ITU-T SG17 Mini Workshop on ITU-T X.1060

Exploring the Transformative Journey: Algeria Telecom's Implementation of the X.1060 Framework

Abdenour Bourennane

Algérie Télécom

إتصالات الجزائر
ALGERIE TELECOM
دائما أقرب

22 February 2024
Geneva, Switzerland

Objectives

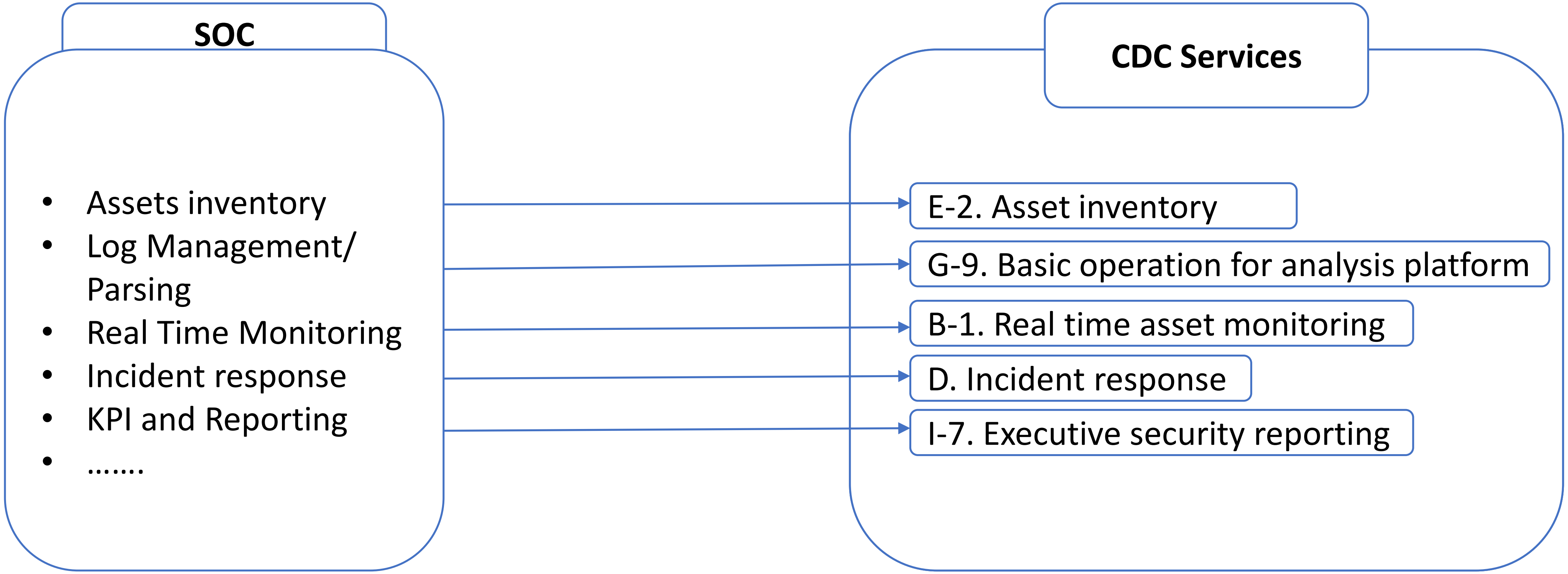
- Increase security capabilities.

- Establishment an entity that handles Cyber security services/operations.

- Create a common language for stakeholders.

The shift from SOC to CDC

- SOC functions were mapped to CDC services



SOC

- 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

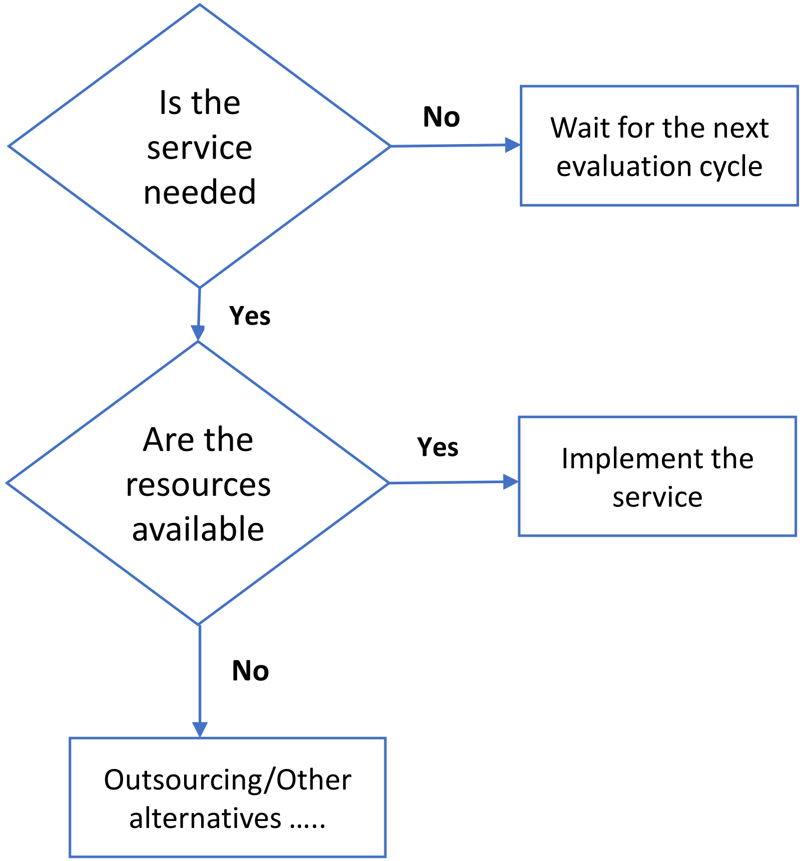
D. Incident response

I-7. Executive security reporting

The New Services

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

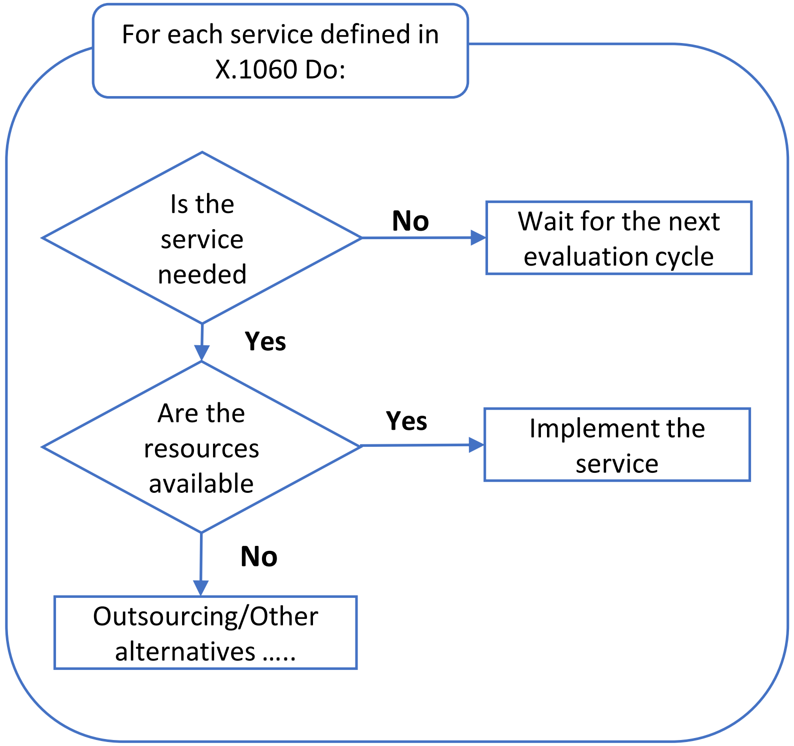
Considering these questions assisted in identifying the required services for implementation and determining the optimal approach for their execution.


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

Service Evaluation

- 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

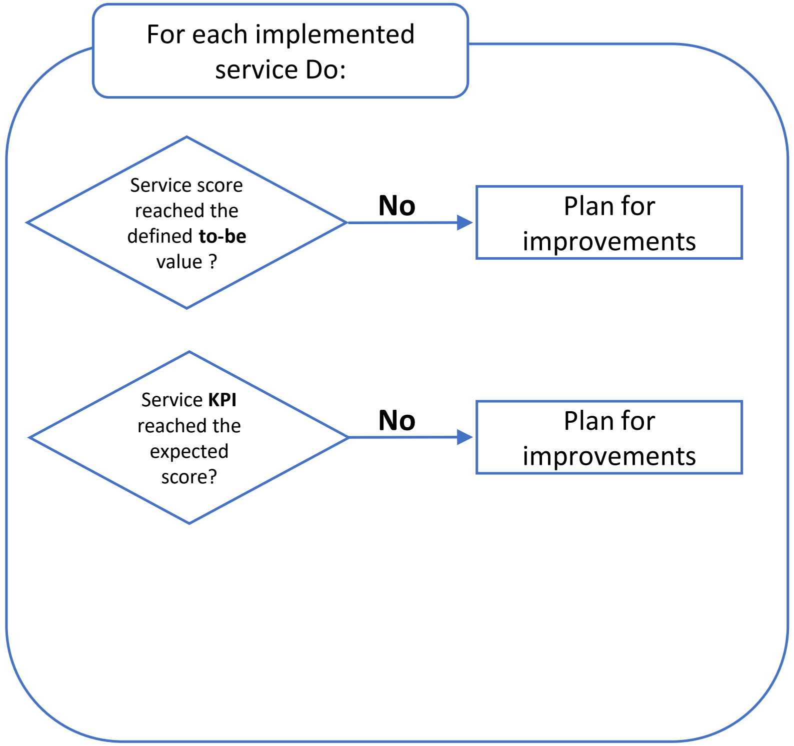
Yes

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

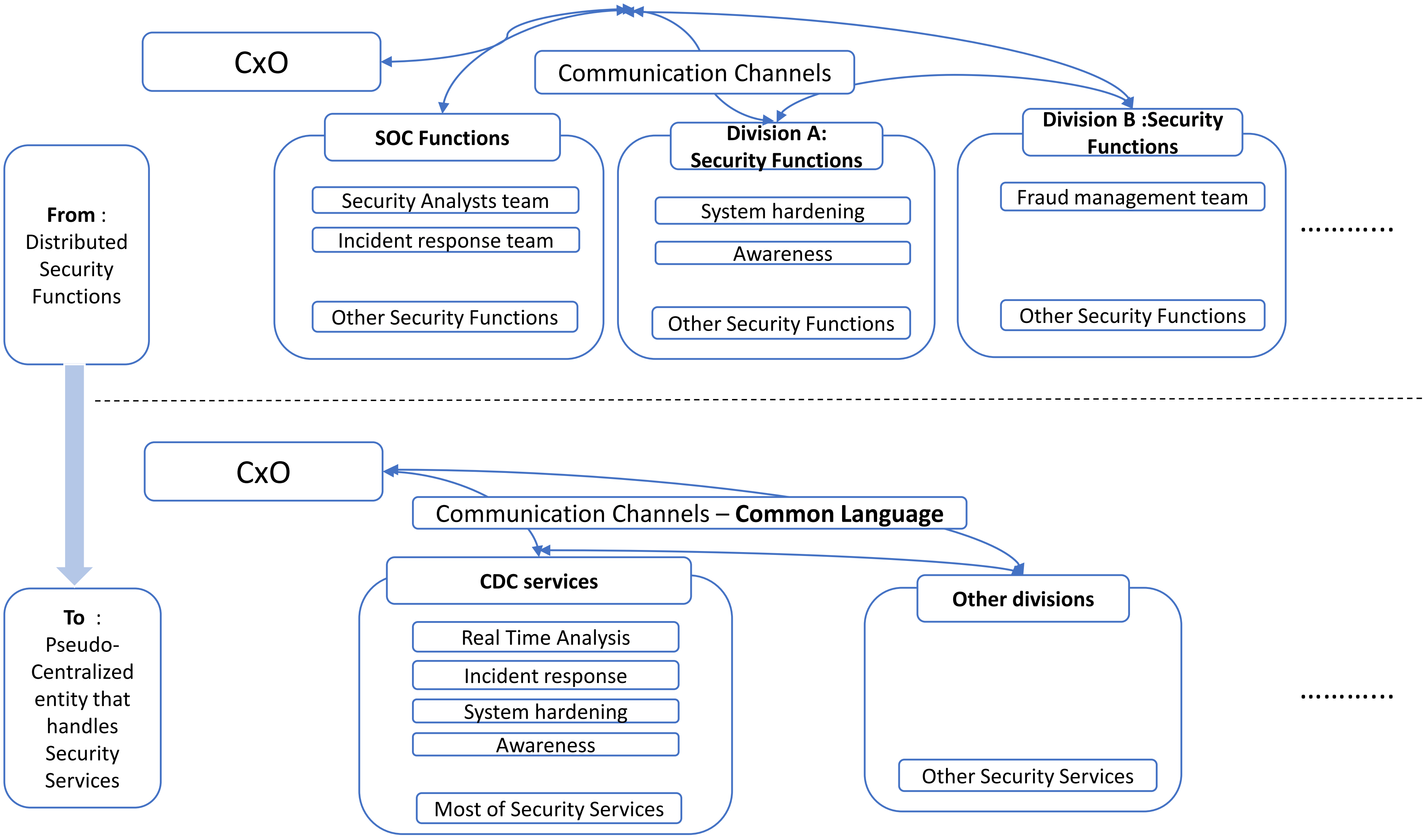
The organizational structure - 1

- The services detailed in X.1060 are extensive and address the essential elements needed for an **entity** to proficiently handle security needs.

- 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**.

The organizational structure -2



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

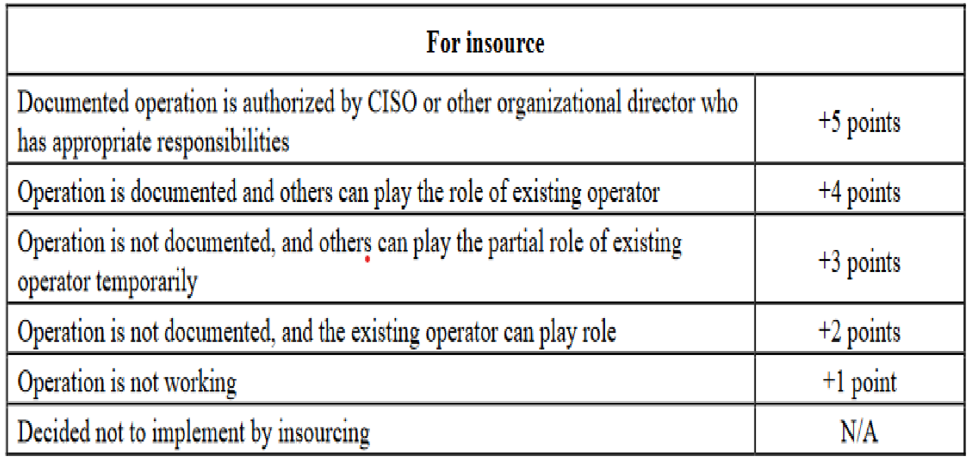
Other divisions

- Other Security Services

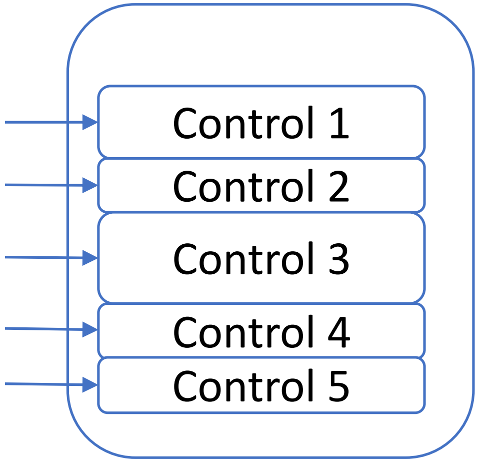
....

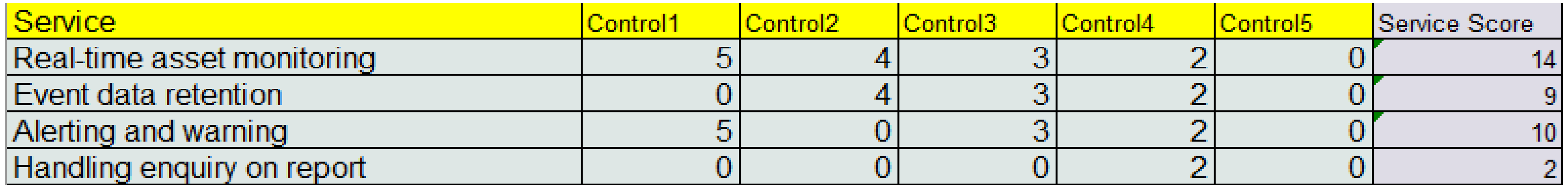
Service Assessment -1

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

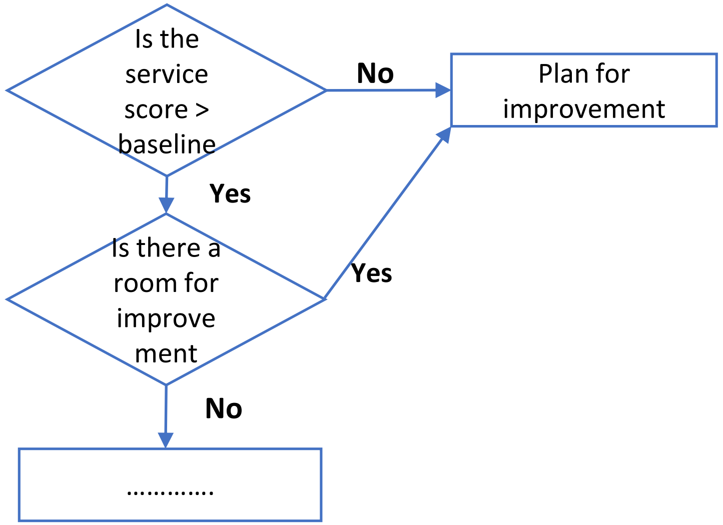




Service	Control1	Control2	Control3	Control4	Control5	Service Score
Real-time asset monitoring	5	4	3	2	0	14
Event data retention	0	4	3	2	0	9
Alerting and warning	5	0	3	2	0	10
Handling enquiry on report	0	0	0	2	0	2

Service Assessment -2

- The process of assessment:
  - Define a value that is considered good enough (a baseline)



Is the service score > baseline
No
Plan for improvement
Yes
Is there a room for improve ment
Yes
No
………….

Service Performance (KPI) -1

It is beyond the scope of the X.1060 recommendation.

Each service exhibits distinct characteristics.

It is not feasible to establish universal performance indicators applicable to all services.

Service Performance (KPI) -2

The methodology pursued involved:

- Re-using the Same KPIs used to measure SOC performance.
- Developing Key Performance Indicator (KPI) metrics tailored to individual services/teams.
- Assessing each service/team independently.
- Formulating metrics to assess the overall performance of the CDC.

Service Performance (KPI) -3

- Example: KPIs for services B1 and B3.
  - Mean Time to Detect
  - Mean Time to Attend and Analyze
  - Ratio of Detected/Not Detected Attacks
  - Ratio of Monitored/Not Monitored Assets

  ………

Added Value of X.1060

- Facilitates straightforward exploration and comprehension.

- Applicable to both C-level Executives and technical teams alike.

- Establishes a standardized communication conduit.

- Adaptable and offers numerous implementation possibilities.

Thank you!

Abdenour.Bourennane@algerietelecom.dz
+213661866747