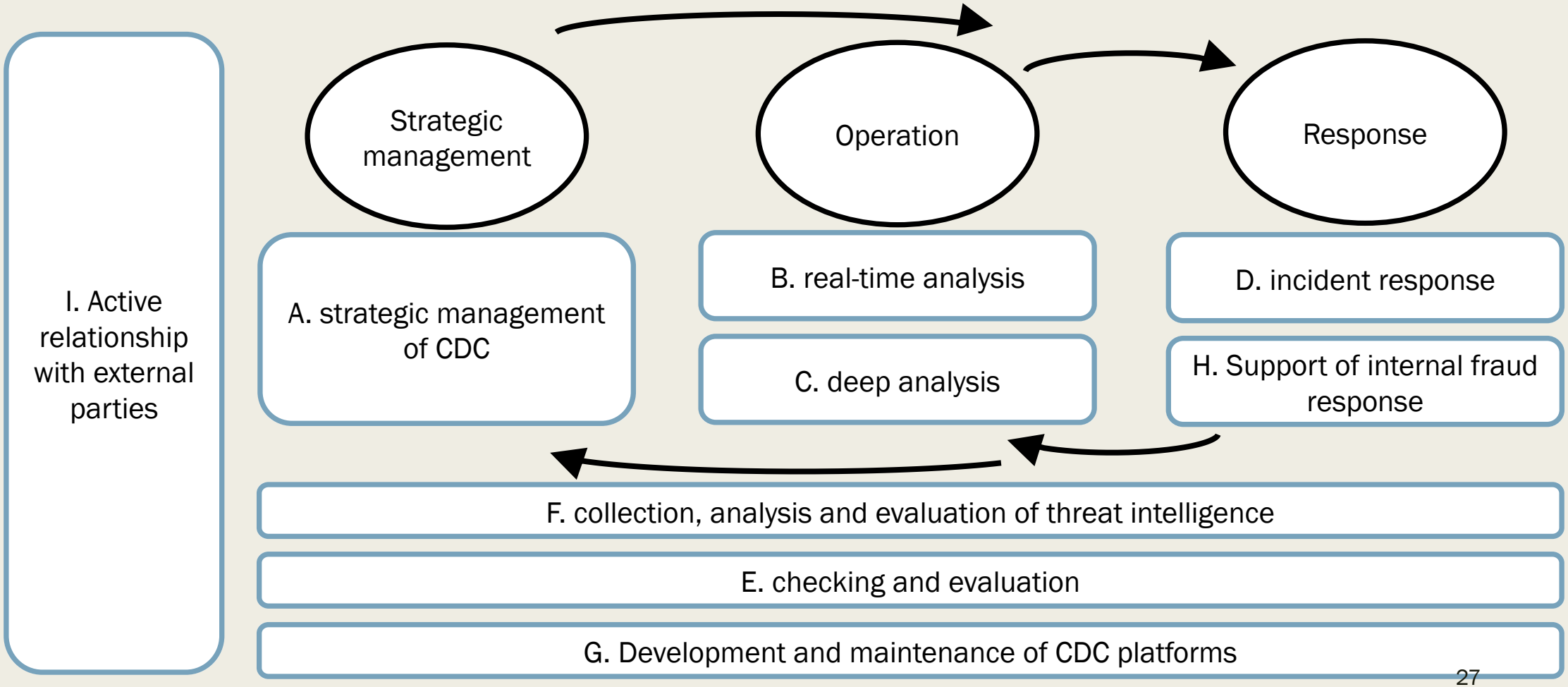


Figure 6 - CDC management process

2 Cycles
- Short
- Long

Mapping service categories and “Management process”.



OUTCOME FROM SG17 MEETING

What happened

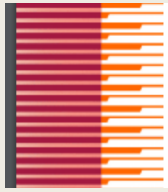
- Q3/17 met and reviewed 2 contributions for X.sup-cdc from editors
  - *One concentrating on the base text and the tutorial*
  - *One concentrating on next steps*
- A joint Q3/SG17AFR meeting
- Participation to SG17AFR meeting
- A great informal lunch with SG17AFR delegates (learnt a lot and fun)
- A very valuable CDC work-day on X.sup-cdc

Main outcomes

- Key progress on the layout of X.sup-cdc + content
- Great input from SG17AFR for the next questionnaire
- A lot of enthusiasm
  - *Need for a governance model*
  - *Need for an assessment model*
  - *Need for a certification approach*
  - *Need for detailed implementation (service templates, etc.)*
- But the bar of entry to go the next steps is contradicted by some other gaps elsewhere

The problem

- Provoking Statement
  - *“There is no international agreed consensus of a security architecture since X.800 (1991)”*
- We miss a context!
- SG17 worked hard since 5 years (CG-XSS, CG-SECAD, CG-WTSA-PREP, etc.)
  - *This already changed the national cybersecurity of some countries*
    - (incredible? But true!)
- Big important first success at WTSA20 in March 2022 on Resolution 50



WORLD TELECOMMUNICATION STANDARDIZATION ASSEMBLY
Geneva, 1-9 March 2022

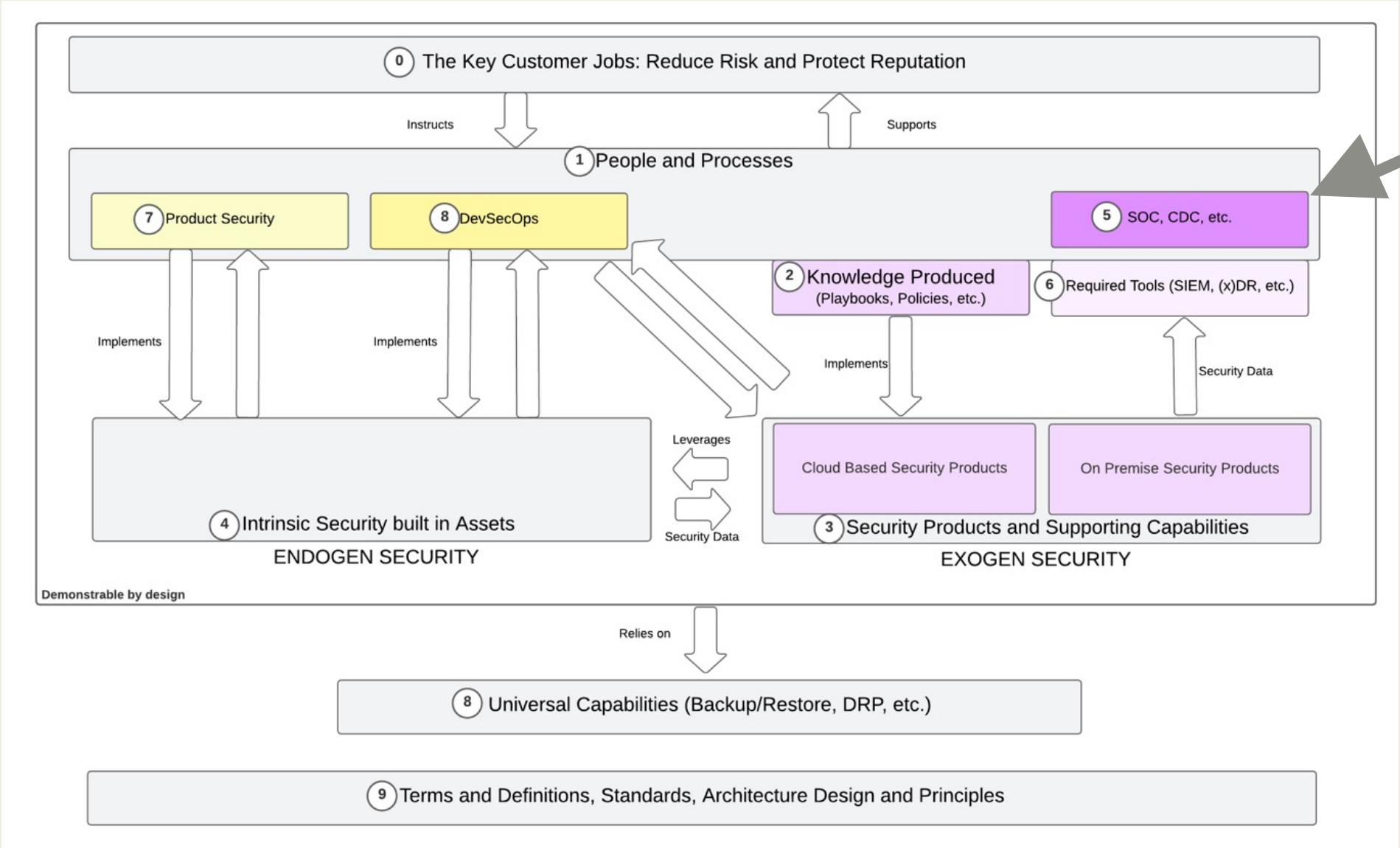
Resolution 50 – Cybersecurity

instructs Study Group 17

5 to define a general/common set of security capabilities for each phase of information system/network/application lifecycles, so that consequently security by design (security capabilities and features available by design) could be achieved for systems/networks/applications from day one;

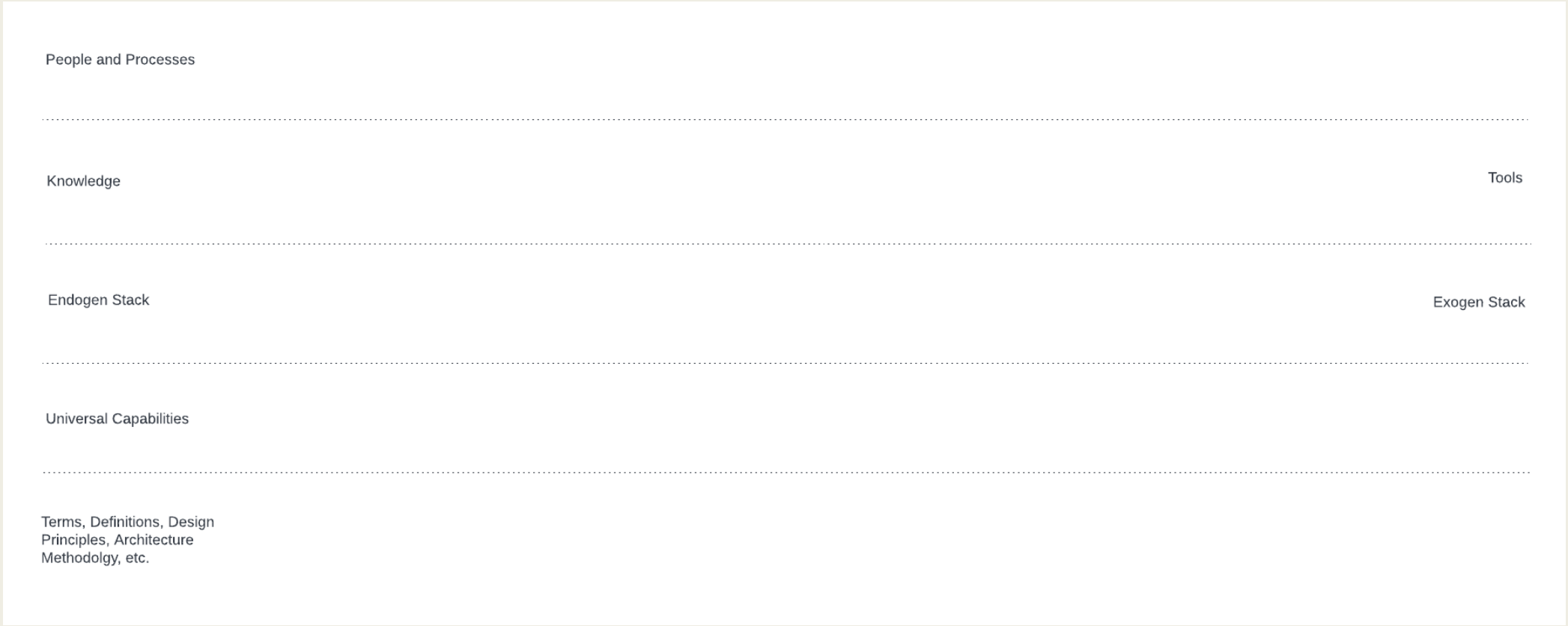
6 to design one or more security architecture reference frameworks with security functional components which could be considered as the basis of security architecture design for various systems/networks/applications in order to improve the quality of Recommendations on security,

The Quest for a new Context!
Current Candidate → An OSI model for Security-!



We are here on the map

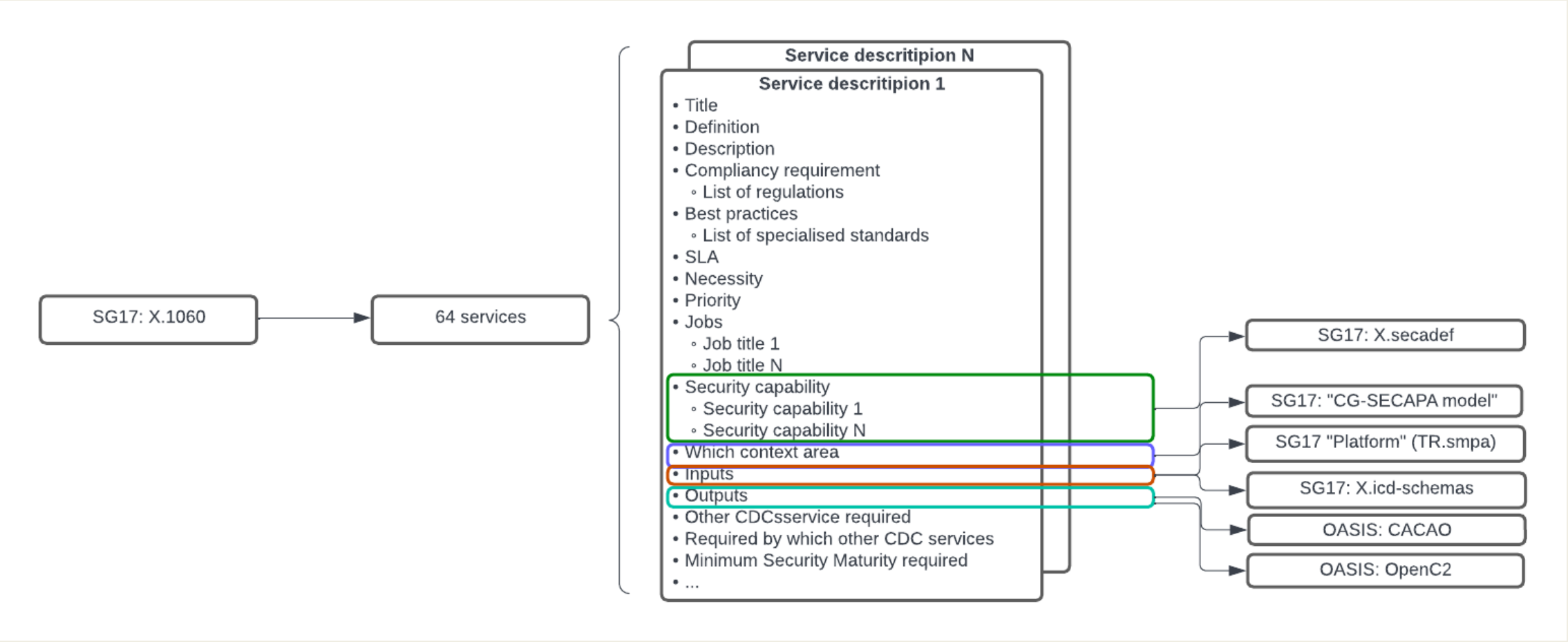
If you layer the candidate model (looks more and more like an OSI model)



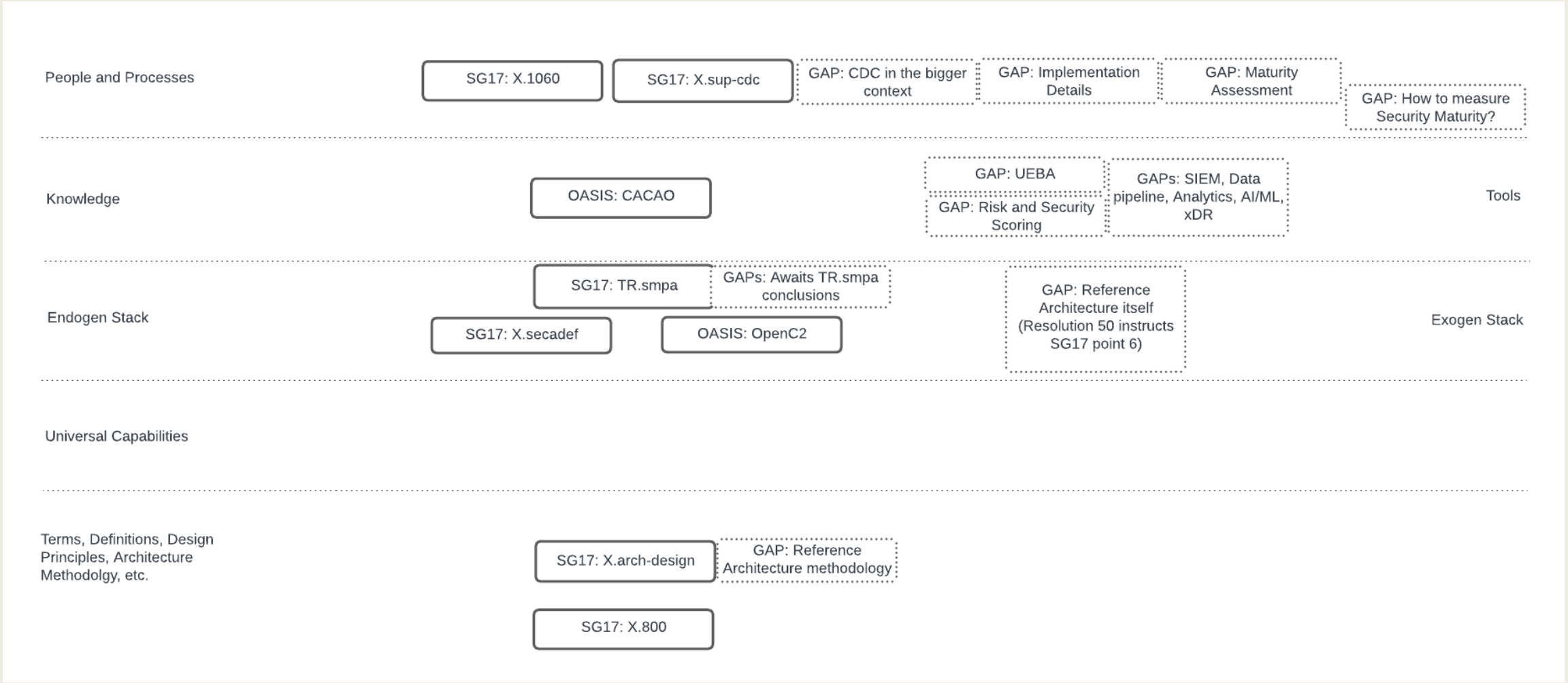
Mapping CDC


People and Processes
SG17: X.1060
SG17: X.sup-cdc
Knowledge
OASIS: CACAO
Tools
Endogen Stack
SG17: TR.smpa
SG17: X.secadef
OASIS: OpenC2
Exogen Stack
Universal Capabilities
Terms, Definitions, Design Principles, Architecture Methodolgy, etc.
SG17: X.arch-design
SG17: X.800

A service template shows a LOT of dependencies to the context



And a lot of gaps



My asks

- Give feedback – Nothing is perfect!
- Join the effort
- Bring **contributions** to the next SG17 meeting end of August
- Need contributions on the detailed description of some or all of your services
  - *do not share data you cannot share of course*
  - *Do not even try to map to CDC, just describe in your words what you have*
    - Title, Description, SLA
    - Input to the service (tools, data, etc.)
    - Output to the service (playbooks, policy suggestions, remediation, responses, etc.)
    - Dependencies (service X depends on service Y, service A inputs to service B)
    - List of security capabilities needed
    - Etc.

Thank you

X.1060 Editors	Mr. Arnaud TADDEI	Broadcom Inc.
	Mr. Shigenori TAKEI	NTT Corporation
	Mr. Shinji ABE	
Q3/17 Rapporteur	Ms. Miho NAGANUMA	NEC Corporation