

A successful usage of X.1060 by the industry

Arnaud Taddei – Global Security Strategist – Broadcom's Symantec Enterprise Division
X.1060 co-editor

Sharing an example

- Broadcom will show exactly how it is using
 - X.1060 and X.sup-cdc
 - and other SG17 outcomes
- To support its customers
- This is the story of the group CISO of a French multinational €34B revenue, 85 countries and acquiring one company ... per month!

The situation

- Customer had a CERT, multiple CSIRT, SOC, etc.
 - Obtained through acquisitions
- “They believed” they were covering their protection
- But they didn’t prevent 2 huge ransomware attacks
 - They nearly lost an MVNO of 30 years of business, €1.3B
 - By one backup link!
 - One of their subsidiary was completely damaged
 - The attacker used a specific security vendor machine as pivot of the attack!

The recognition

- This customer understood:
 - Their entities were bottom up
 - Were siloed
 - Didn't realize their blind spot
 - The security entity leaders behaved as 'prima donas'
- They recognized they needed another approach
 - Without realizing about X.1060 they called it CDC

Lucky!

- Their deputy group CISO attends a meeting where X.1060 is presented by co-editor
- He recognized the coincidence on terms:
 - Their requirements for a CDC
 - The term CDC defined by X.1060
- It took him 6 months to convince his peers to request
 - an executive advisory session
 - with co-editor X.1060
 - on the basis of customer/vendor relationships

Honoring the request

- Reused ALL the available materials of X.1060, X.sup-cdc
 - And more results of SG17
- Organized a 2 hours meeting with the group CISO direct reports
- Presented the materials step by step
 - The X.sup-cdc was a huge key factor of success

The feedback

- The customers recognized
 - The presentation addressed a 100%+ of their requirements
 - They learned a lot and it helped them prepare an internal retreat with all their leaders from SOC, CSIRT, CERT, etc.
 - They realized that
 - ‘we lost 6 months of work engaging consultancy firm XYZ’
 - They particularly appreciated that this is an external normative text
 - This is forcing their leaders to fight against an external force and not an internal force
- We invented the concept that X.1060, in executive advisory can be used as a ‘martyr’ Recommendation
 - People will resist but they fight an external input to their organization
 - And it is the winning approach because this is coming from an INTERNATIONAL CONSENSUS

Attached

- The anonymized exact materials used during the session



Conclusion

- This experiment confirmed that the approach taken is
 - Not only is correct
 - IT IS VALUABLE FOR THE INDUSTRY
 - IT SERVES its purpose!
- This is one more proof point of the relevance of X.1060
- Now we need to move to the next steps
 - (And we exposed to several other customers!)
- Broadcom's Symantec Enterprise Division
 - Proposed a first Revision of X.1060
 - Proposed a new Recommendation to recognize the relationships with FIRST





Can X.1060 help the <CUSTOMER NAME> on its CDC strategy?

Strategy approaches

April 11th, 2023
Arnaud Taddei – Global Security Strategist

<CUSTOMER-NAME> – X.1060/CDC – Proposed Agenda

- 10:00 - ... : Introductions
: <CUSTOMER-NAME> strategy vs its CDC
: Why X.1060
: What is X.1060 / What it is not
: Organizations feedback and what is at stake
: The next steps and the problems
: What are we doing with it
- ... 12:00 : Open discussion Potential Next Steps and wrap-up
- This is a workshop
➔ Interactive
➔ I may use other materials if needed
- This is your project and your workshop
➔ you define all the steps

Disclaimer:

- Symantec sold its MSSP to Accenture after the Broadcom acquisition
- This is a pure consultancy based on ITU-T SG17 strong engagement

<CUSTOMER-NAME> Strategies



What is your strategy?

Both internal and for your business

- Why do you want to create a CDC?
- Why now?
- What is it for you?
- How are you getting it off the ground?
- Risks of doing, Risks of not doing?
- How success looks like?

Disclaimer:

- Symantec sold its MSSP to Accenture after the Broadcom acquisition
- This is a pure consultancy based on ITU-T SG17 strong engagement

X.1060 Editors

Mr. Arnaud TADDEI

Broadcom Inc.

Mr. Shigenori TAKEI

NTT Corporation

Mr. Shinji ABE

Q3/17 Rapporteur

Ms. Miho NAGANUMA

NEC Corporation

Why X.1060 and CDC



ITU-T X.1060 Framework for the creation and operation of a Cyber Defence Center (CDC)

<https://www.itu.int/rec/T-REC-X.1060-202106-1>

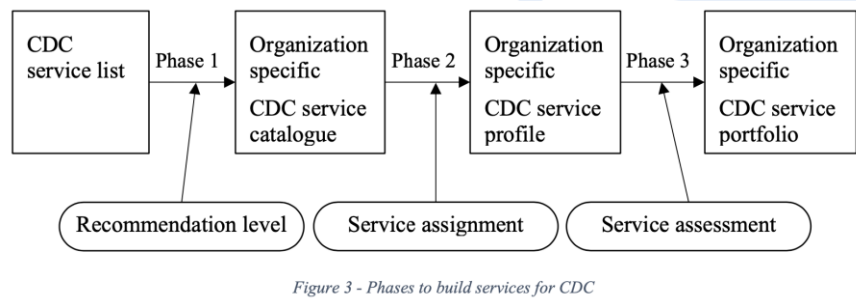


Figure 3 - Phases to build services for CDC

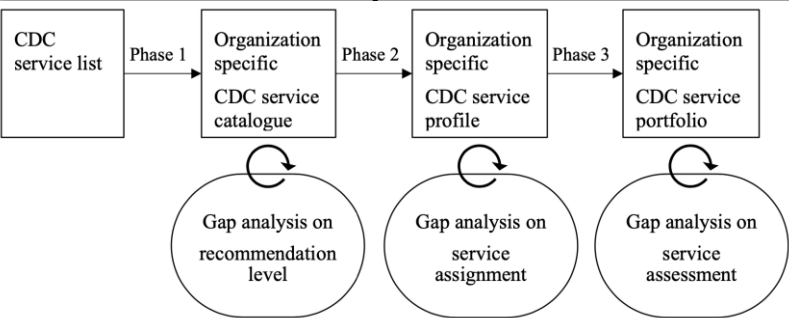
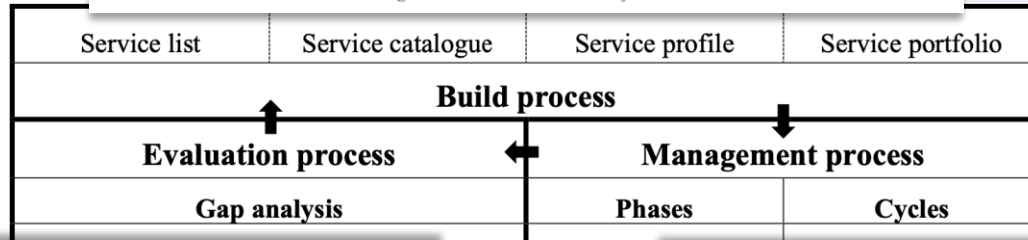


Figure 7 - CDC evaluation process

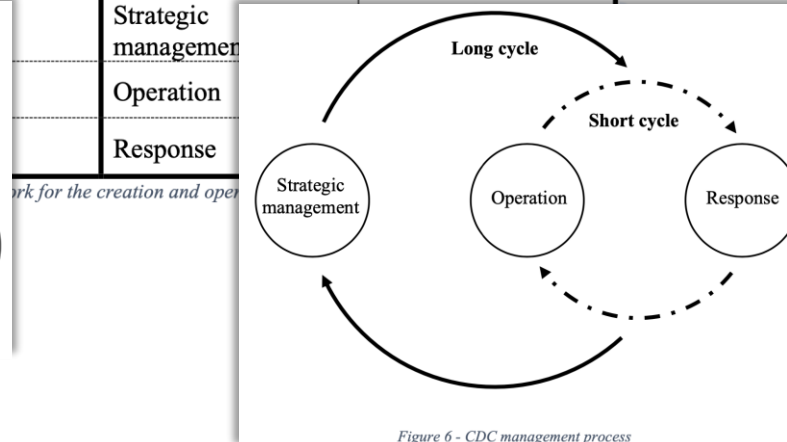


Figure 6 - CDC management process

Editors

Broadcom/Symantec

NTT Security for the ISOG-J

- 20+ Japan Security Providers

Critical contributions

NEC for the CRIC

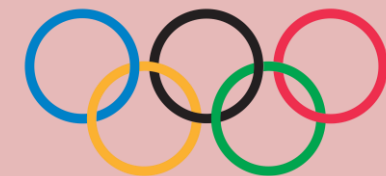
- 42 CISOs of top Japan business

Japan, Malaysia, China, US, UK,

Canada, Argentina, Oman, Kenya, . .

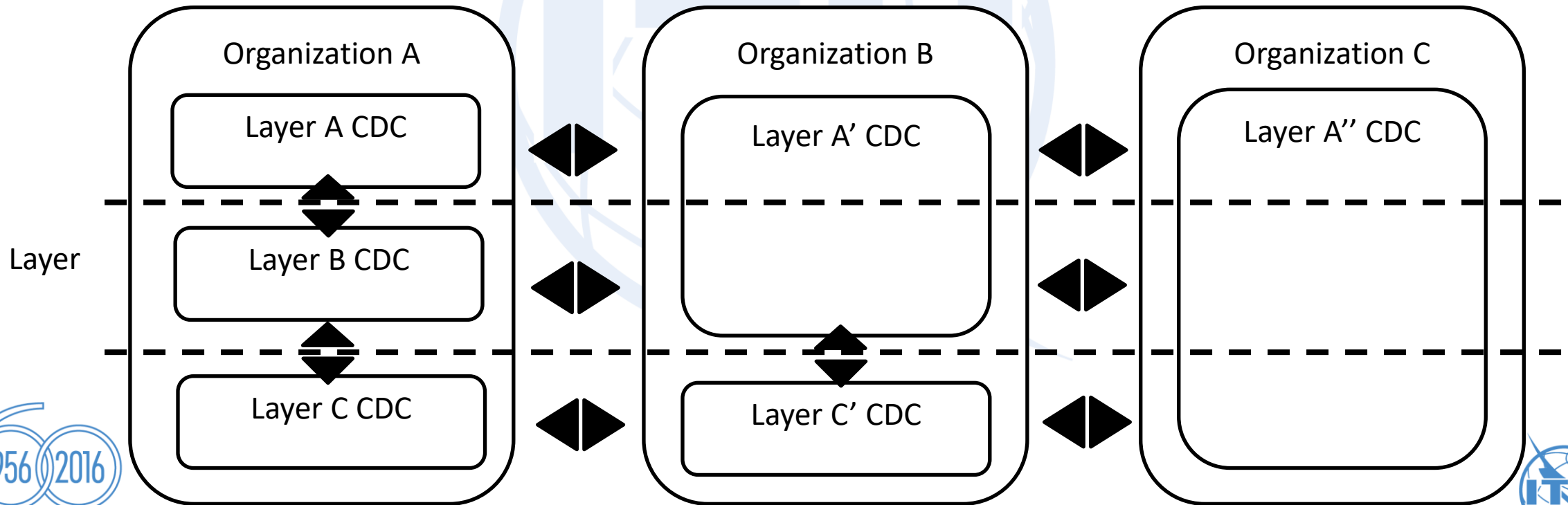
Used @

TOKYO 2020



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)



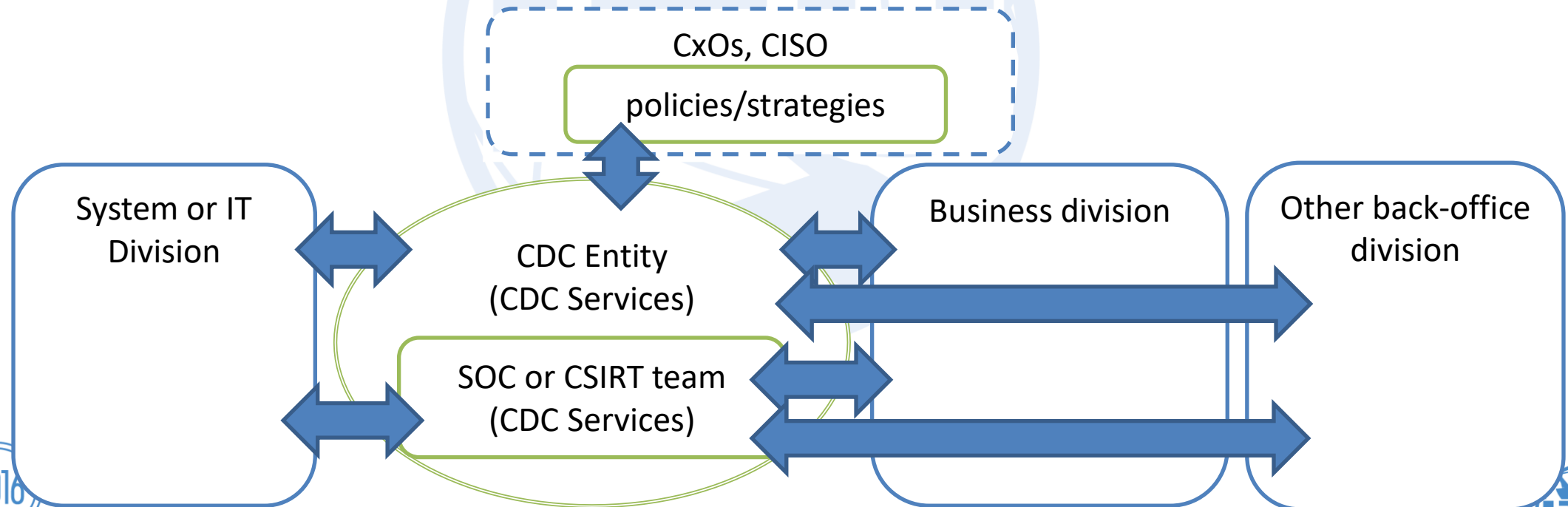
3. CISO decide to organize the CDC



4. Reference the X.1060 as a framework

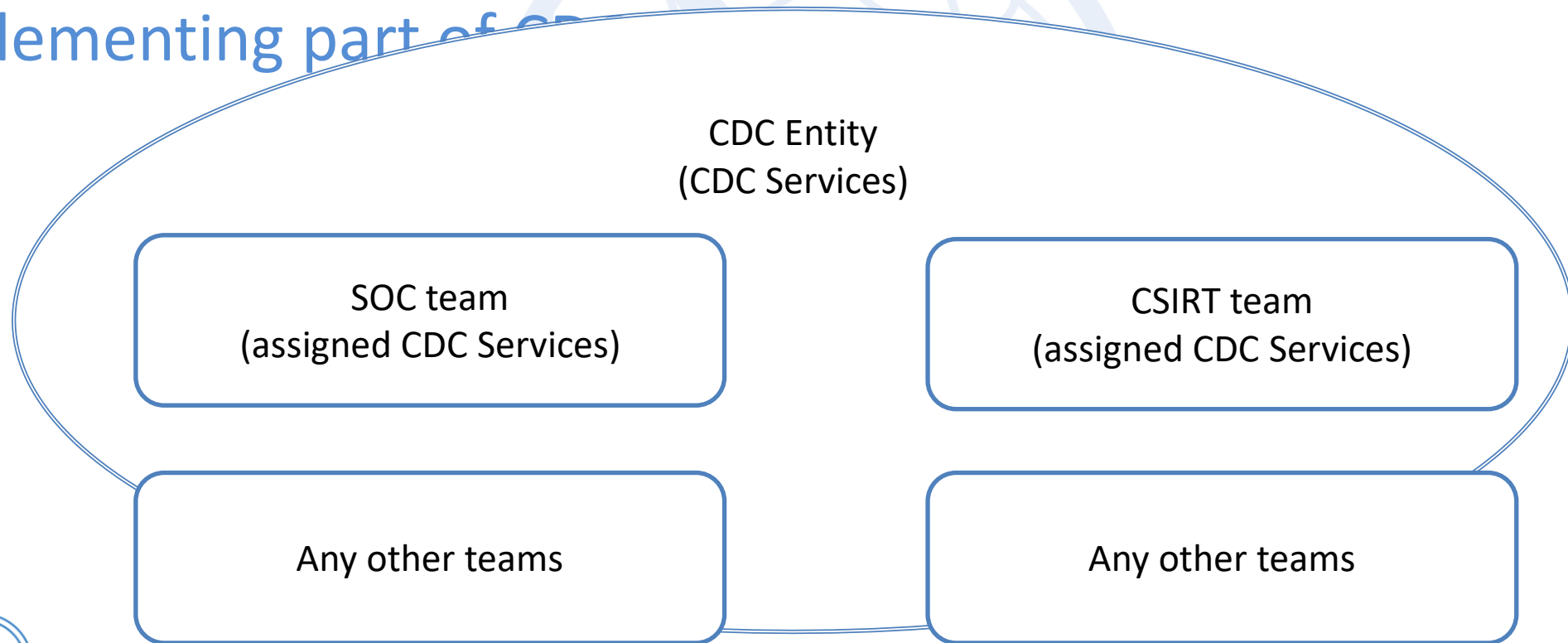
CDC provides security services which counter business risks.

- 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 “CSIRT” and implements CDC services, we can think of it as implementing part of CDC



What is X.1060



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

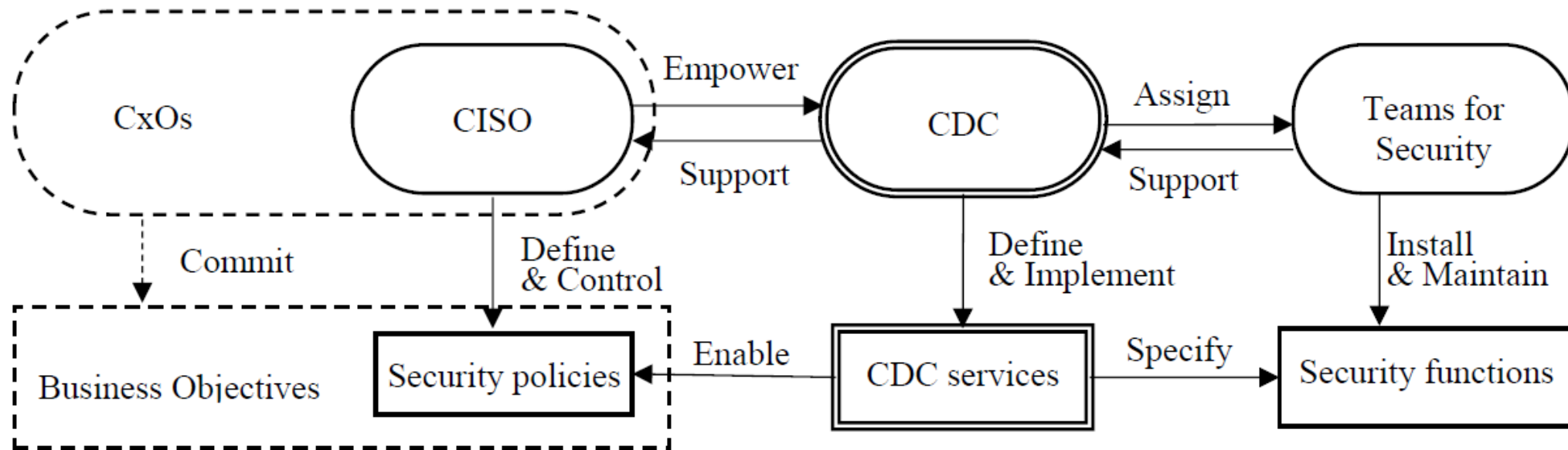


Figure 1 – Stakeholders and their roles for CDC operation

CDC in the organization

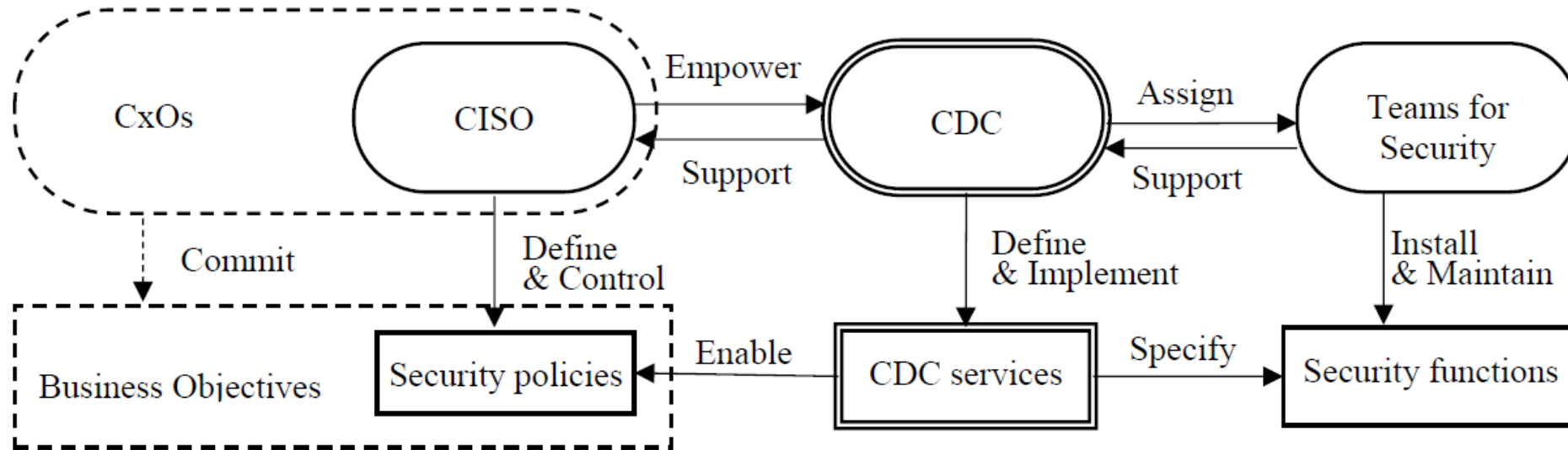


Figure 1 – Stakeholders and their roles for CDC operation

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

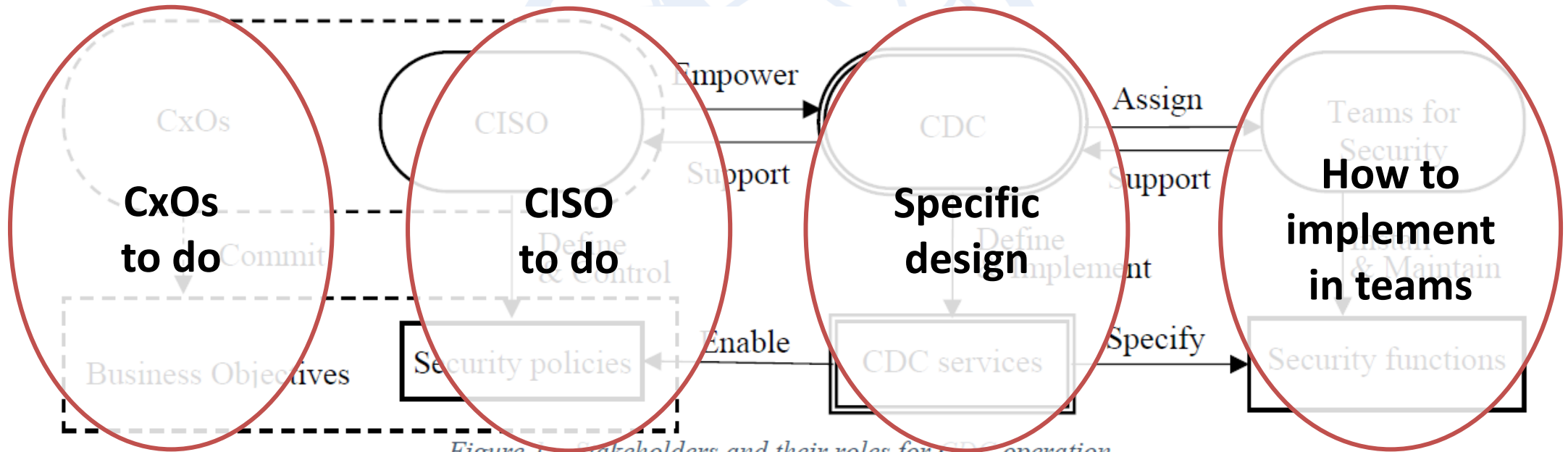
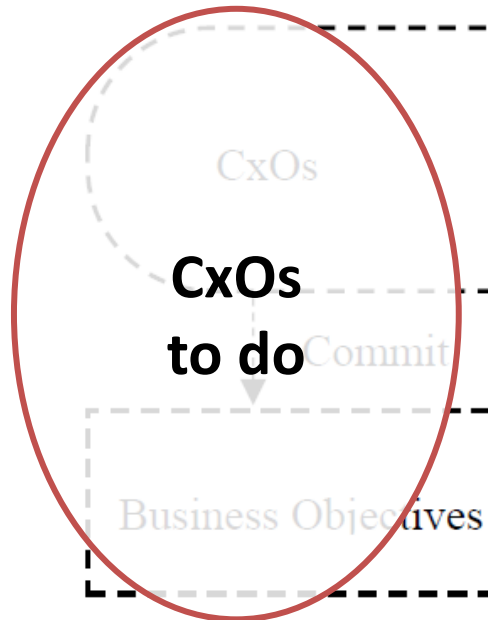


Figure 1 – Stakeholders and their roles for CDC operation

Out of scope of X.1060



X.1060 doesn't specify how the C-level board ("CxOs" in the diagram):

- recognizes the importance of cybersecurity
- assigns the CISO
- define the instructions to CISO
- decide to establish a CDC

Out of scope of X.1060

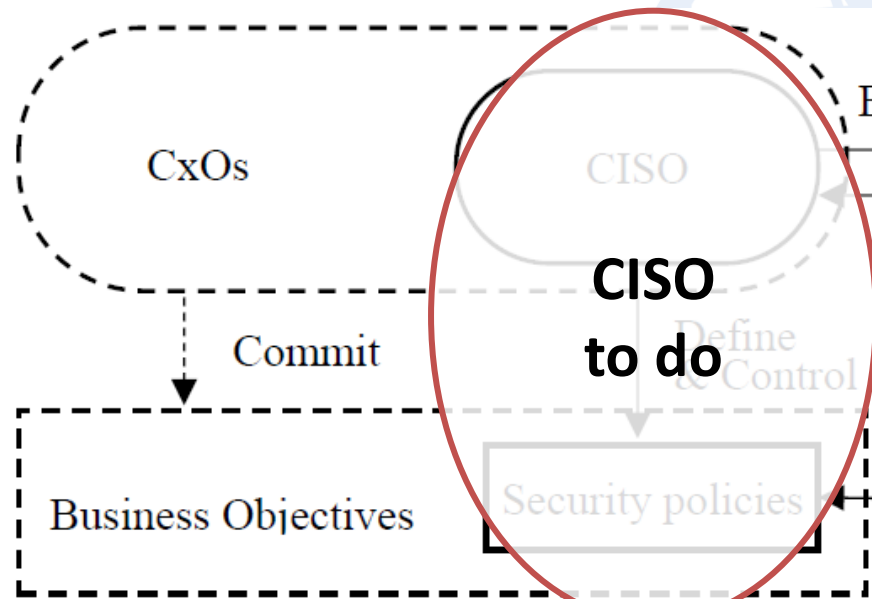


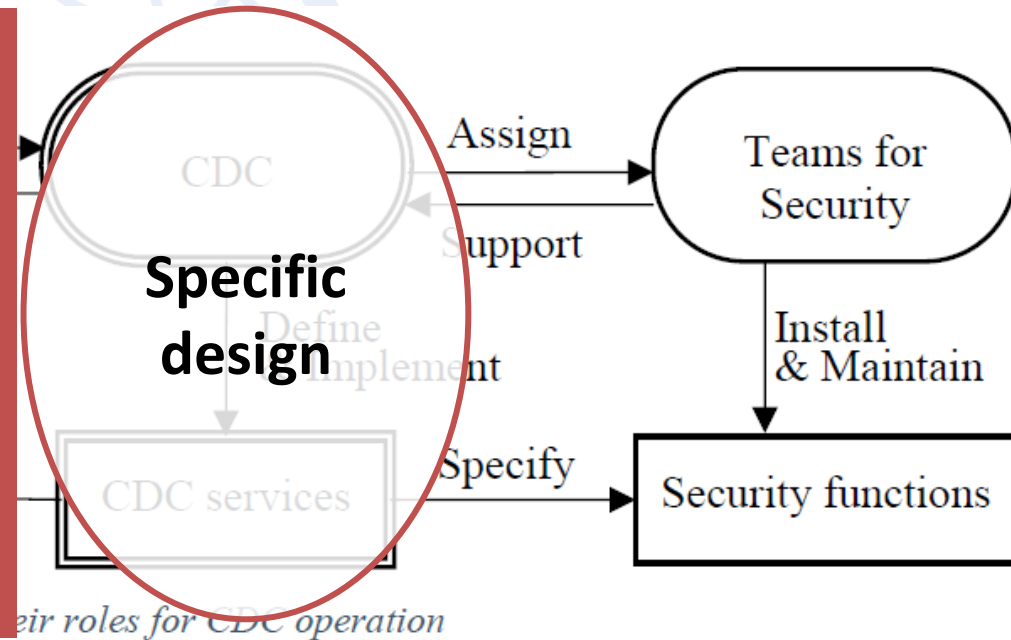
Figure 1 – Stakehold

X.1060 doesn't specify how the CISO:

- defines the security policies that result from both
 - considerations of the organization business environment and business objective
 - instructions by the C-level board
- creates awareness and promotes the establishment of a CDC to the C-level board

Out of scope of X.1060

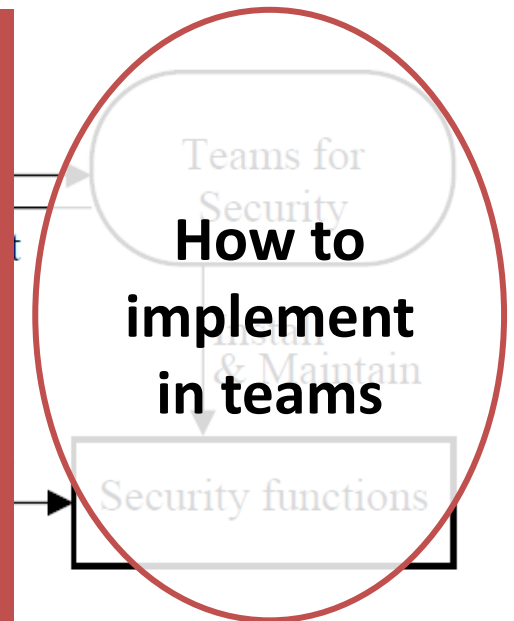
X.1060 doesn't specify the specific design of a CDC which is deployed in each organization.



Out of scope of X.1060

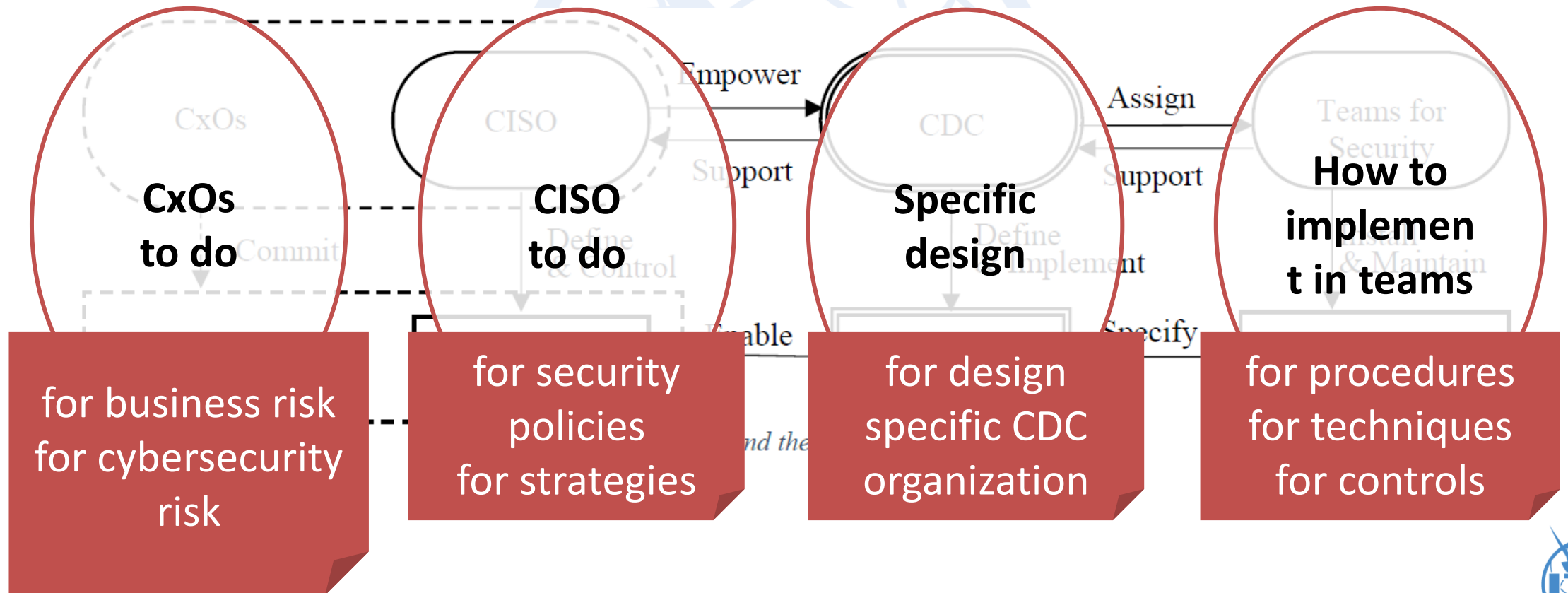
X.1060 doesn't specify how to implement the CDC services which were defined to do:

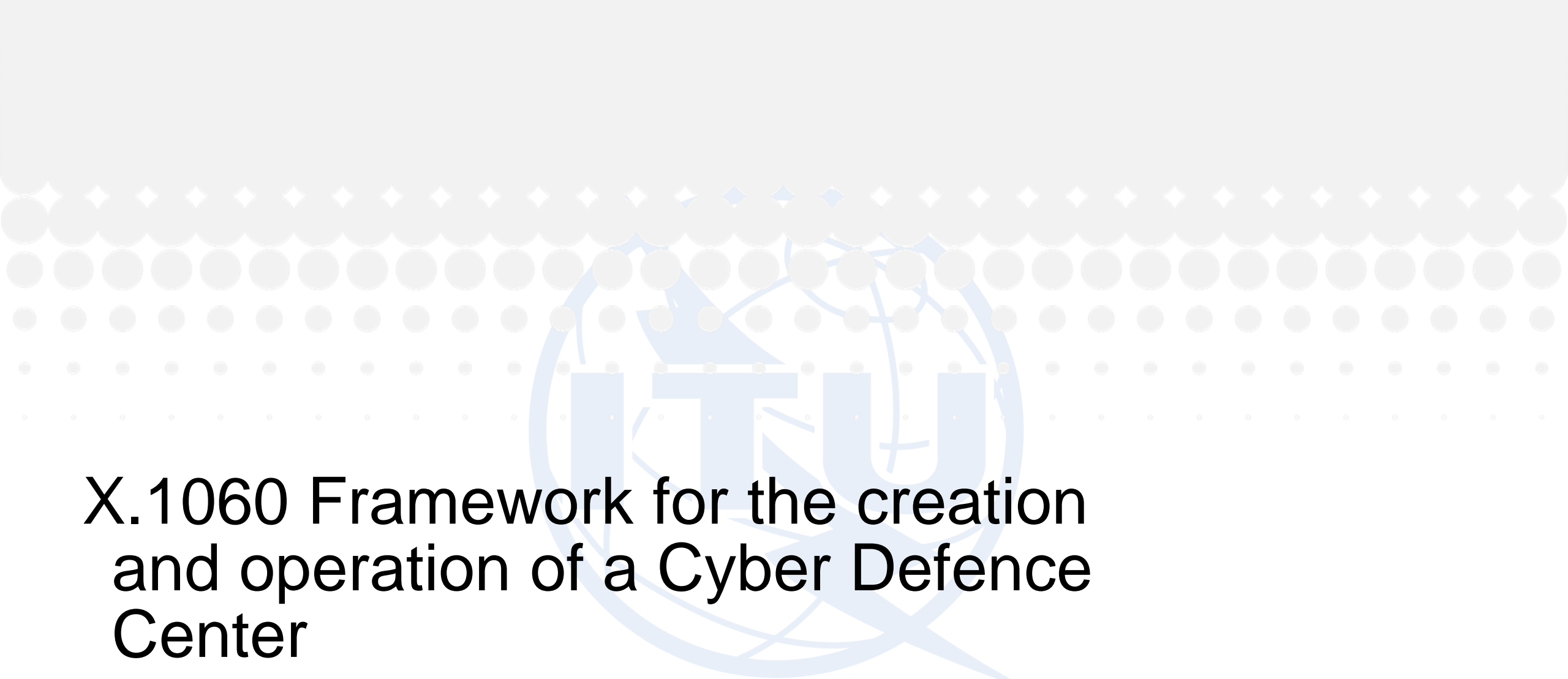
- what systems and processes are used
- scope each of the CDC services



Out of scope of X.1060

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





X.1060 Framework for the creation and operation of a Cyber Defence Center



The framework

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

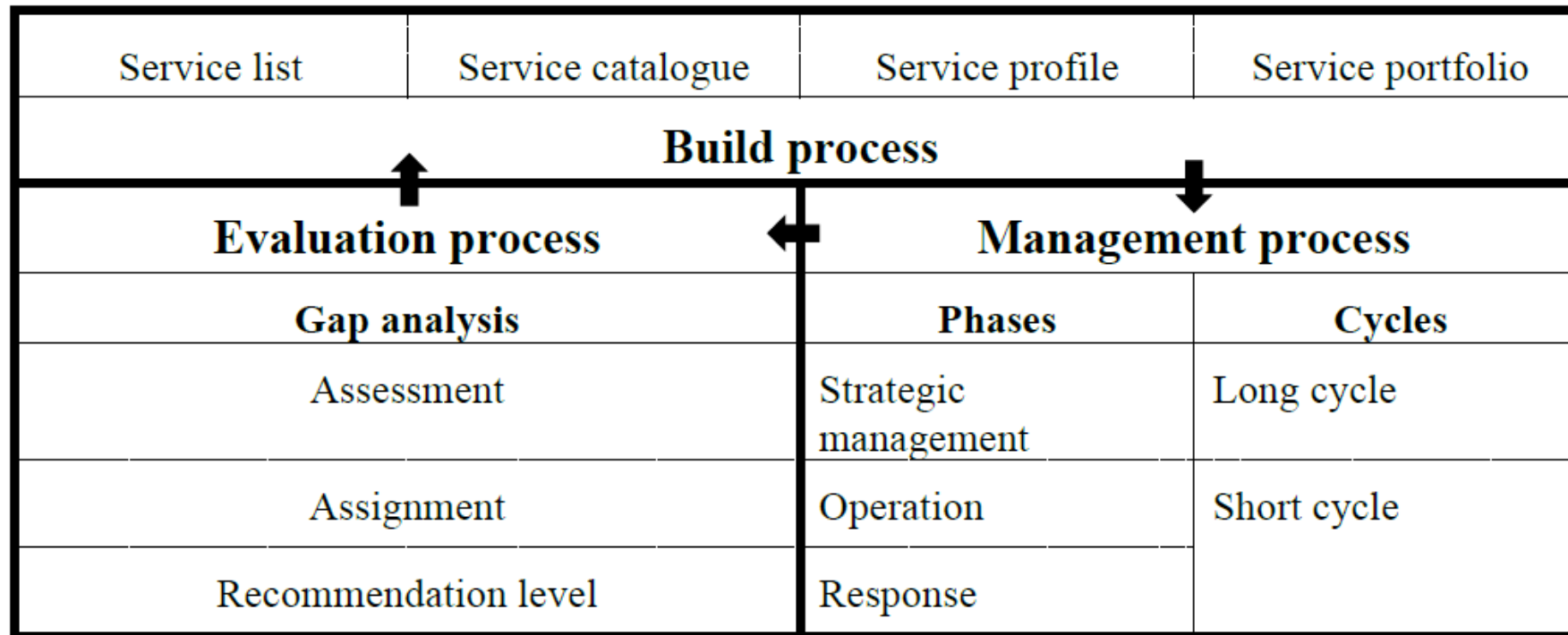


Figure 2 - Framework for the creation and operation of CDC

Build Process

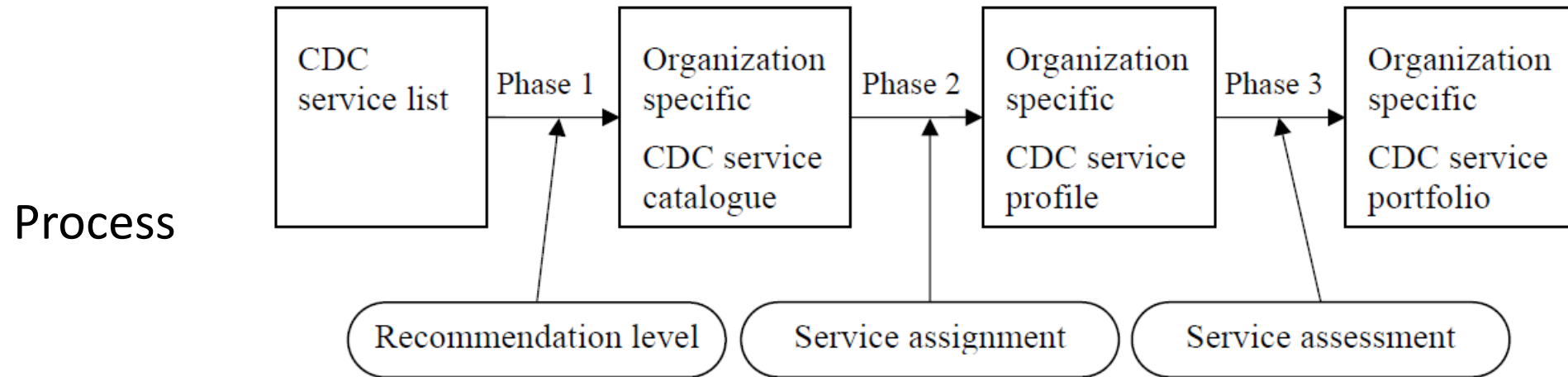


Figure 3 - Phases to build services for CDC

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 |

← Service list →

← Service catalogue →

← Service profile →

← Service portfolio →

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 | F | Collecting, analyzing and evaluating threat intelligence |
| A-1 | Risk management | F-1 | Post mortem analysis |
| A-2 | Risk assessment | F-2 | Internal threat intelligence collection and analysis |
| A-3 | Policy planning | F-3 | External threat intelligence collection and evaluation |
| A-4 | Policy management | F-4 | Threat intelligence report |
| A-5 | Business continuity | F-5 | Threat intelligence utilization |
| A-6 | Business impact analysis | G | Development and maintenance of CDC platforms |
| A-7 | Resource management | G-1 | Security architecture implementation |
| A-8 | Security architecture design | G-2 | Basic operation for network security asset |
| A-9 | Triage criteria management | G-3 | Advanced operation for network security asset |
| A-10 | Counter measures selection | G-4 | Basic operation for endpoint security asset |
| A-11 | Quality management | G-5 | Advanced operation for endpoint security asset |
| A-12 | Security audit | G-6 | Basic operation for cloud security products |
| A-13 | Certification | G-7 | Advanced operation for cloud security products |
| B | Real-time analysis | G-8 | Deep analysis tool operation |
| B-1 | Real-time asset monitoring | G-9 | Basic operation for analysis platform |
| B-2 | Event data retention | G-10 | Advanced operation for analysis platform |
| B-3 | Alerting & warning | G-11 | Operates CDC systems |
| B-4 | Handling inquiry on report | G-12 | Existing security tools evaluation |
| C | Deep analysis | G-13 | New security tools evaluation |
| C-1 | Forensic analysis | H | Supporting internal fraud response |
| C-2 | Malware sample analysis | H-1 | Internal fraud response and analysis support |
| C-3 | Tracking & tracing | H-2 | Internal fraud detection and reoccurrence prevention support |
| C-4 | Forensic evidence collection | I | Active relationship with external parties |
| D | Incident response | I-1 | Awareness |
| D-1 | Incident report acceptance | I-2 | Education & training |
| D-2 | Incident handling | I-3 | Security consulting |
| D-3 | Incident classification | I-4 | Security vendor collaboration |
| D-4 | Incident response & containment | I-5 | Collaboration service with external security communities |
| D-5 | Incident recovery | I-6 | Technical reporting |
| D-6 | Incident notification | I-7 | Executive security reporting |
| 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 | | |

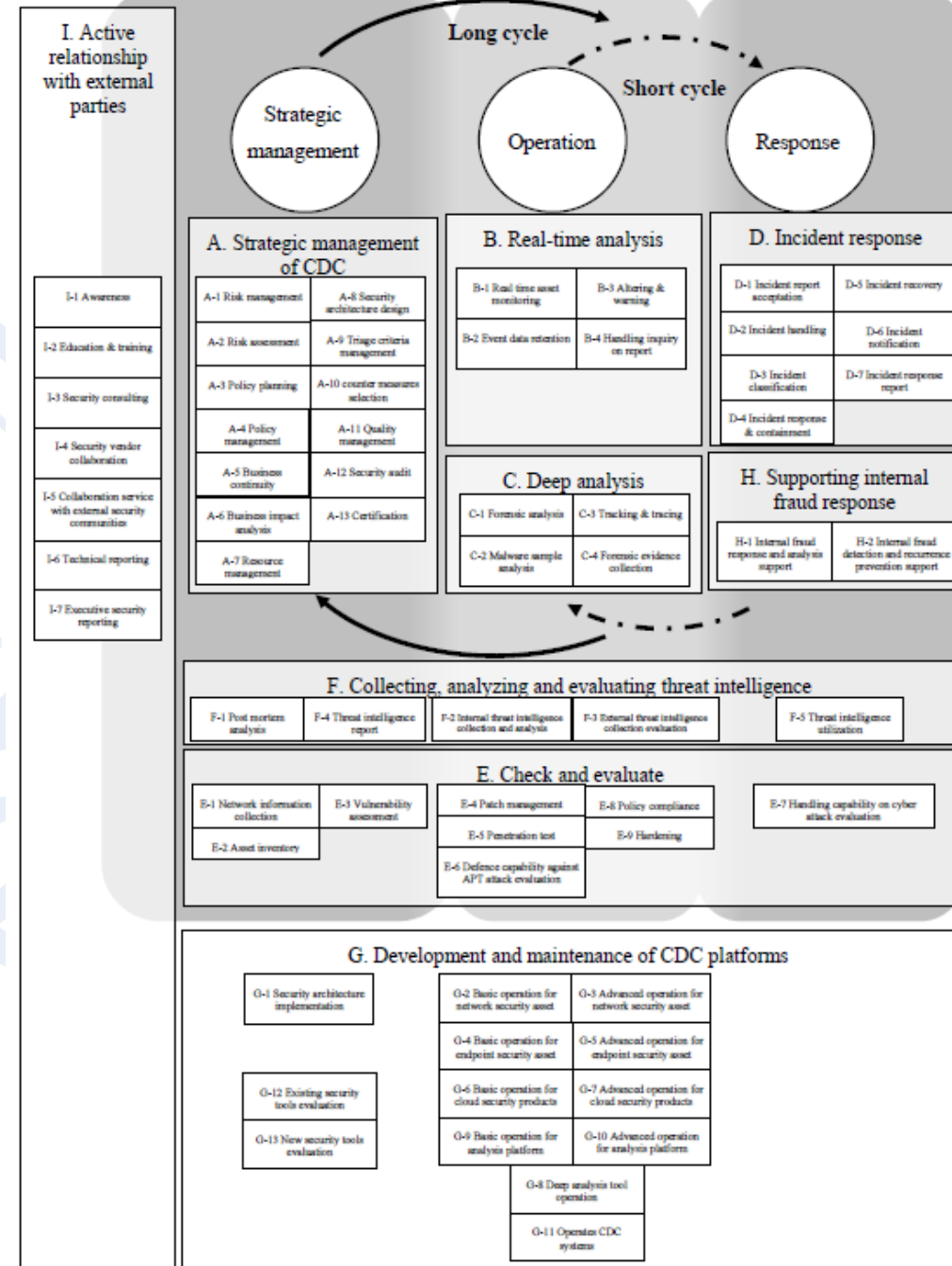


Figure 8 - CDC service categories

Build process

Phase 1: Making a catalogue

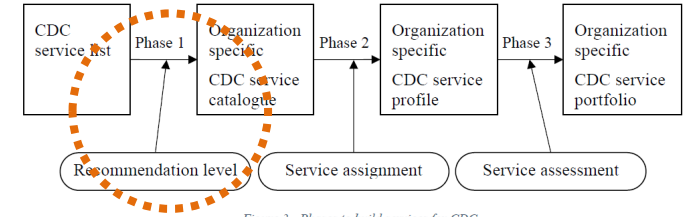


Figure 3 - Phases to build services for CDC

- CDC services from ITU-T X.1060 Annex - Select the following level
- You can also define and add services, if necessary

| 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 |



Build process

Phase 2: Making a profile

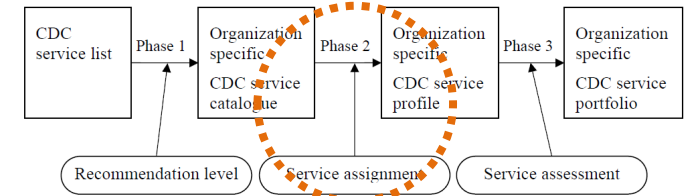


Figure 3 - Phases to build services for CDC

- Determine the specific organization to be responsible for providing each service in the catalogue
- The policy for assignments should be determined with reference to the following types;
- Below indicators can be considered types of insource or outsource.

| Type | Description |
|-------------|---|
| Insourcing | Services are provided by a team within the organization. The organization should specify the team in charge. |
| Outsourcing | Services are provided by a team outside of the organization. The organization should specify the outsourcer. |
| Combination | The organization uses insourcing and outsourcing together. A responsible team and a contractor should be specified by the organization. |
| Unassigned | Although the organization recognises a service, but there is no assignee in the organization. |

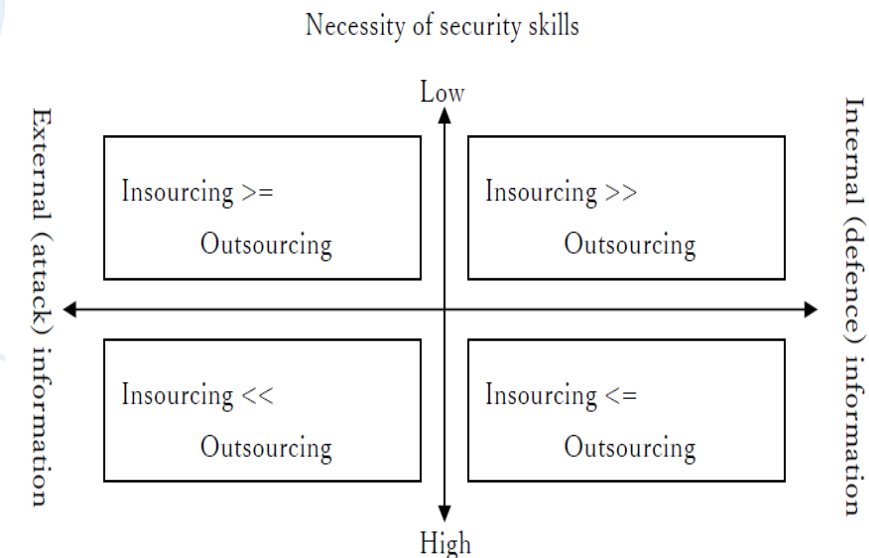


Figure 5 - Sourcing quadrants

Build process

Phase 3: Making a portfolio

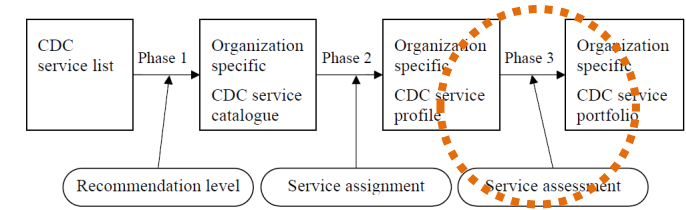


Figure 3 - Phases to build services for CDC

- Set the current and target scores according to the assignment status
- The following criteria can be used for reference in scoring

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 |

For outsource:

| | |
|--|-----------|
| Content of service and expected output are understood and their outputs are as expected | +5 points |
| Content of service and expected output are understood but their outputs aren't as expected | +4 points |
| Either content of service or expected output isn't understood | +3 points |
| Both content of service and expected output aren't understood | +2 points |
| Nether output nor report isn't reviewed | +1 point |
| Decided not to implement by outsourcing | N/A |

Management process - 3 phases

1. Strategic management phase

- Responsibility and accountability for all the strategic services relevant to definitions, design, planning, management, certification, etc. that ensure the long-term development of CDC

2. Operation phase

- The maintenance of the introduced framework
- The work at ordinary/usual time
- Typically includes routine activities e.g., analysis of incident detection, monitoring and maintenance of security response systems.
- The team is often called “Security Operation Center (SOC)”

3. Response phase

- An incident response should be executed when an event is detected by the analysis
- Always under emergency
- The team is often called Computer Security Incident Response Team (CSIRT)
- The input to the response phase is not limited from the operation phase, but the team should also have response to reports or notifications from third parties

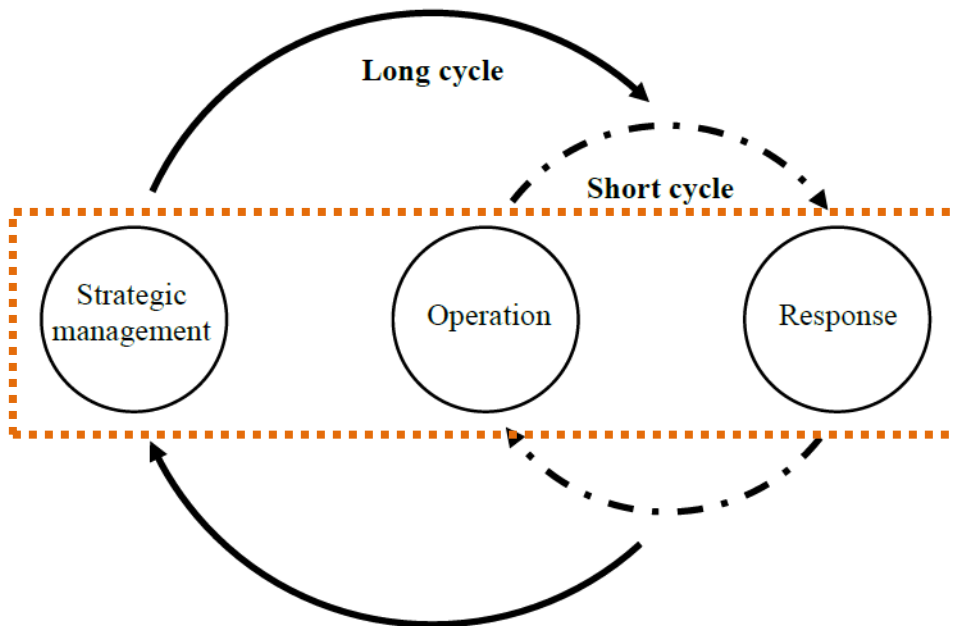


Figure 6 - CDC management process

Management process - 2 cycles

1. Short cycle

- “Operation” and “Response” are performed daily
- Continuous improvement to resolve problems/issues, e.g., simple automation of simple tasks, improvement of tools to analysis accuracy, and review of report items, are necessary within the allocated resources (people, budget, system) in a short cycle.

2. Long cycle

- A review that requires the allocation of new resources should be applied to a long cycle.
- If any issues that cannot be solved by the current system are found when reviewing the short cycle, it should be responded with a long-term perspective and plan, e.g., the introduction of a new security product, a drastic review of security policies, and a large-scale configuration change of the security systems

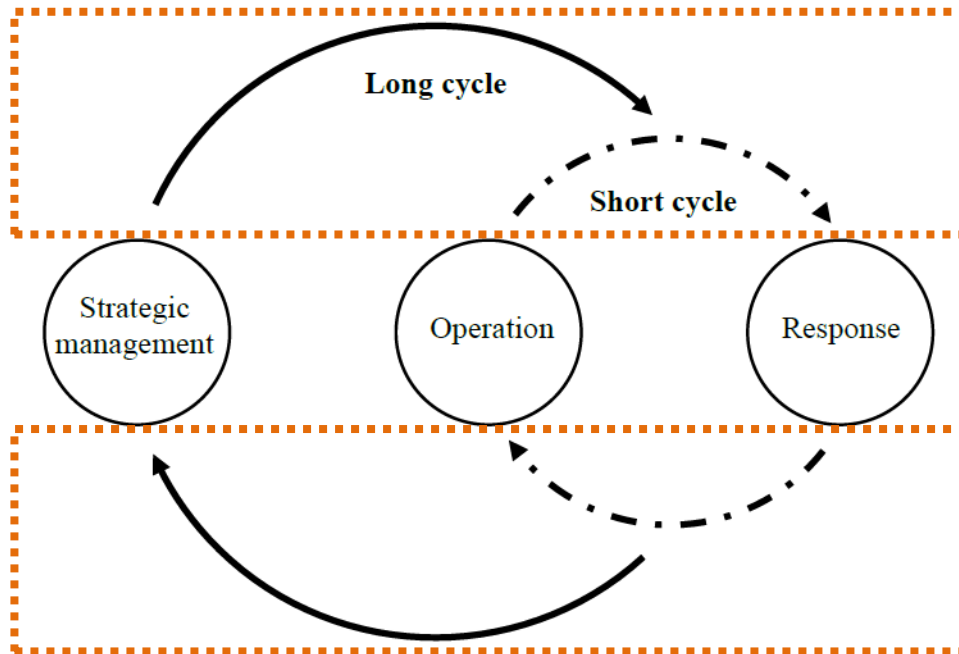
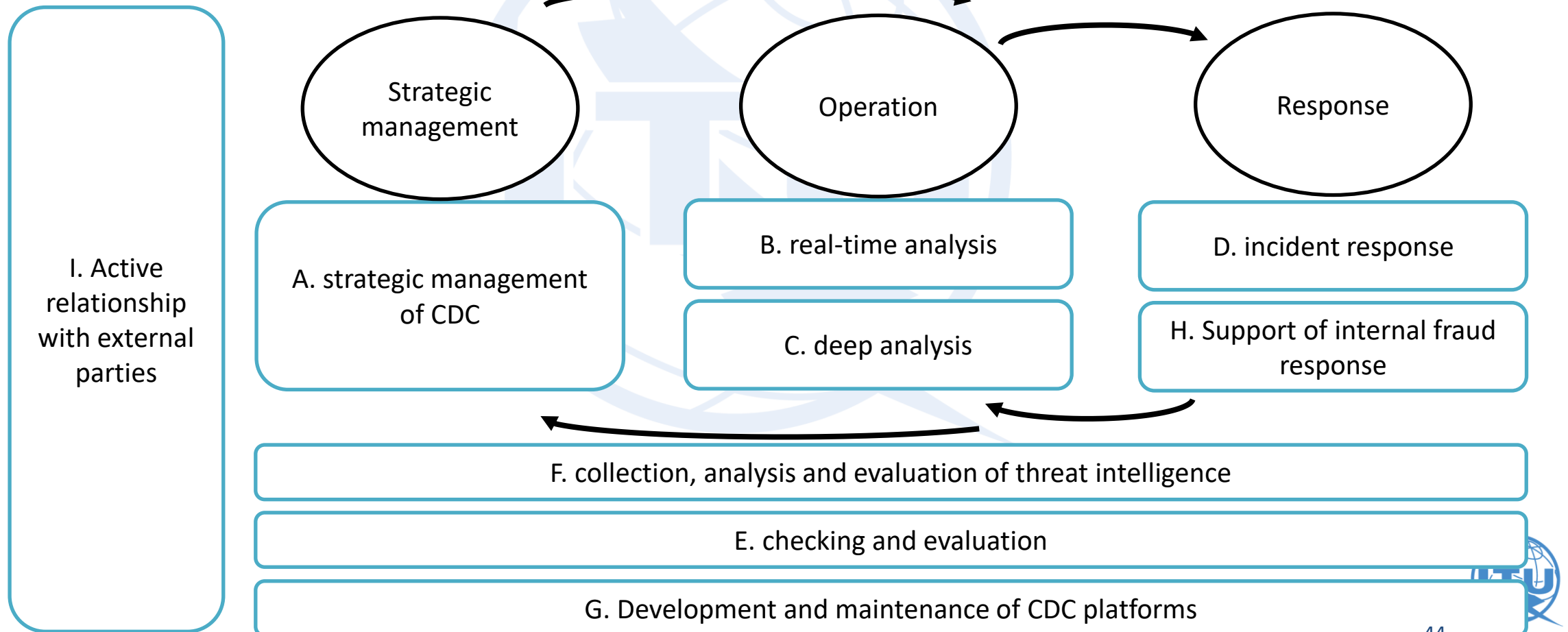


Figure 6 - CDC management process

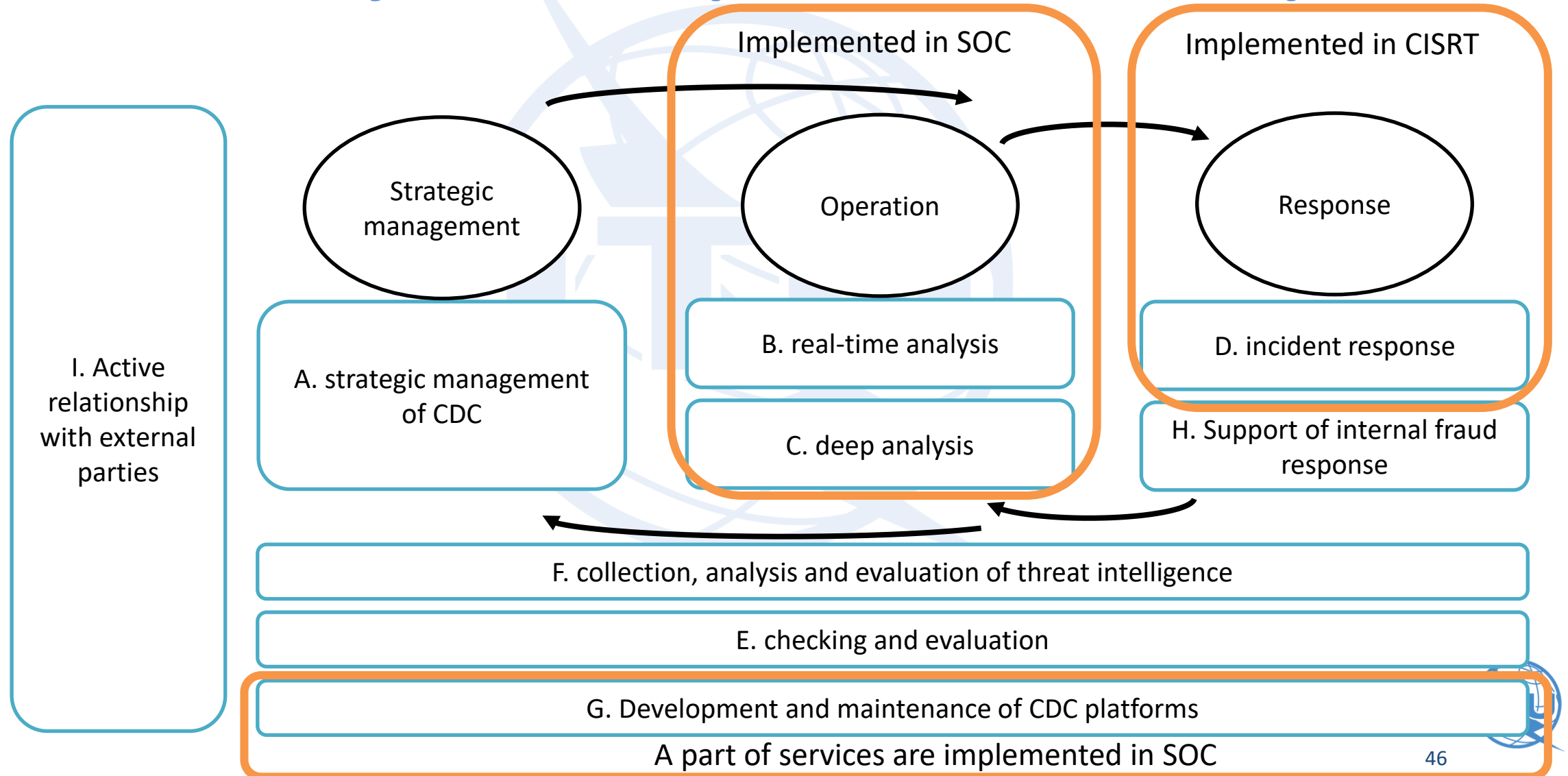
Mapping service categories and “Management process”.



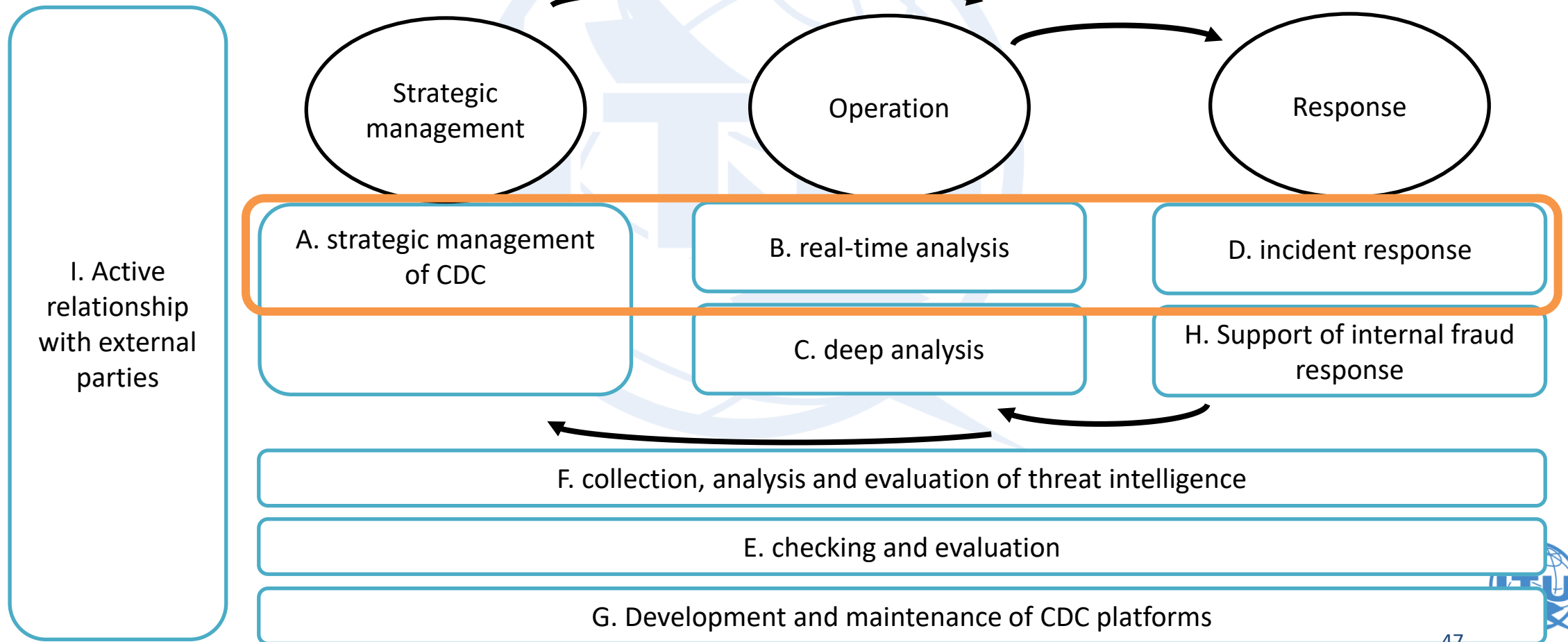
Implement from necessary services.

- Those are determined by the priority of security service for cybersecurity and resources that the organization has.
- X.1060 is a framework which suggests to improve the organization continuously.

Case: already do the “Operation” and “Response”



Case: minimum implementation for starting management process.



Evaluation Process

Note:

The process of reviewing each of the service catalogs, profiles, and portfolios defined in the Build process

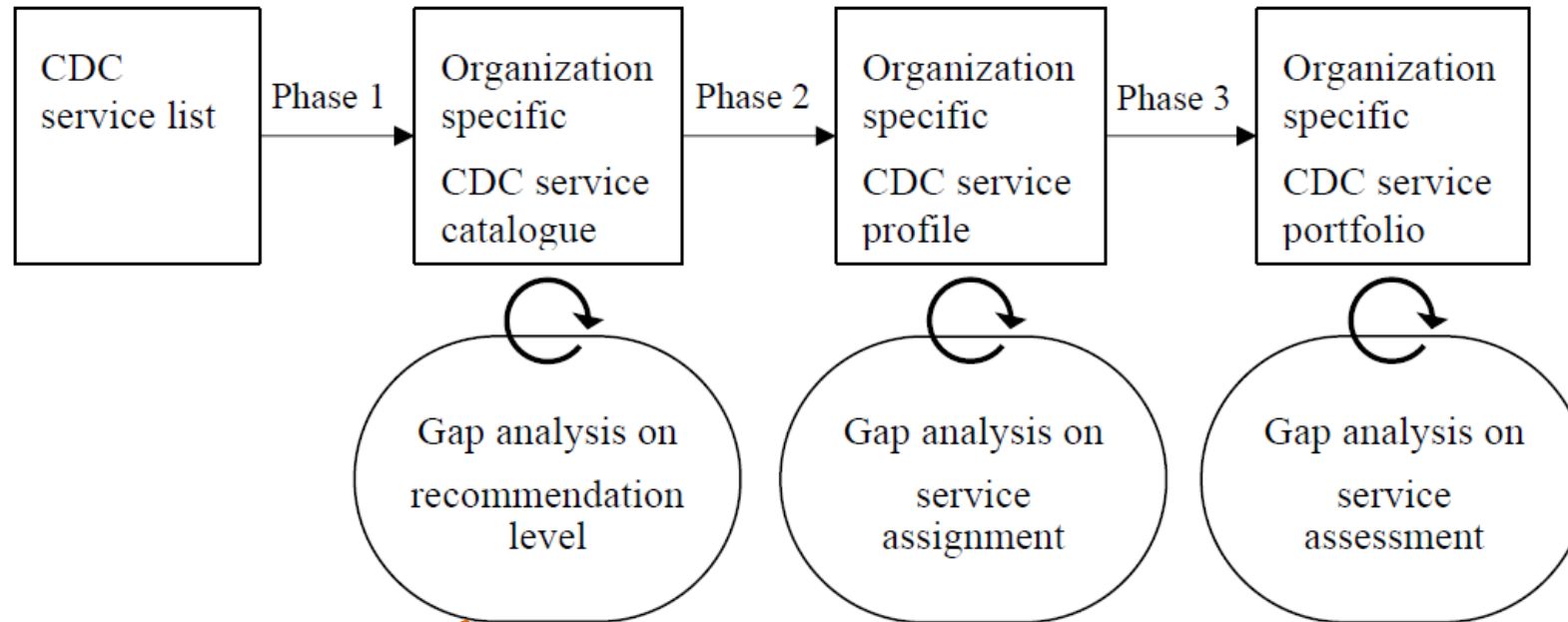


Figure 7 - CDC evaluation process

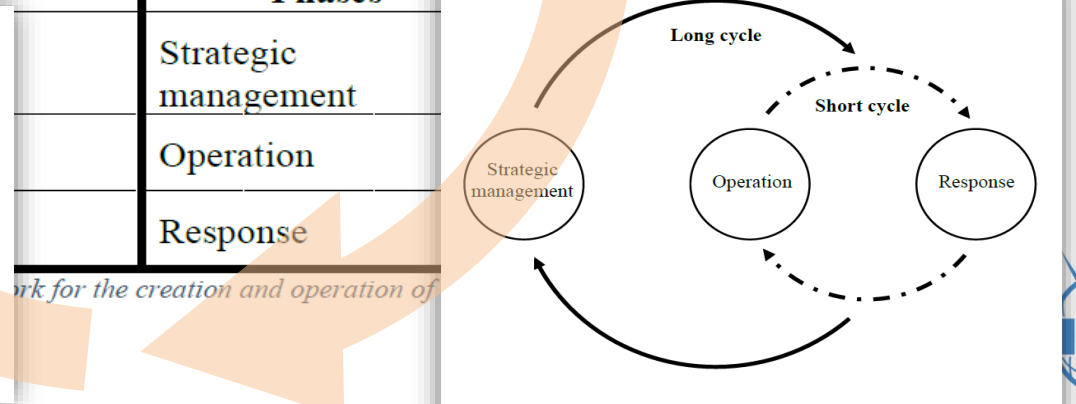
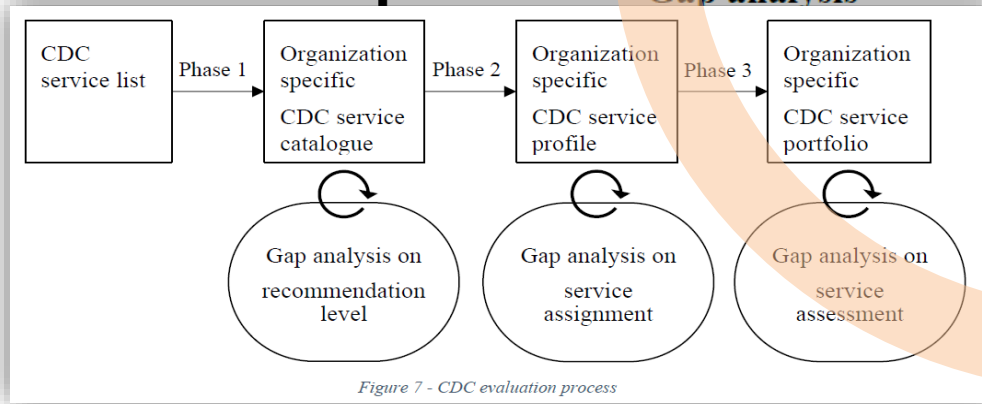
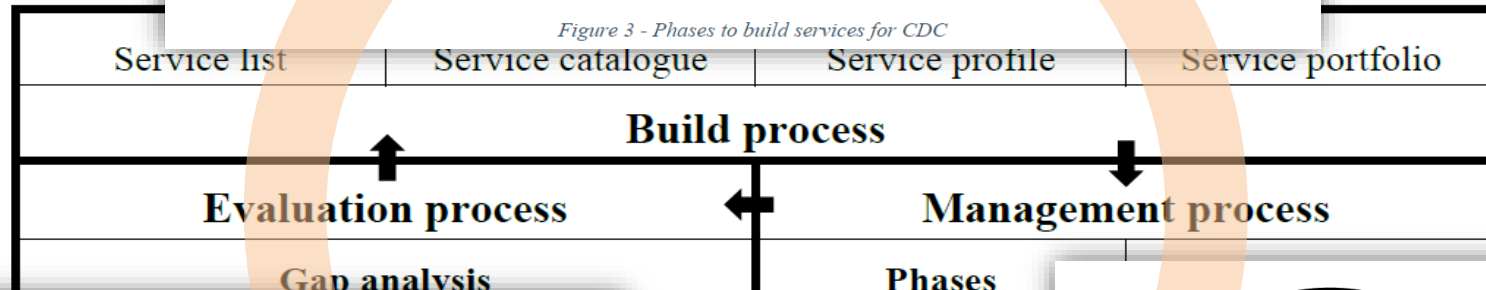
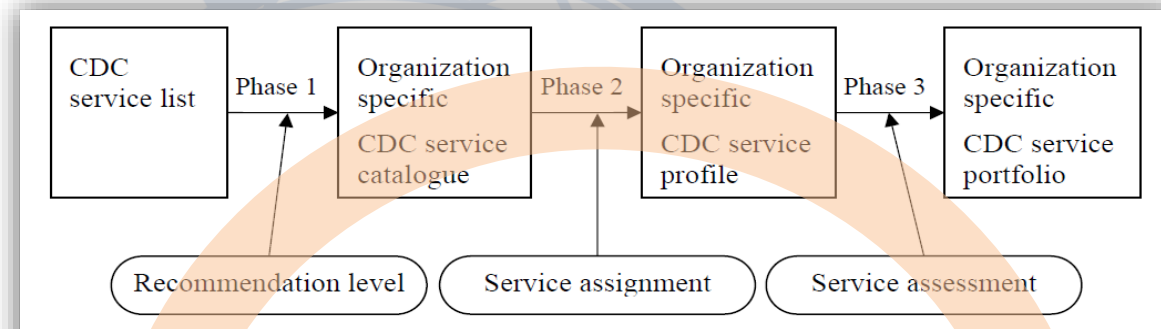
Are there any excesses or shortages in the services selected for the service catalog?

Are the assignments made in the service profile reasonable?

Does it achieve the target score set in the service portfolio?



X.1060 Framework for the creation and operation of a Cyber Defence Centre



Organizations feedback



Customers feedback

A spectrum

- Customers in ITU aware region are picking up
 - APT, AFR and ARB groups but RCC out of the game
 - Government agencies
 - Businesses
 - On the West this is a slow pick up
 - CEPT, CITEC believe they have their solutions
 - Businesses are now asking questions
 - Was contacted by 'NoLimitSecu' for a podcast
- In particular
- Japan businesses
 - Japan government agencies
 - 5000 downloads of X.1060 in Japanese version
 - African and Arab group government agencies (many!)
 - African and Arab group Operators
- But as well
- Some very large businesses are evaluating X.1060
 - They need to transform their disparate current setup
 - They appreciate the neutral language vs "prima dona"

We received a lot of feedback

A lot of enthusiasm

- Key progress on the layout of X.sup-cdc + content
- Great input from SG17AFR for the next questionnaire
- There should be more work with FIRST
- 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

Before anything!

This is about leadership!

- 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!
- 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”

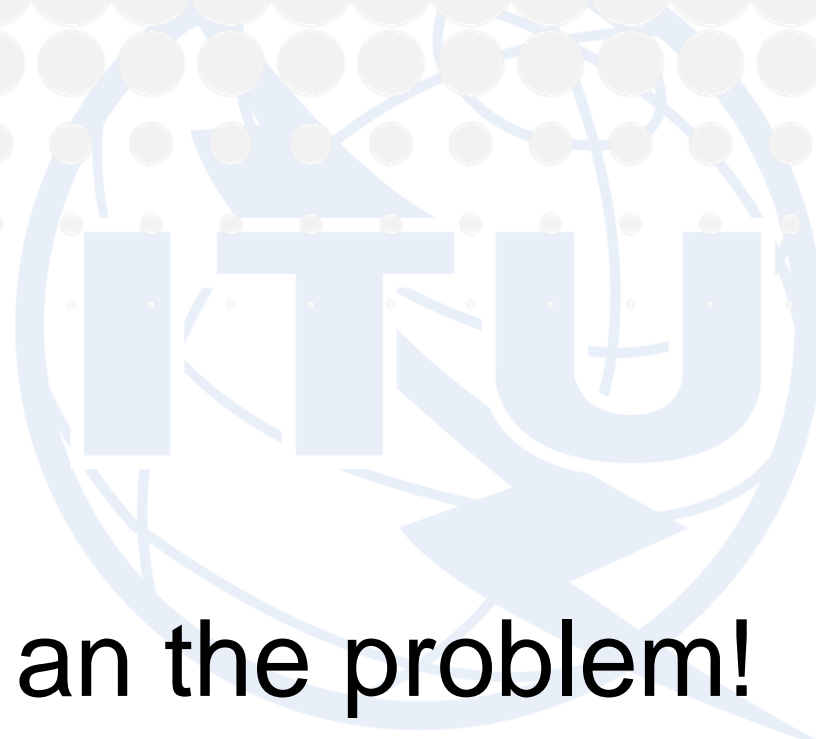
The ‘astuce’ is that X.1060 is ‘external’ to the organization so it blocks internal politicking

What is at stake at regional level

- 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 countries in a given region of the world 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 a region 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”



The next steps an the problem!



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

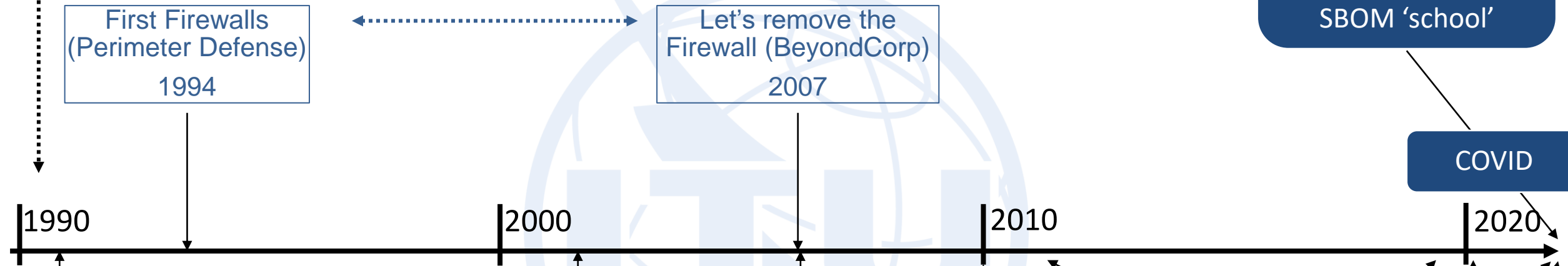
5 to define a general/common set of security capabilities for each phase of information system/network/application lifecycles, so that consequently security by design (security capabilities and features available by design) could be achieved for systems/networks/applications from day one;

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,

Paradoxes in the history of cybersecurity

Last international consensus?

Shift from ZT'school' to SBOM 'school'



ITU X.800
1991

Jericho Forum
2003

BeyondCorp
(Google)
2007

ZT
(Forrester)
2010

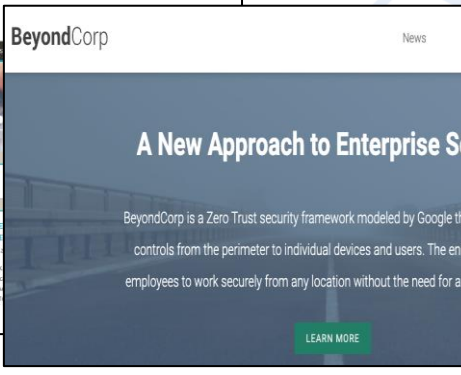
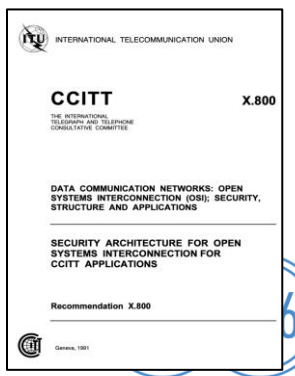
Defense in Depth
(NIST)
2012

NIST / UK NCSC / ...
ZT Architectures

SASE
(Gartner)
2019

SSE
(Gartner)
2022

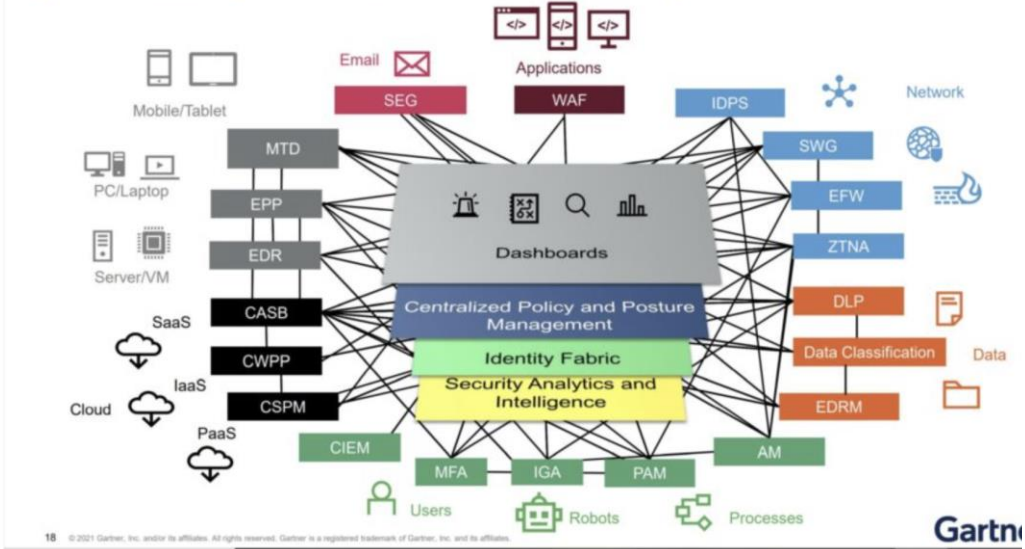
MESH
(Gartner)
2022



If ZT is a principle, is the destination something like MESH?

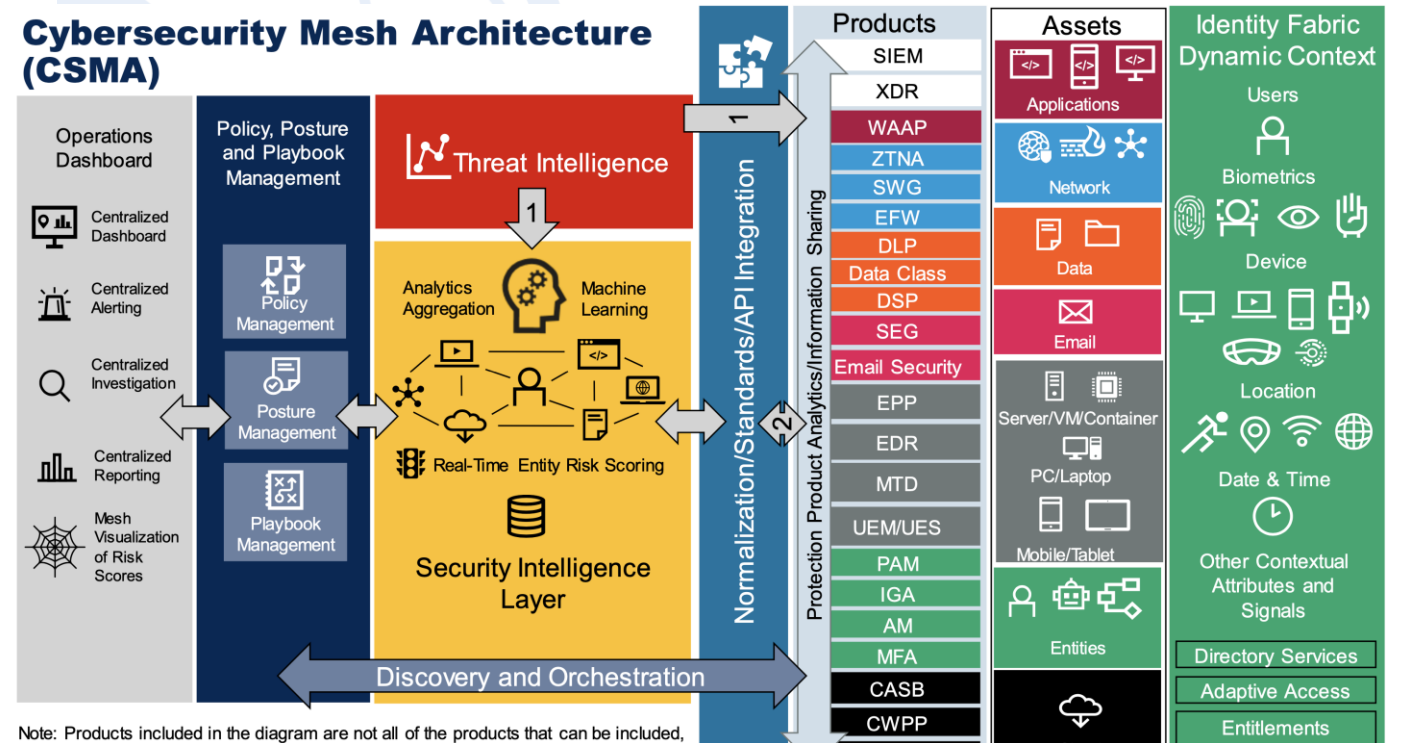
And we think that this is a candidate destination ... but there are problems too!

Cybersecurity Mesh Architecture Complete



Cybersecurity mesh architecture (Source: Gartner)

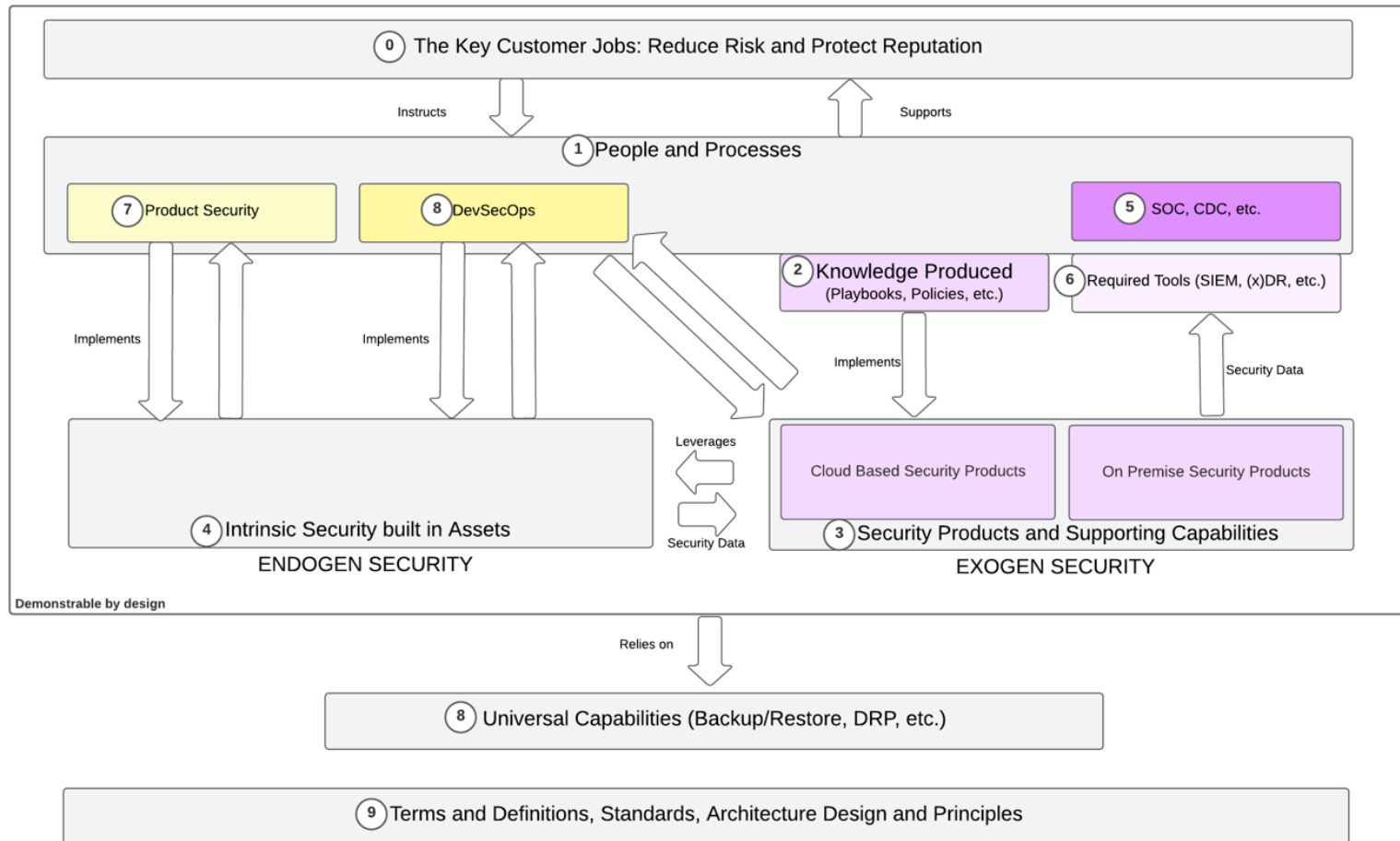
Cybersecurity Mesh Architecture (CSMA)



Note: Products included in the diagram are not all of the products that can be included,

ITU-T SG17 Common Foundation?

Work in Progress → Discussion for an "OSI model for cybersecurity"



Narrative: "if all the job is to reduce risk and protect reputation then what are the key constituencies for a reasonable operational security:

- People and process ...
- ... who extract their knowledge ...
- ... to instruct a product stack ...
- ... to protect assets"

This narrative already transformed an entire community, changed national cybersecurity policies, added two new instructions by UN Resolution, agreement to establish new Compendium ... several key contributions expected by Fall 2023

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

People and Processes

Knowledge

Tools

Endogen Stack

Exogen Stack

Universal Capabilities

Terms, Definitions, Design
Principles, Architecture
Methodolgy, etc.

Mapping CDC

People and Processes

SG17: X.1060

SG17:
X.sup-cdc

Knowledge

OASIS:
CACAO

Tools

Endogen Stack

SG17:
TR.smpa

Exogen Stack

OASIS:
OpenC2

SG17:
X.secadef

SG17:
X.icd-schemas

Universal Capabilities

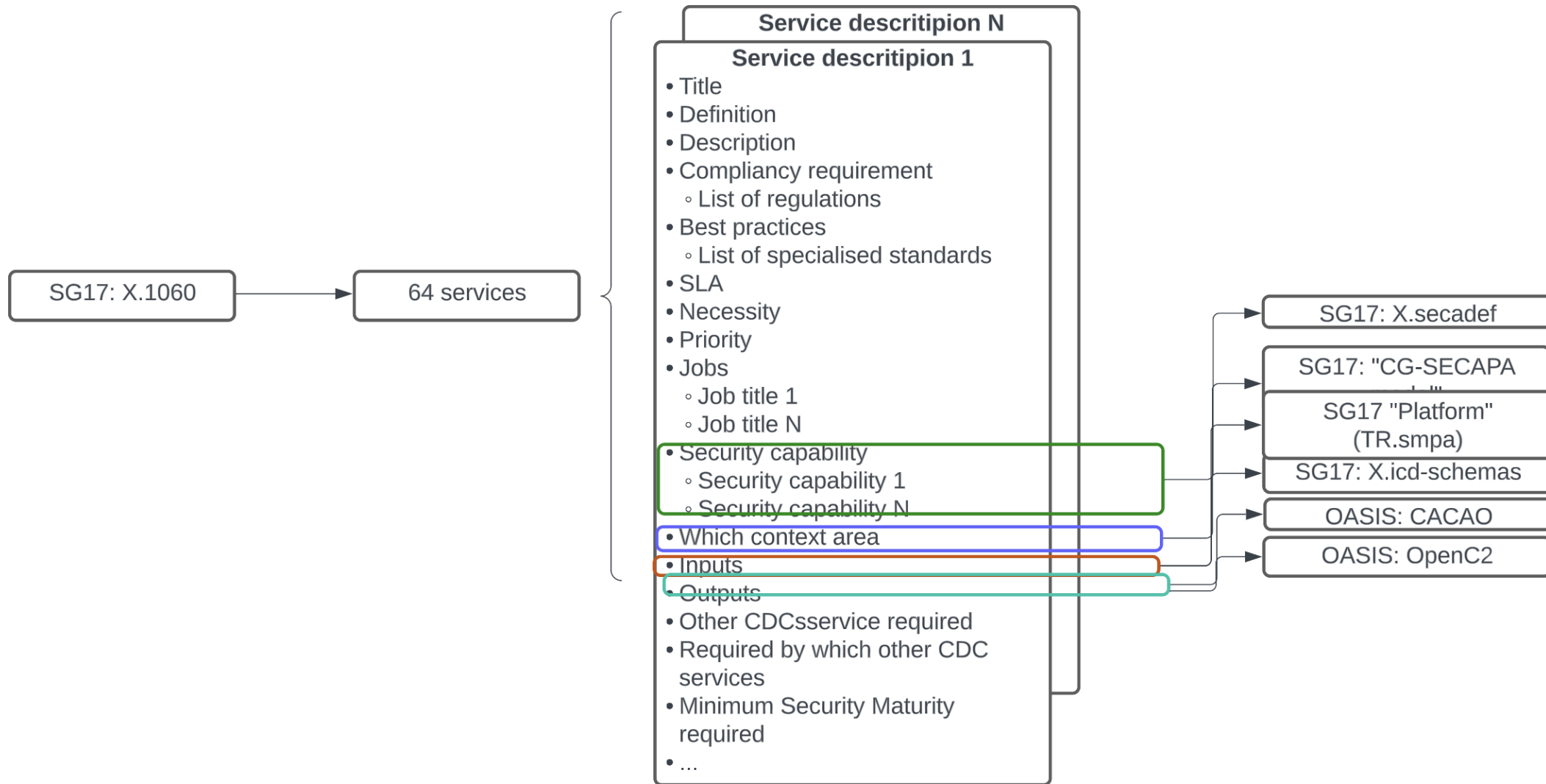
Terms, Definitions, Design
Principles, Architecture
Methodolgy, etc.

SG17:
X.arch-design

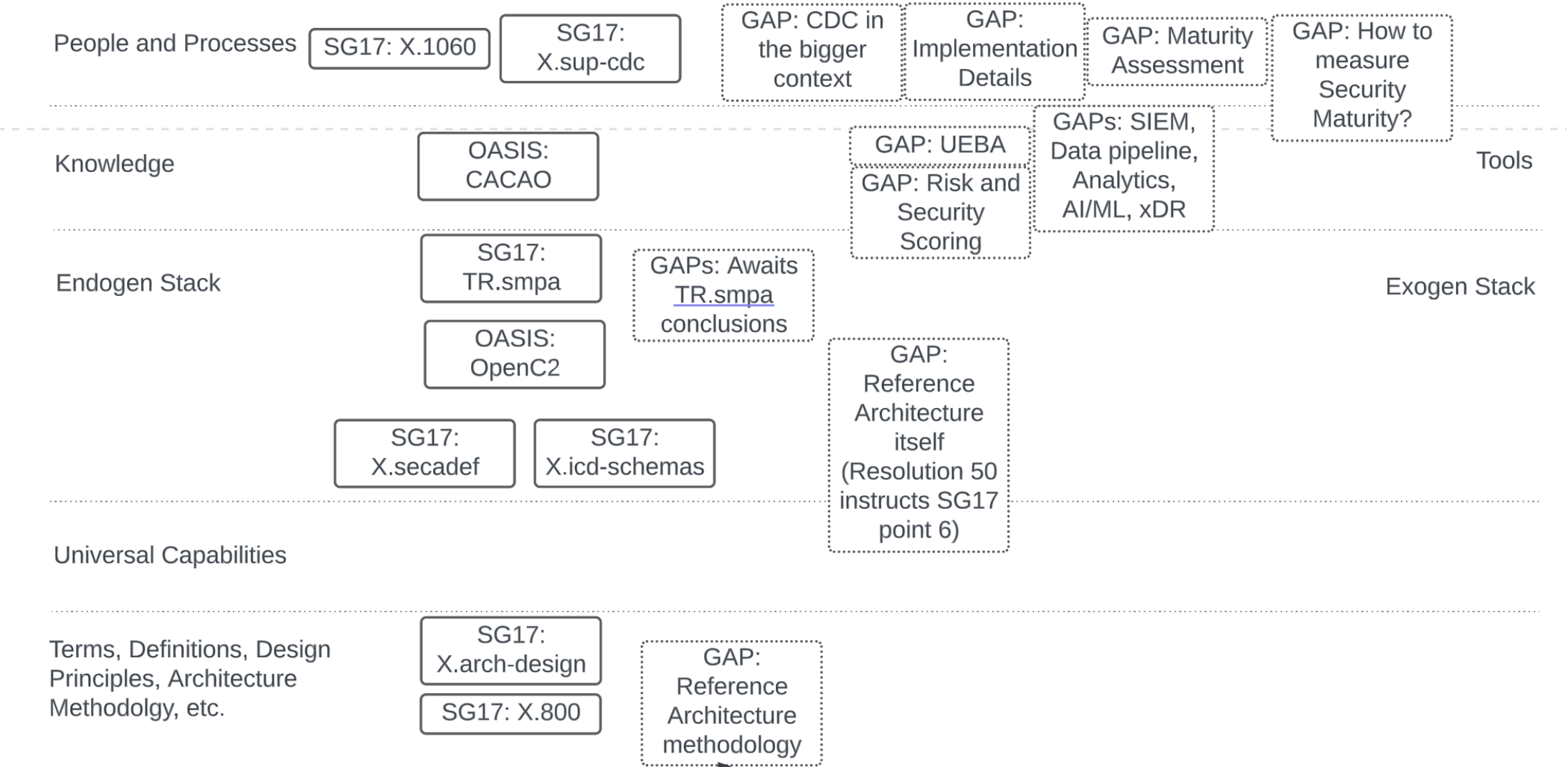
SG17: X.800

A service template shows a LOT of dependencies

to the context



And a lot of gaps



CDC Conclusion

This is a journey

- CDC raised the bar already for some regions of the world
- The intention was to stop a gap in the overall cybersecurity world (amongst many)
- Now we enter the development part
- And we see all the missing links



Conclusions





Symantec™

by Broadcom Software