REGIONAL CYBERSECURITY SUMMIT FOR AFRICA

Insights on Algeria telecom's experience implementing X.1060 framework

Abdenour Bourennane

Algérie Télécom

20-23 November 2023
Kampala, Uganda

The build process

How we approached it?

Where did we start from?

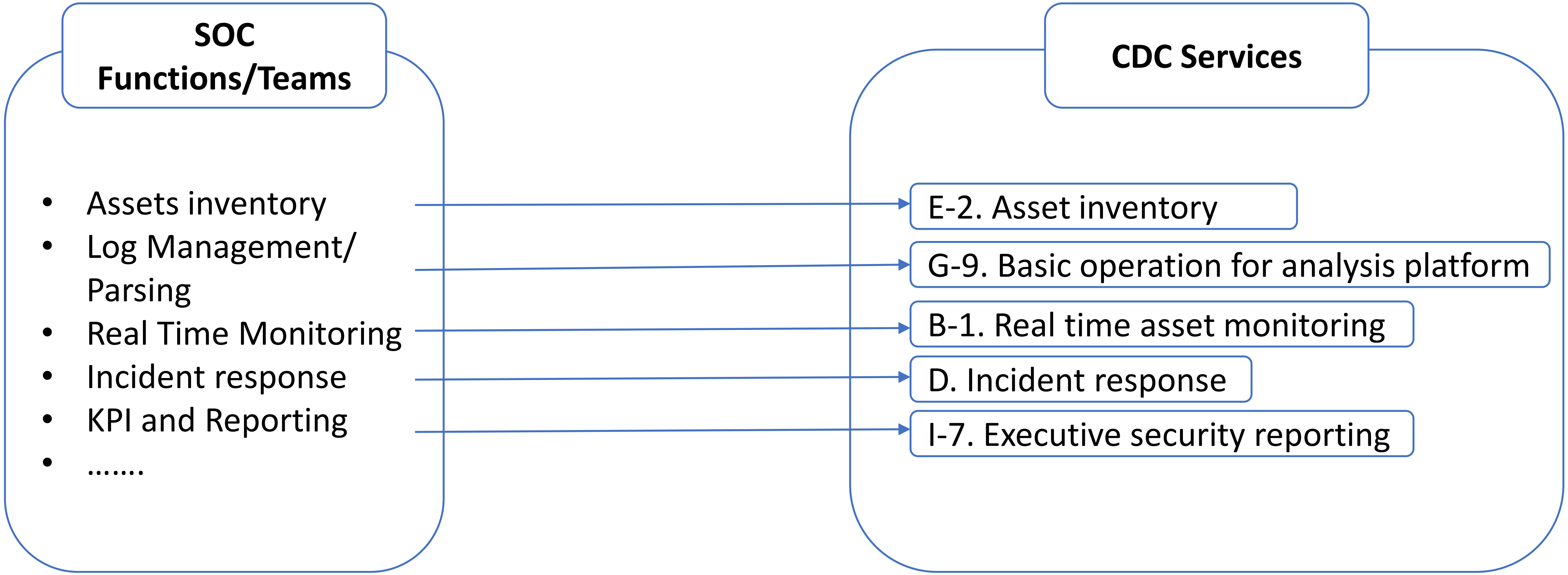
- A Security Operations Center (SOC) was already established
- Other security teams also existed
- A set of security functions were already implemented, and in operational mode

How did X.1060 help?

- Finding a ready to go, rich and adaptive framework made the building process less harder.
- The defined service list cover all of our needs.

How to handle existing SOC functions?

- SOC functions were mapped to CDC services



SOC Functions/Teams

- Assets inventory
- Log Management/ Parsing
- Real Time Monitoring
- Incident response
- KPI and Reporting
- …….

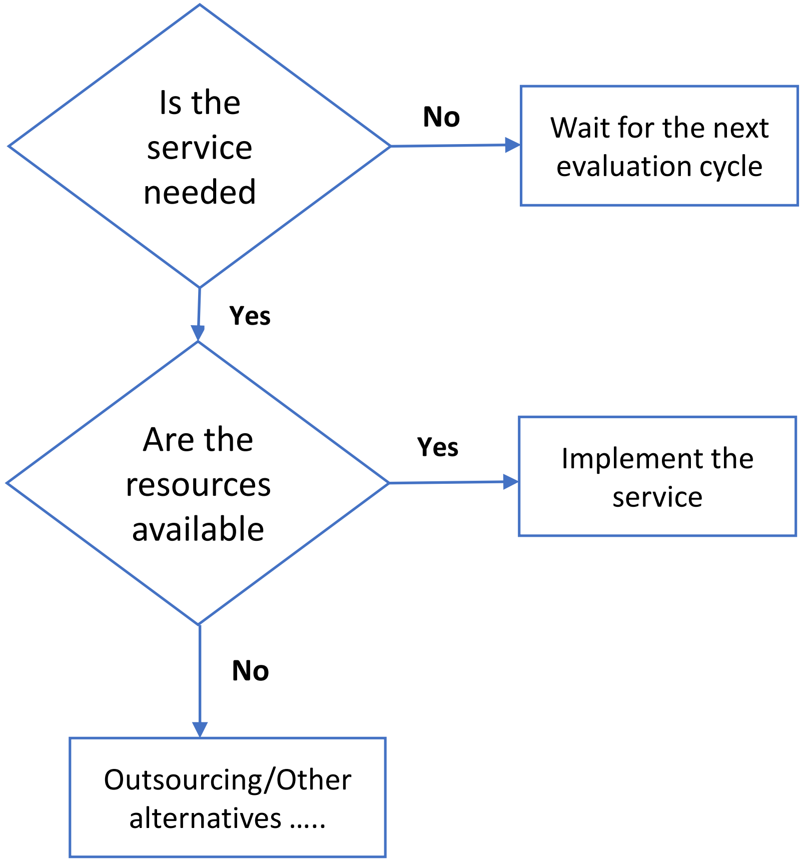
CDC Services

- E-2. Asset inventory
- G-9. Basic operation for analysis platform
- B-1. Real time asset monitoring
- D. Incident response
- I-7. Executive security reporting

How to choose which services to implement?
(Service Catalogue)

- Considerations:
  - Is the service needed (Business needs, risks, Objectives …)?
  - Are the resources available (Financial, Human …)?

Answering these questions helped us to identify the necessary services to implement and the way they needs to be implemented.


Is the service needed
No
Wait for the next evaluation cycle
Yes
Are the resources available
Yes
Implement the service
No
Outsourcing/Other alternatives …..

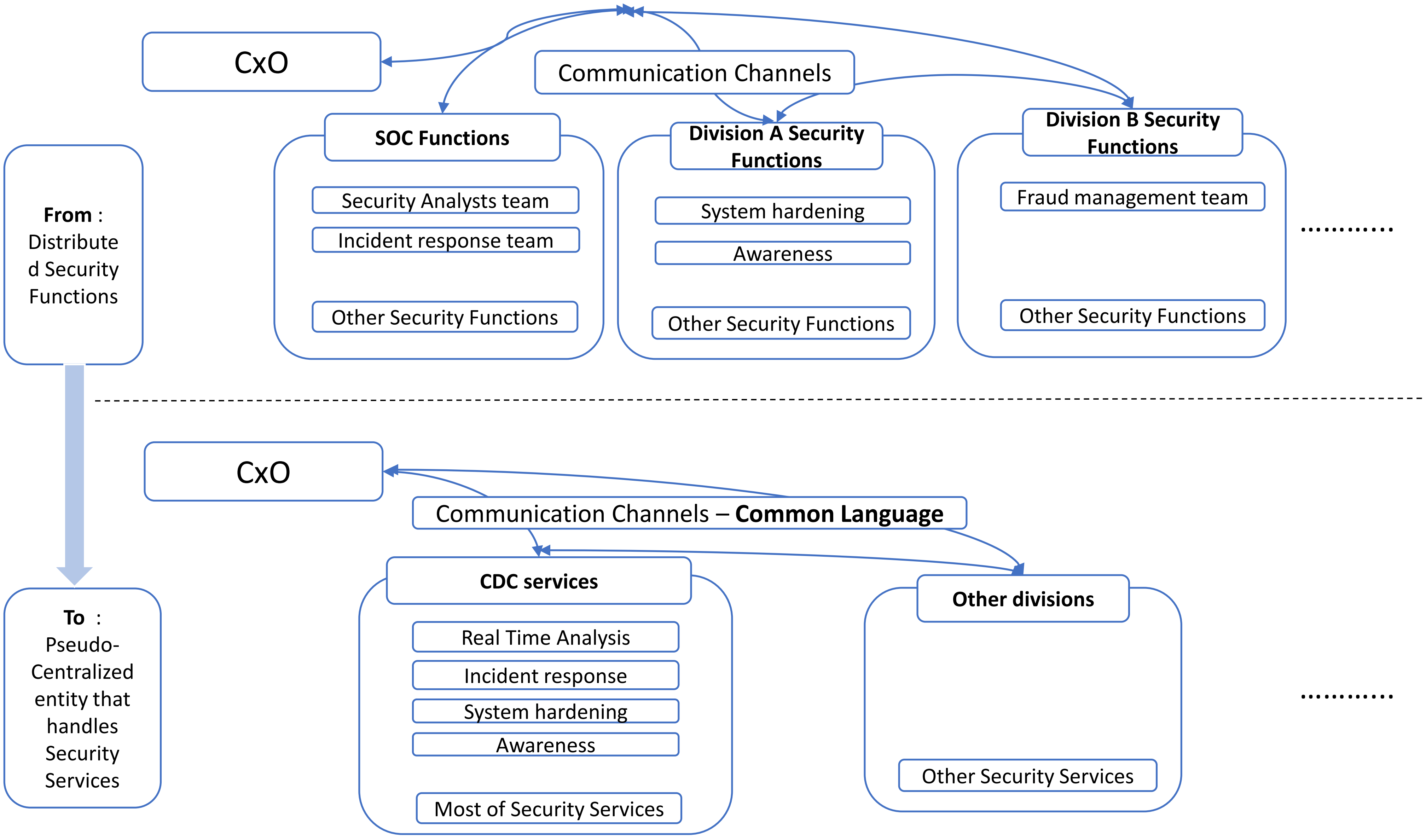
How to Design a CDC?(1)
(Service Profile)

- The services outlined in X.1060 are comprehensive and covers the necessary components for an **entity** capable of managing security services effectively.

- A service could be implemented as an entity/Team, such as a team that handle **Penetration Testing (E.5)**.

- An entity/Team can handle a set of services --> **incident response** team can handle services defined in **Category D**.

Can we centralize security services ?



From : Distributed Security Functions

CxO

Communication Channels

SOC Functions

Security Analysts team

Incident response team

Other Security Functions

Division A Security Functions

System hardening

Awareness

Other Security Functions

Division B Security Functions

Fraud management team

Other Security Functions

…………

To : Pseudo-Centralized entity that handles Security Services

CxO

Communication Channels – **Common Language**

CDC services

Real Time Analysis

Incident response

System hardening

Awareness

Most of Security Services

Other divisions

Other Security Services

…………

What we have Achieved?

- What we aimed for:
  - Creating a central entity called CDC!
  - The entity (CDC) will handle security services
- What we achieved
  - Migrate a lot of security functions to a central entity
  - Not all functions were migrated
  - Add other security services
  - Create a common language
  - Reduce and facilitate communication
  - Make **security capabilities** evaluation processes easier

CDC is up and running

How is X.1060 still helping

How to assess services and plan for improvement?

Tables in section 9.3 are a good reference in the assessment process

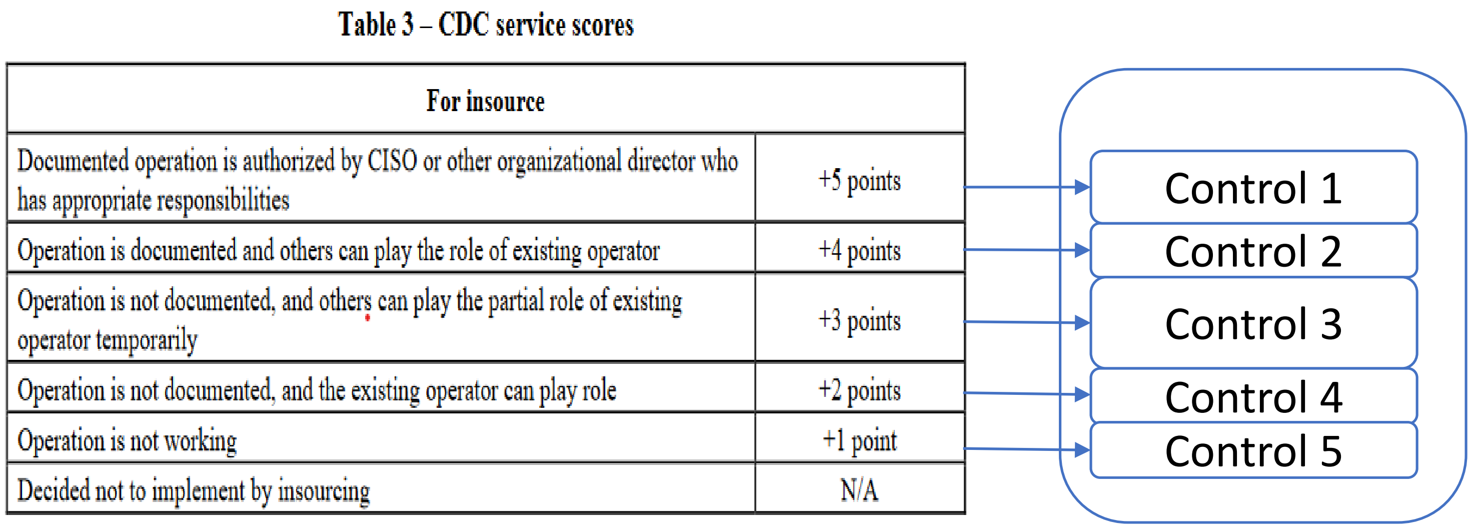
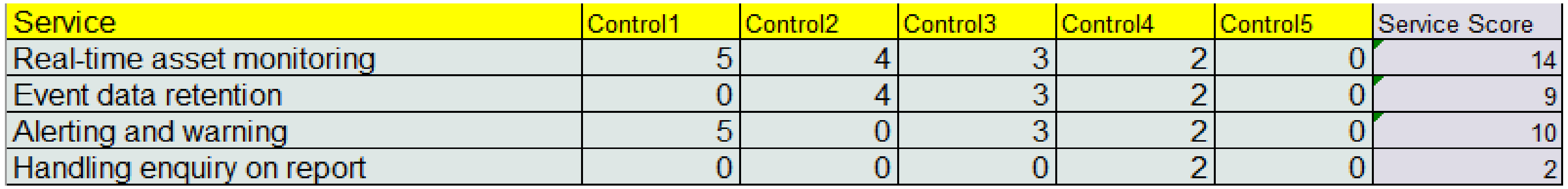


Table 3 – CDC service scores

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

Control 1
Control 2
Control 3
Control 4
Control 5



Service	Control1	Control2	Control3	Control4	Control5	Service Score
Real-time asset monitoring	5	4	3	2	0	14
Event data retention	0	4	3	2	0	9
Alerting and warning	5	0	3	2	0	10
Handling enquiry on report	0	0	0	2	0	2

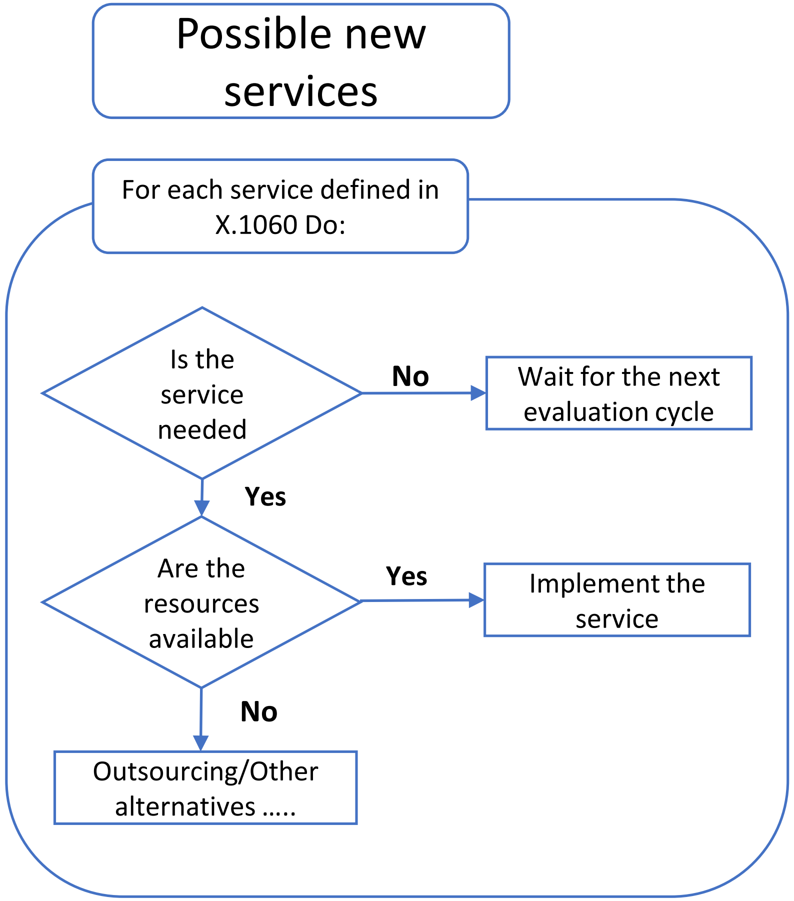
How to measure services performance (KPI)?

- This is out of scope of X.1060 recommendation
- What we gathered
  - Each service is specific
  - No universal performance indicators can be applied to all services.

- The following path was followed:
  - Create KPI measurements for each service/team
  - Evaluate each service/team separately
  - Create indicators for measuring the CDC as a whole

How to evaluate the CDC (services)?

- Evaluation should be periodic



Possible new services

For each service defined in X.1060 Do:

Is the service needed

No

Wait for the next evaluation cycle

Yes

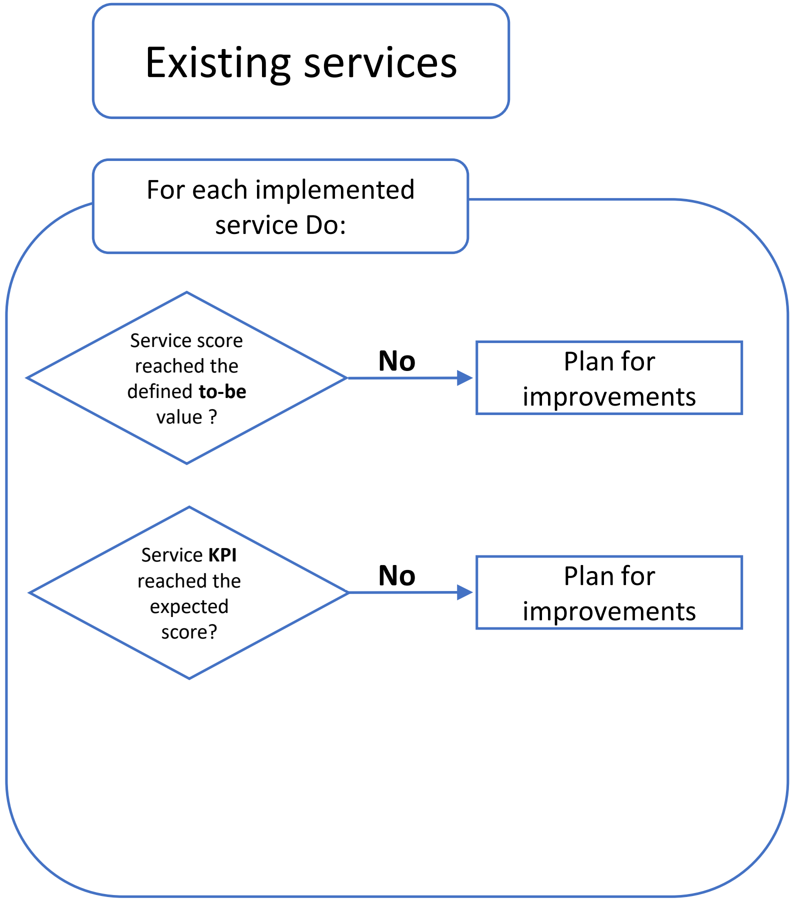
Are the resources available

Yes

Implement the service

No

Outsourcing/Other alternatives .....



Existing services

For each implemented service Do:

Service score reached the defined **to-be** value ?

No

Plan for improvements

Service **KPI** reached the expected score?

No

Plan for improvements

Thank you!

Abdenour.Bourennane@algerietelecom.dz
+213661866747