REGIONAL CYBERSECURITY SUMMIT FOR AFRICA

Cyber Defence Centre based on ITU-T X.1060

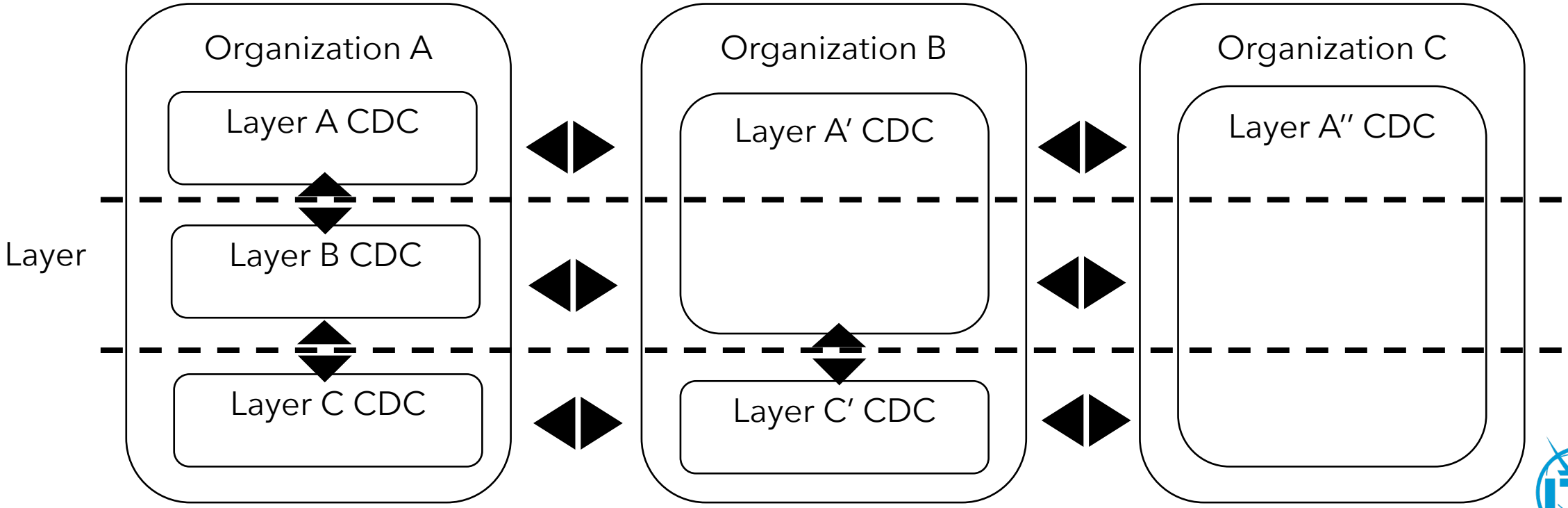
Shigenori TAKEI
ITU-T SG17 WP3 Q3

20-23 November 2023
Kampala, Uganda

Why is X.1060 needed?

Common language

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

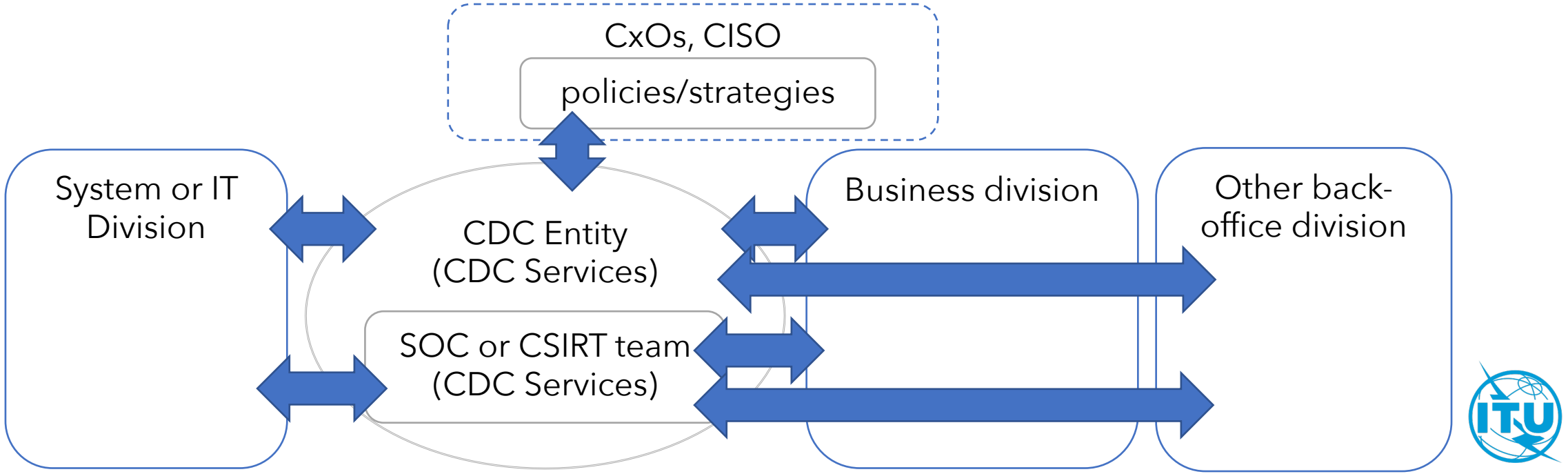


CDC = Broader concept that embraces the existing organizations

- 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

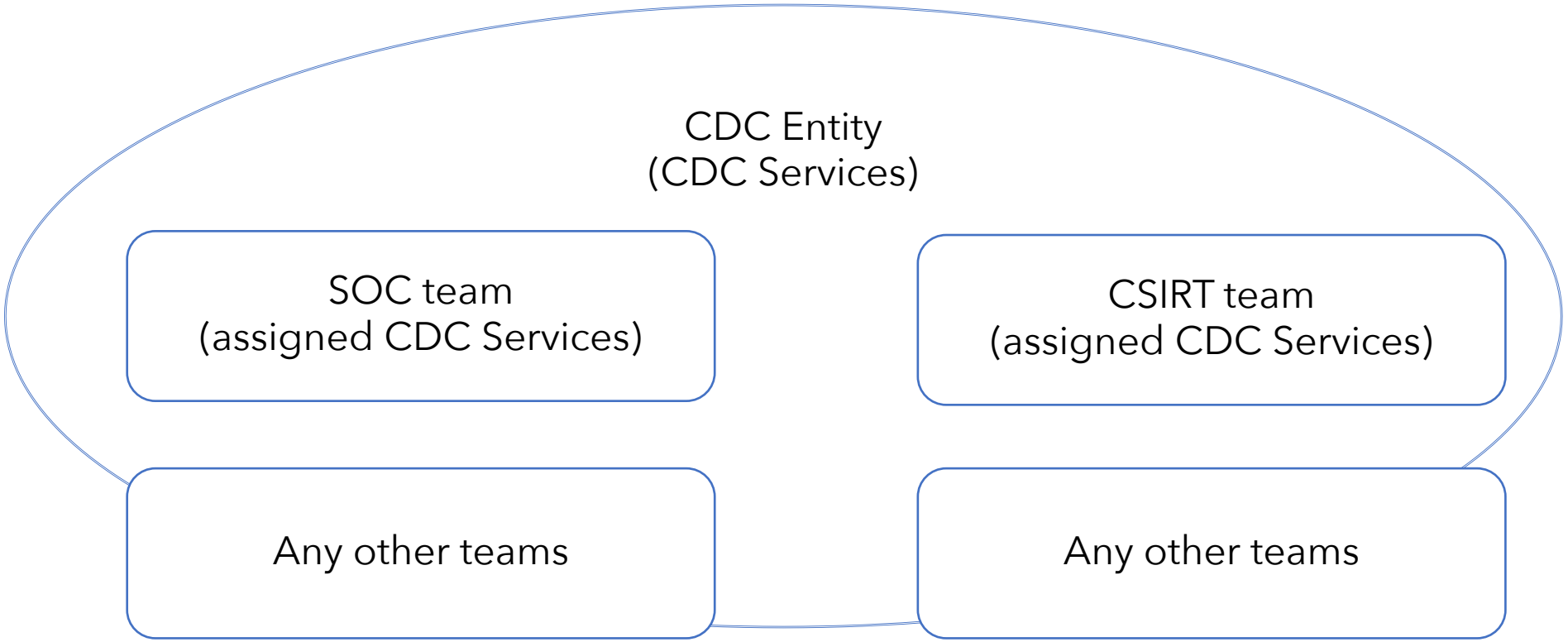
CDC provides security services which counter business risks.

- 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.



Processes of X.1060

The framework

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

Service list	Service catalogue	Service profile	Service portfolio
Build process			
Evaluation process		**Management process**	
Gap analysis		**Phases**	**Cycles**
Assessment		Strategic management	Long cycle
Assignment		Operation	Short cycle
Recommendation level		Response	

Figure 2 - Framework for the creation and operation of CDC

Overview of a process

1. Mapping existing services to CDC services
2. Define CDC service portfolio
    1. Select from CDC service catalog with recommendation level
    2. Assigning services which is insourcing or outsourcing
    3. Assessment each service the score As-Is, To-Be
3. Do the management process
4. Evaluation and improvement continuously

Build Process

Process

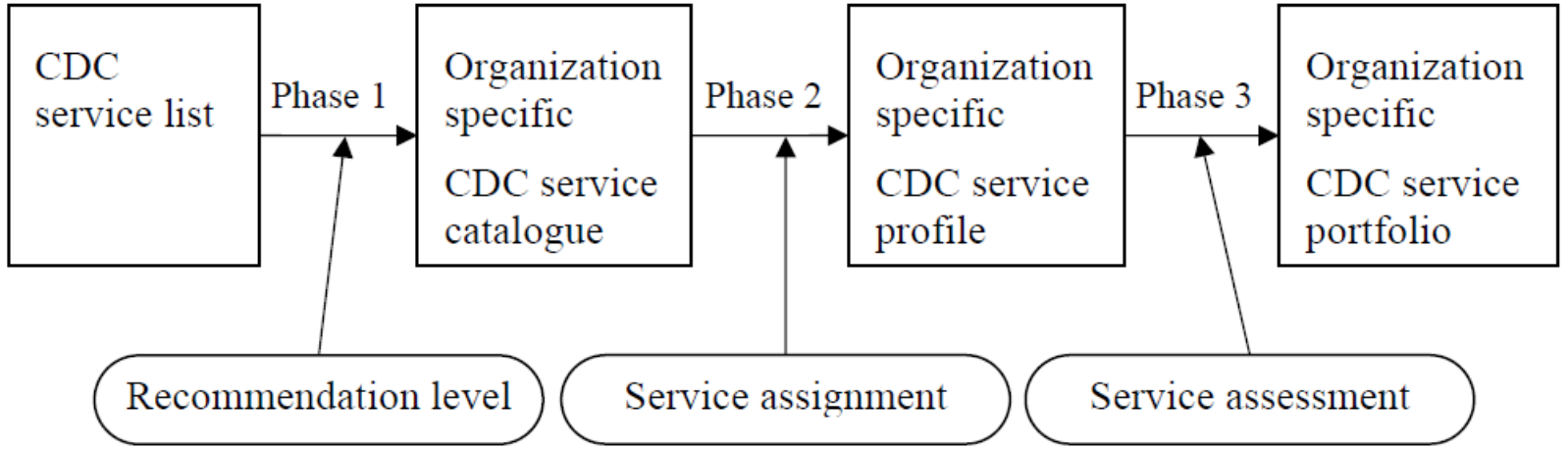
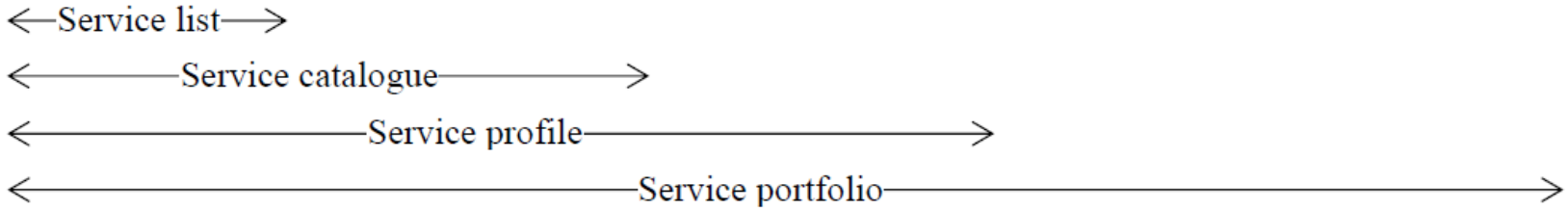


Figure 3 - Phases to build services for CDC

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

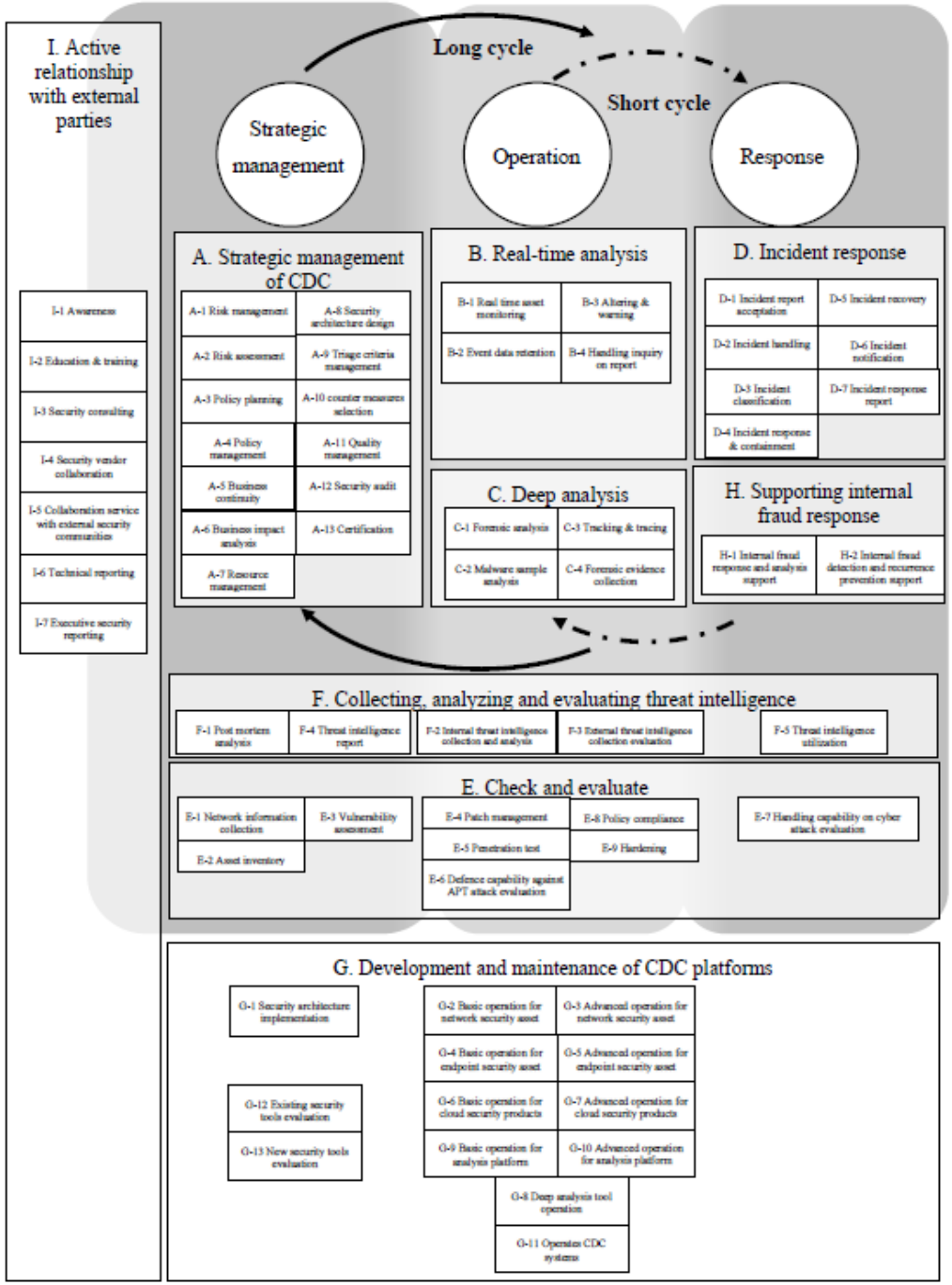
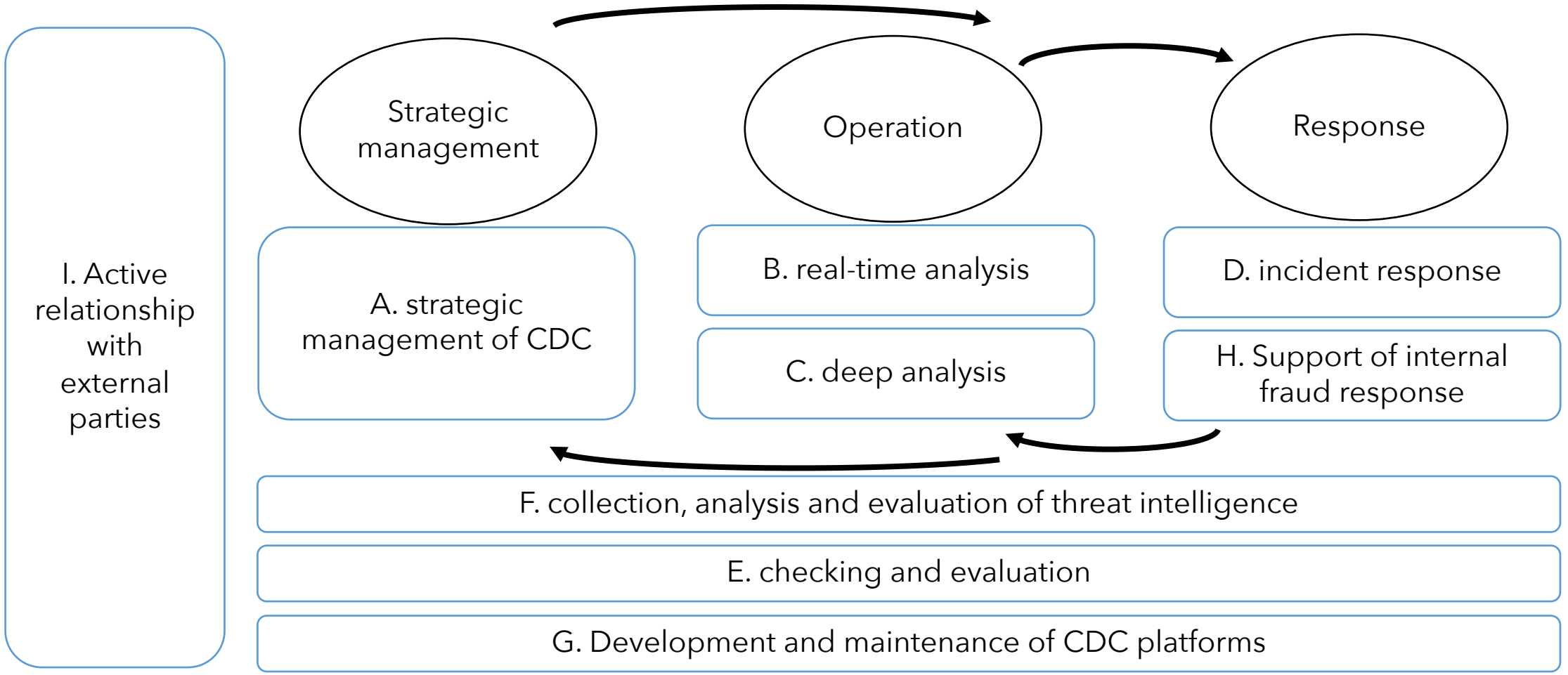


Figure 8 - CDC service categories

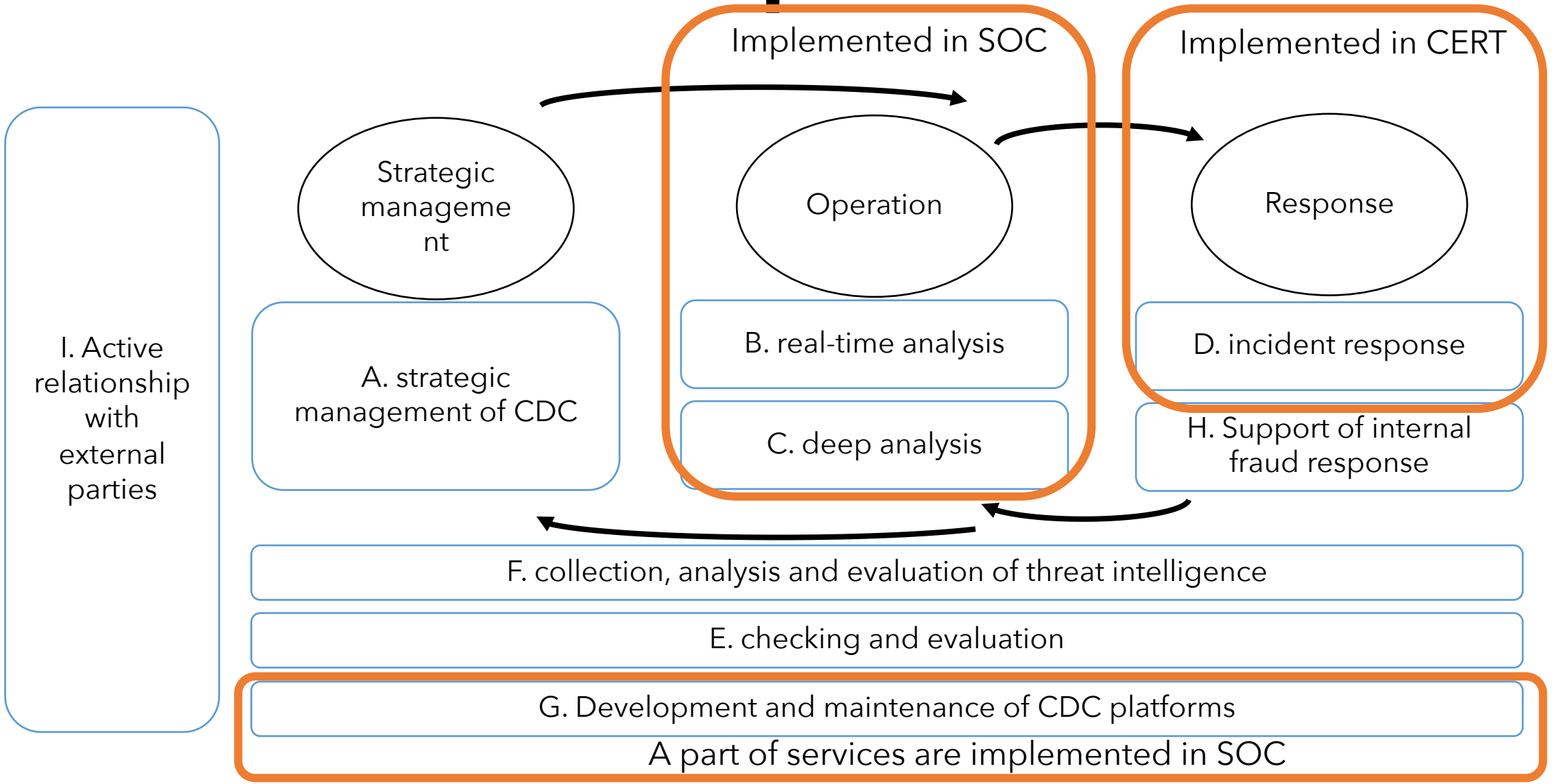
Mapping service categories and "Management process"



Mapping existing services to the CDC

- If the organization already has the security team called SOC or CERT or xIRT, mapping existing security services to CDC services.
- In the management process, it has three phases, strategic management, operation and response.
- In X.1060, operation phase is defined below:
  - … The team that performs such operations is often called a security operations centre(SOC)
- In X.1060, response phase is defined below:
  - An incident response should be executed when an event is detected by the analysis in the operation phase. This phase is always an emergency. Those responding to the incident are often called the computer security incident response team(CSIRT)

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



xIRT services are mapped to category D

- Category D is mapped for the response phase in management process.
- Services in Category D are below:
  - D-1. Incident report acceptance
  - D-2. Incident handling
  - D-3. Incident classification
  - D-4. Incident response and containment
  - D-5. Incident recovery
  - D-6. Incident notification
  - D-7. Incident response report

Build process
Phase 1: Making a catalogue

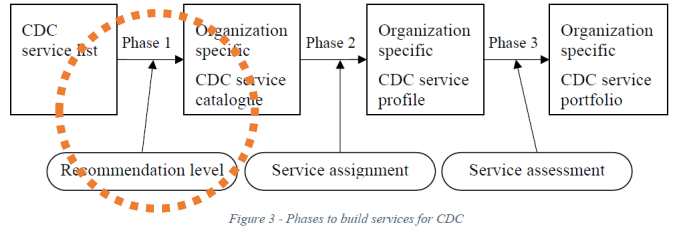
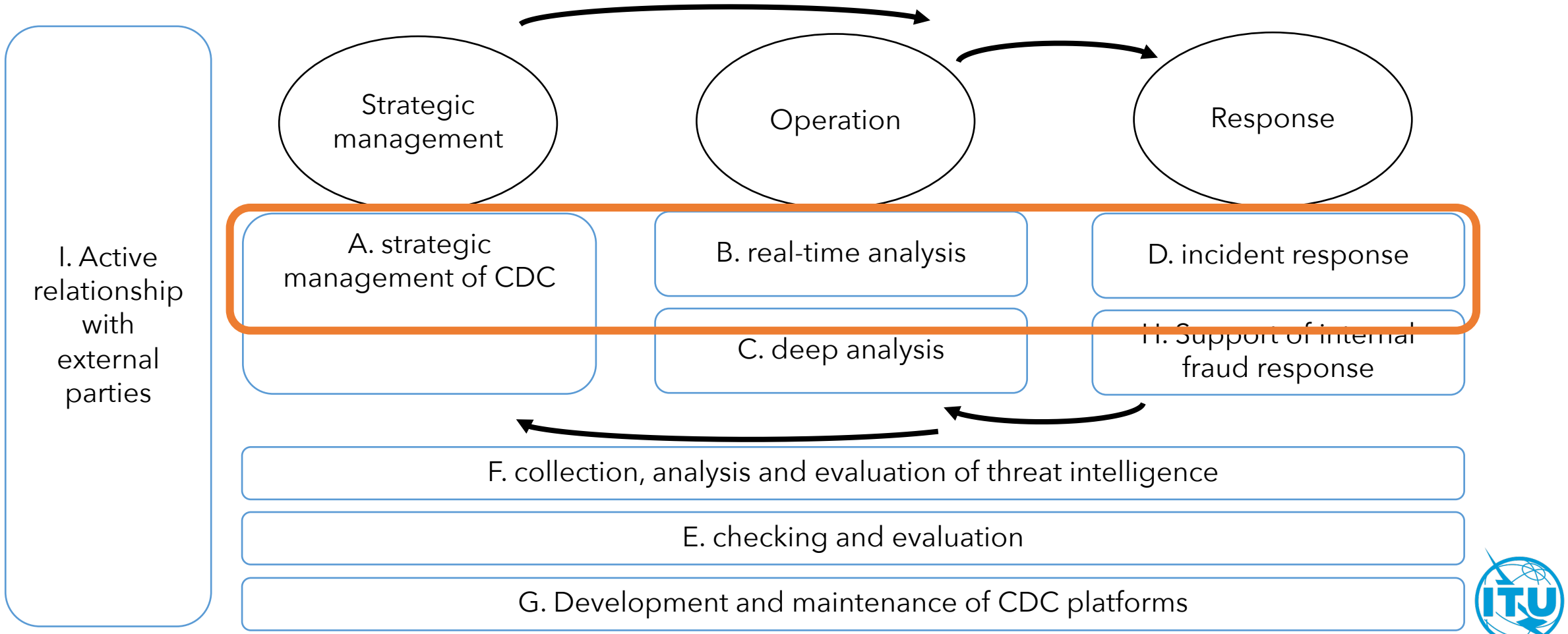


Figure 3 - Phases to build services for CDC

- 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

Category A,B,C,D is needed for management process



Using CDC services Recommendation level

Service	Recommendation level	Service assignment	Service score	
			As-is	To-be
A-1. Risk management	Basic			
A-2. Risk assessment	Basic			
…				
B-1. Real-time asset monitoring	Basic			
B-2. Event data retention	Standard			
…				

Build process
Phase 2: Making a profile

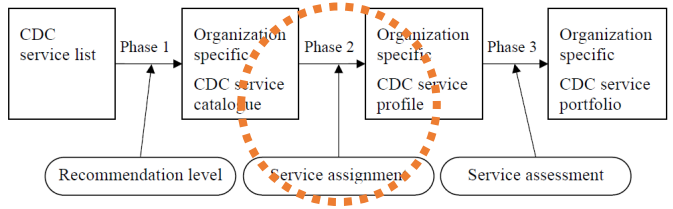


Figure 3 - Phases to build services for CDC

- 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;

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.

- Below indicators can be considered types of insource or outsource.

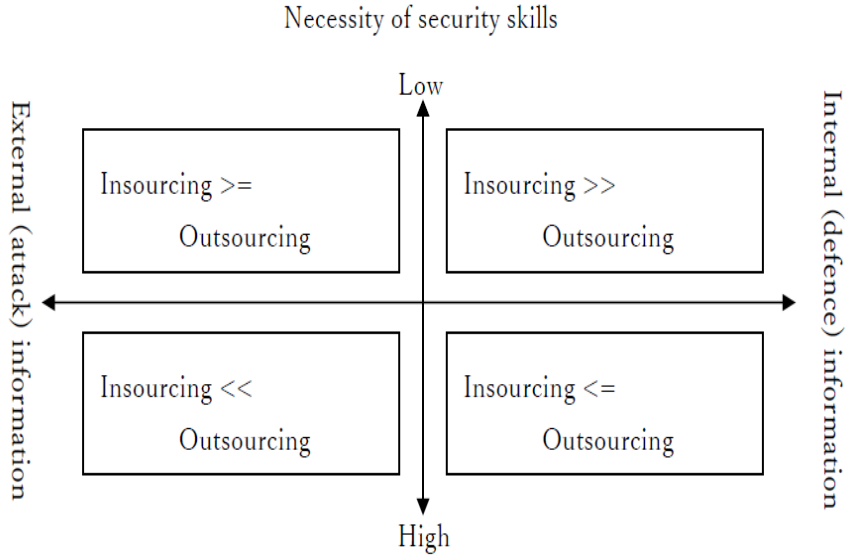
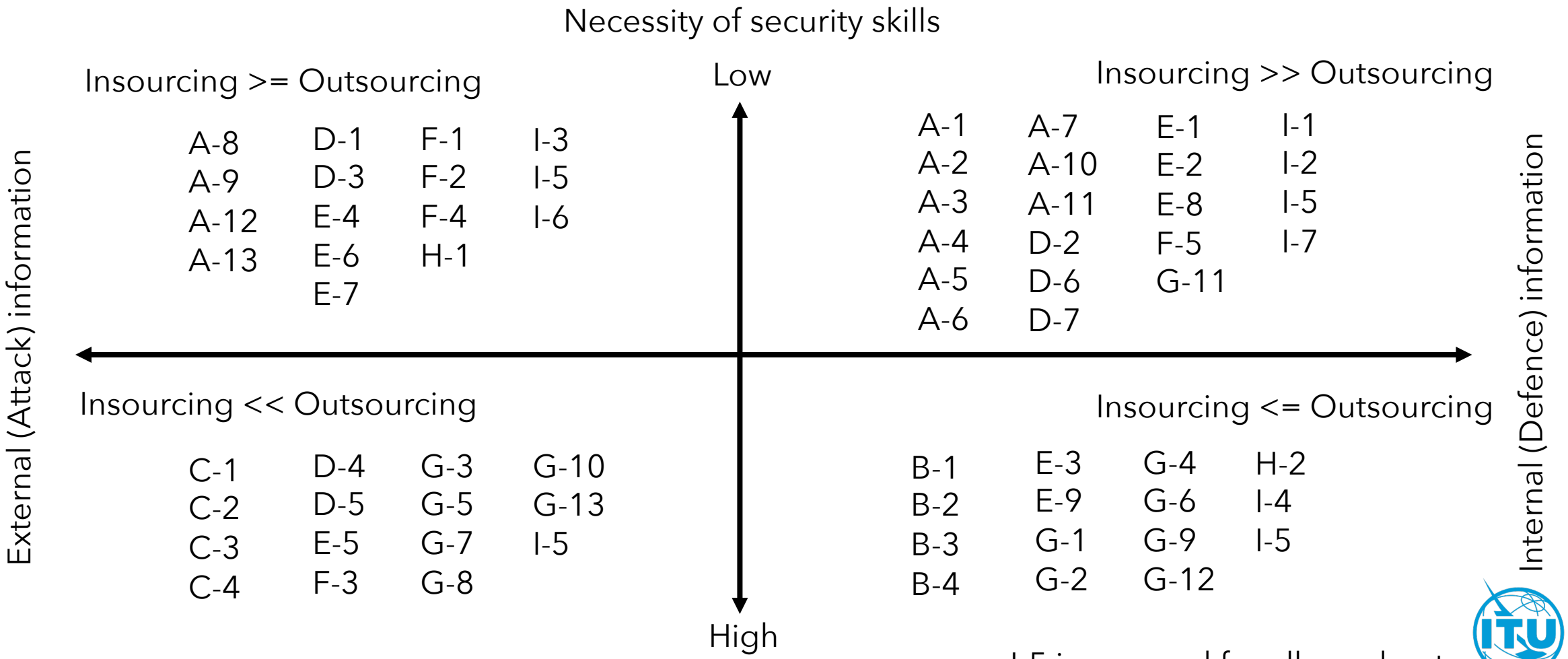


Figure 5 - Sourcing quadrants

Services for insourcing and outsourcing

One example case for the organization



I-5 is mapped for all quadrant

Using CDC services assignment

Service	Recommendation level	Service assignment	Service score	
			As-is	To-be
A-1. Risk management	Basic	**Insourcing(AB Dept.)**		
A-2. Risk assessment	Basic	**Insourcing(AB Dept.)**		
…				
B-1. Real-time asset monitoring	Basic	**Outsourcing(Z-MSSP)**		
B-2. Event data retention	Standard	**Outsourcing(Z-MSSP)**		
…				

Build process
Phase 3: Making a portfolio

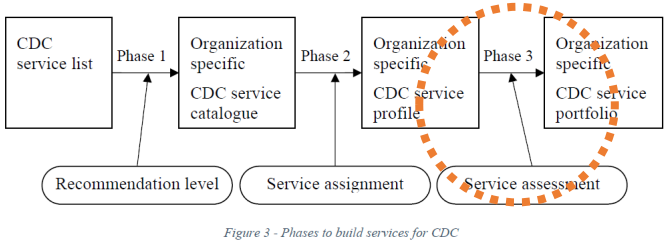


Figure 3 - Phases to build services for CDC

- 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

Using CDC services assessment

Service	Recommendation level	Service assignment	Service score	
			As-is	To-be
A-1. Risk management	Basic	Insourcing(AB Dept.)	**3**	**4**
A-2. Risk assessment	Basic	Insourcing(AB Dept.)	**3**	**4**
…				
B-1. Real-time asset monitoring	Basic	Outsourcing(Z-MSSP)	**2**	**3**
B-2. Event data retention	Standard	Outsourcing(Z-MSSP)	**2**	**3**
…				

Management process - 3 phases

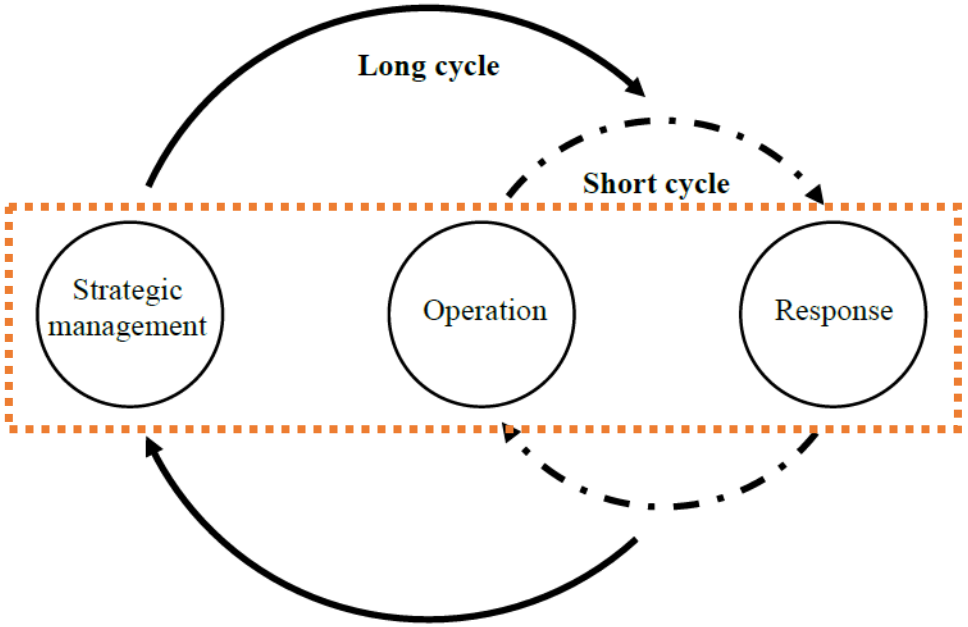


Figure 6 - CDC management process

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 cover response to reports or notifications from third parties

Management process - 2 cycles

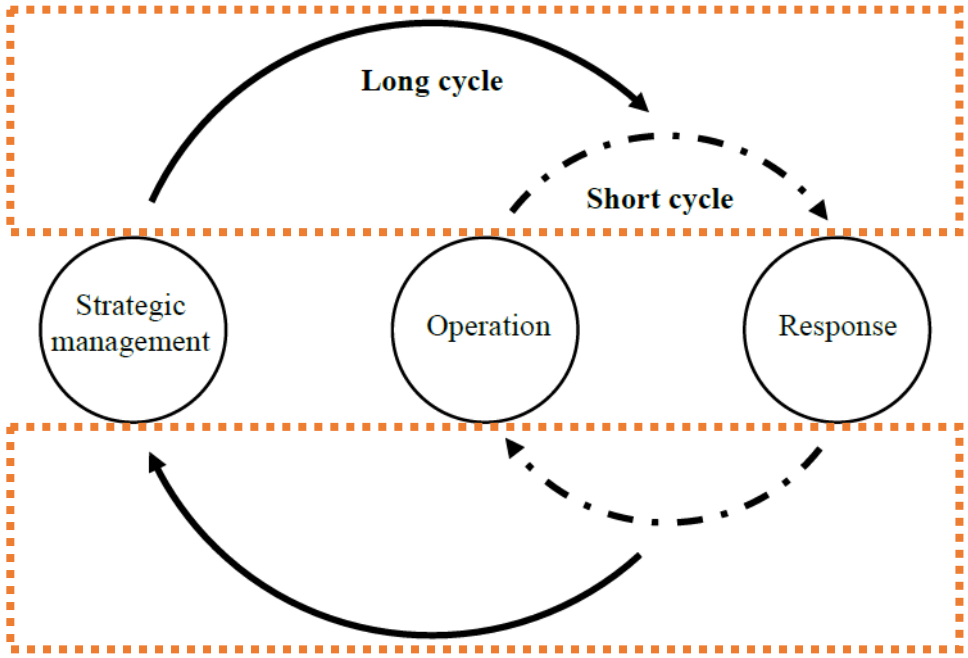


Figure 6 - CDC management process

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

Evaluation Process

Note:

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

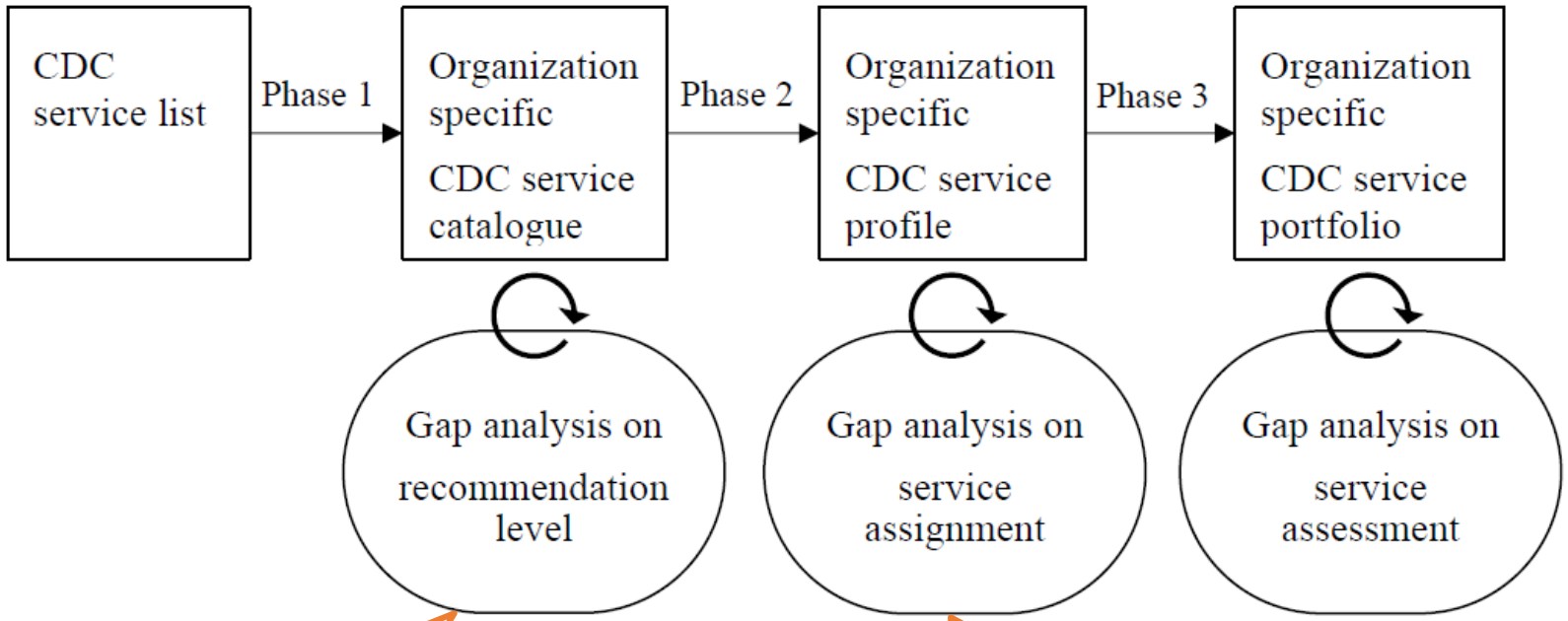


Figure 7 - CDC evaluation process

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

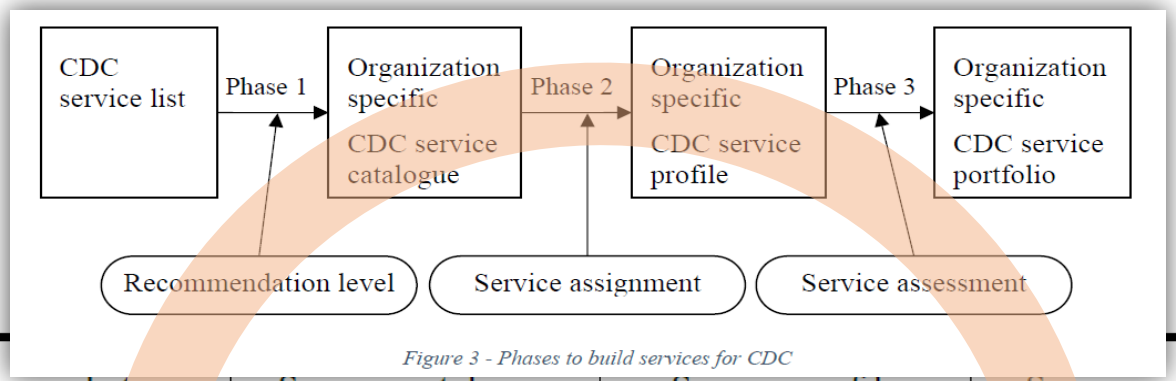
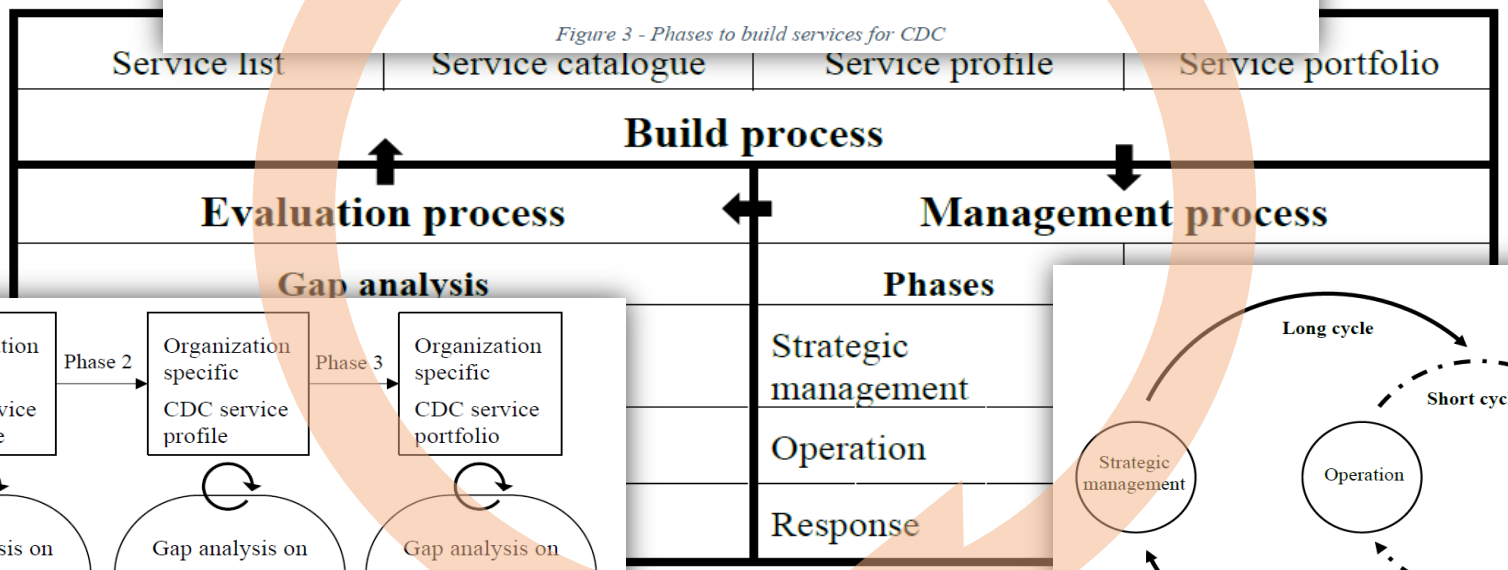


Figure 3 - Phases to build services for CDC



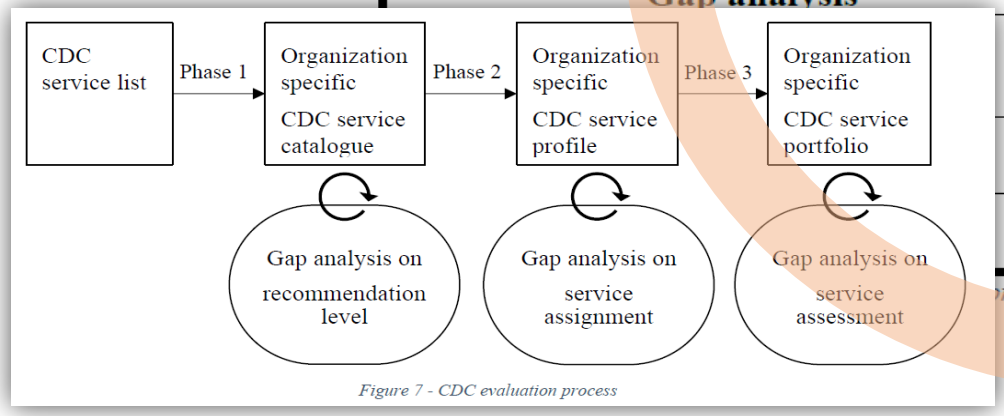


Figure 7 - CDC evaluation process

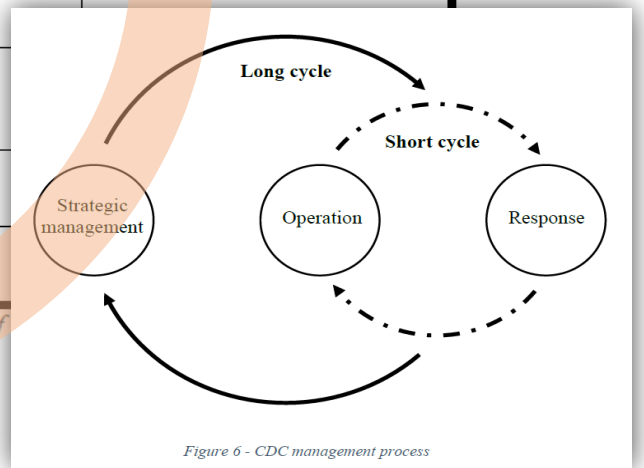


Figure 6 - CDC management process

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