WSIS FORUM 2022
Starting on 15 March
Final week 30 May - 3 June

Cyber Defence Centre Framework Survey Results (ITU-T Study Group 17)

Kwadwo G. Osafo-Maafo
(kwadwo.osafo-maafo[at]nca.org.gh)
ITU-T SG 17 Vice Chair, and Regional Group for Africa Chairman
Ghana, National Communications Authority

Objectives

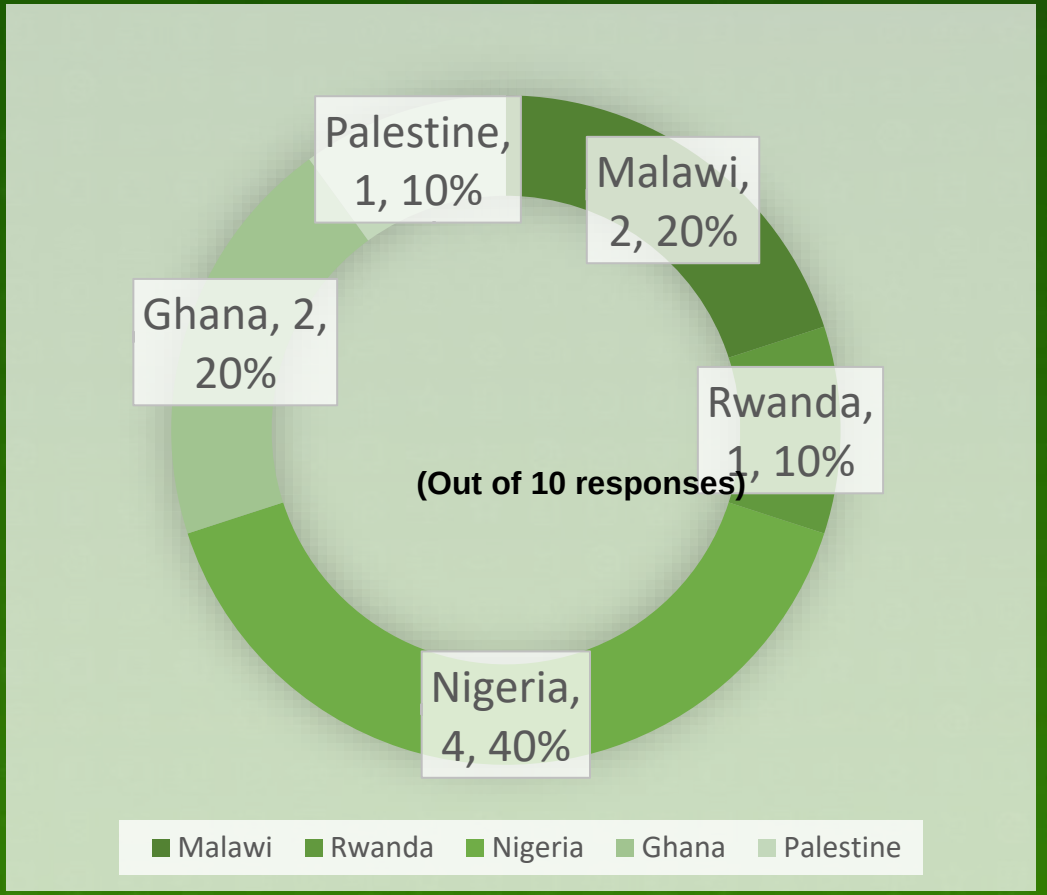
- Understand the background for X.1060, CDC and Africa Region's interest
- Appreciate the survey results and discuss on how to improve the survey and regional group participation
  - Share some perspectives from Ghana
- Encourage more participation, utilization and contribution to security through ITU-T SG 17

Cyber Defence Centre framework survey results

- ITU-T Recommendation X.1060: Framework for the creation and operation of a Cyber Defence Centre (CDC) is a new Recommendation developed by SG17 in 2021.
- A CDC is an entity that **provides security services** in an organization **to manage cybersecurity risks** associated **with its business activities**.
- ITU-T X.1060 provides a framework to build and manage a CDC and to evaluate its effectiveness.
- A portfolio of 54 services that a CDC should have is specified in nine categories.
- This survey was motivated by the interest of some African countries and was conducted (until end of March 2022) with the aim of **understanding the status of cybersecurity measures related to CDC, including SOC, CERT, CSIRT** etc., in African countries that may wish to adopt the X.1060 framework.

Profile of Survey Responses

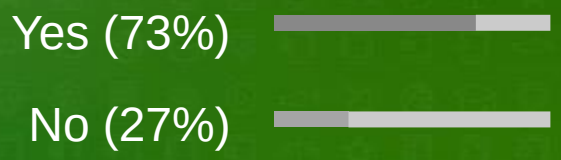
- 21 respondents in total
- Countries represented – see chart
- 11 respondents (52%) chose to remain anonymous
- Organizations represented:
- 6 governmental organizations
- 3 security agencies, 1 telecom regulator; 1 ministry
- 1 from academia
- 1 from the private sector



CDC Survey Results

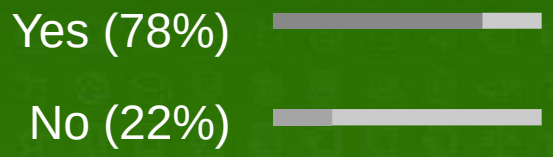
- Countries with legal requirement to establish an organization/unit for CDC services

(Out of 45 responses)



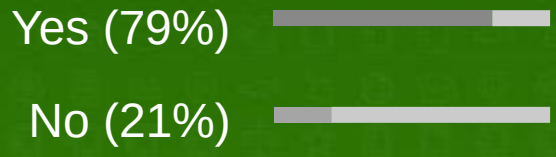
- Organizations with cybersecurity strategies or security policies

(Out of 18 responses)



- Organizations with CDC related services

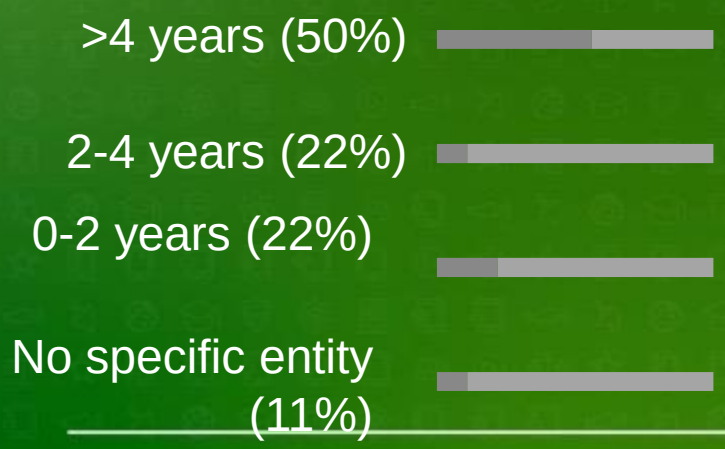
(Out of 14 responses)



CDC Survey Results

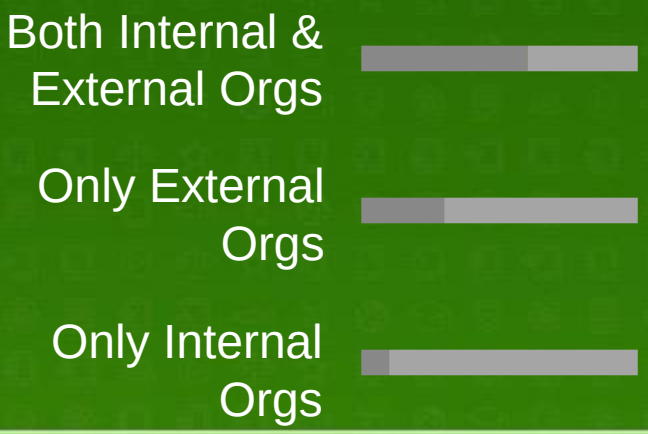
- Period of Establishment

(Out of 9 responses)



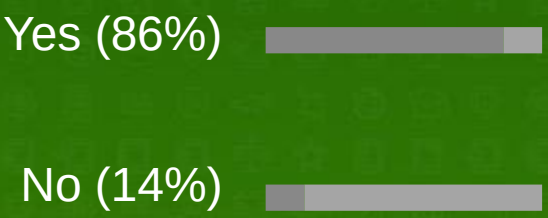
- Organizations that CDC Provides services to

(Out of 9 responses)



- Organizations with a management process for continuous improvement

(Out of 7 responses)



CDC Survey Results

2 **Organizations do not plan to implement CDC services**

10 **Organizations have a designated CSO or CISO**

6 **Organizations with entities responsible for CDC services**

Organizations with CDC related services

Malawi

- Malawi CERT

Rwanda

- Strategic management of CDC
- Real-time analysis
- Deep analysis
- Incident response checking & evaluation
- Collection, analysis & evaluation of threat intelligence
- Development & maintenance of CDC platforms
- Support of internal fraud response
- Active relationship with external parties

Nigeria

- Information security assurance for ICT assets
- Business continuity and incident response teams
- Strategic management of CDC
- Real-time analysis
- Incident response checking & evaluation
- Active relationship with external parties

Ghana

- Receiving, analysing & responding to cybersecurity incidents across all sectoral CERTs
- Coordinating with FIRST
- Operationalising the 24/7 cybercrime/cybersecurity incident reporting Points of Contact (PoC);
- Threat intelligence gathering and analysis
- Issuance of alerts and advisories on potential, imminent or actual cyber threats, vulnerabilities or incidents affecting Ghana's cyber ecosystem

State of Palestine

Palestine CERT (PALCERT) has many services such as:

- Awareness
- Incident handling
- Security information & event management
- Training
- Digital forensics
- Drafting policies and procedure
- Risk assessment
- Risk management
- Auditing of policy implementation

Additional comments/questions provided by respondents

Ghana

Ghana operates a decentralised system in our approach towards addressing cybersecurity risks. The country has more than one Cyber Defence Centre (CDC) comprising the national and sectoral level CDCs. The national CDC is the National Computer Emergency Response Team (CERT-GH) under the Cyber Security Authority (CSA) which coordinates responses from the sectoral CDCs. Hence, the responses provided in this questionnaire are based on our decentralised system and coordinated approach in dealing with cybersecurity risks and threats.

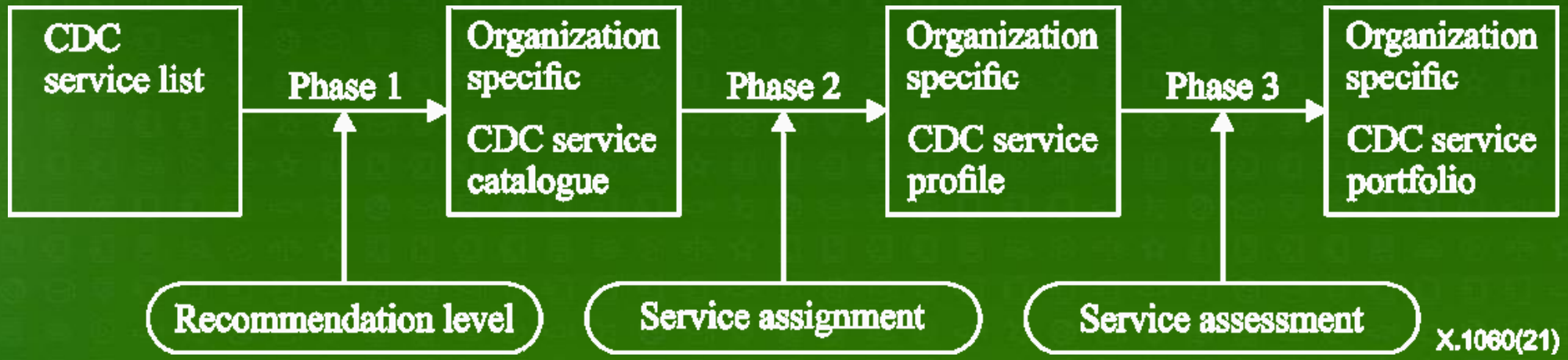
Nigeria

This survey focuses on organisational level CDCs. How do you measure for Nations and Sectors?

CDC Service List

Category A	Strategic management of CDC
Category B	Real-time analysis
Category C	Deep analysis
Category D	Incident response
Category E	Checking and evaluation
Category F	Collection, analysis and evaluation threat intelligence
Category G	Development and maintenance of CDC platforms
Category H	Support of internal fraud response
Category I	Active relationship with external parties

Phases to build Services for CDC



See X.1060, Figure 3 – Phases to build services for CDC

CDC Service Implementation Summary

- Service categories implemented by the most organizations are Categories A and B (by 9 organizations); while the least are Categories C and H (by 5 organizations).
- General trend observed for the preferred service assignment is insourcing; second preferred is a combination of insourcing and outsourcing
- Outsourcing is “least preferred” and not assigned for most services by majority of the respondent organizations:
  - It is only assigned in 5 categories A (A-2, A-13), C (C-2), E (E-5), F (F-2, F-4) and I (I-7)
- Category D is the only category without unassigned services:
  - All other categories have 1 or more unassigned services but there is no information on the specific reason for this – any possible future surveys could explore this aspect

CDC Service Category A

Strategic management of a 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

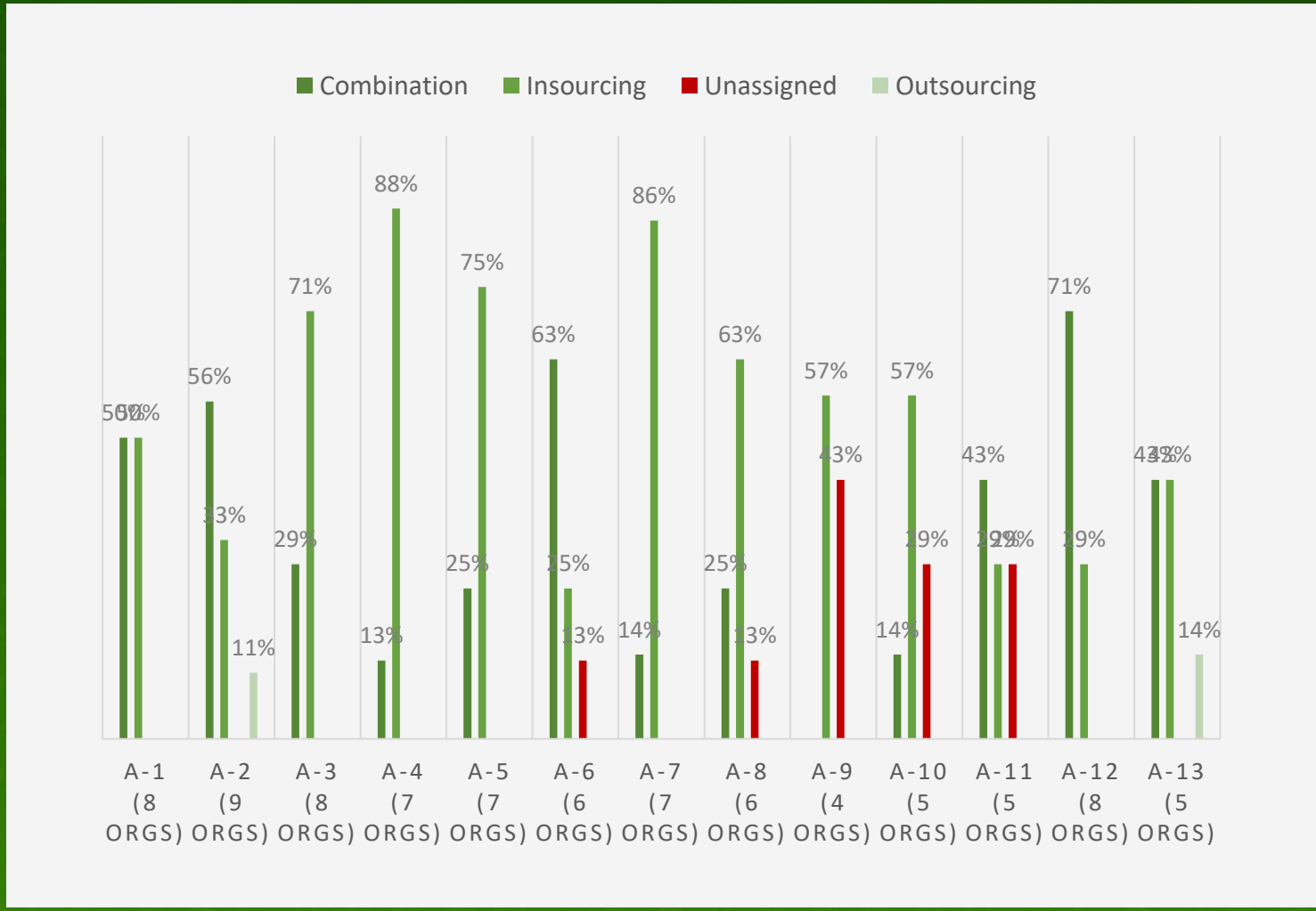
A-9: Triage criteria management

A-10: Counter measures selection

A-11: Quality management

A-12: Security audit

A-13: Certification



Category A: Strategic management of a CDC Observations

- A-2 (Risk Assessment) is the most implemented service (by 9 orgs) and A-9 (Triage Criteria Management) is the least implemented (by 4 orgs)
- Insourcing appears to be preferred CDC service assignment (majority in 7 out of 13 services):
  - 51% of respondents (avg) document operations and others play the role of existing operator (service score “+4 points”)
- Combination of insourcing and outsourcing observed for majority of services:
  - Preferred service assignment for A-2 (Risk Assessment), A-6 (Business Impact Analysis), A-11 (Quality Management) and A-12 (Security Audit) but is not offered for A-9 (Triage Criteria Management)
- Two services (A-2 and A-13) are exclusively outsourced by some respondent organizations
- 45% of respondents (average) choose not to implement outsourcing (service score “N/A”)
- Four services (A-6, A-8, A-9, A-10, A-11) are unassigned: (Business impact analysis, Security architecture design, Triage criteria management, Counter measures selection, Quality management)
  - A-9 is the most common unassigned service: 43% of respondents do not give a service assignment for it

CDC Service Category B

Real-time Analysis

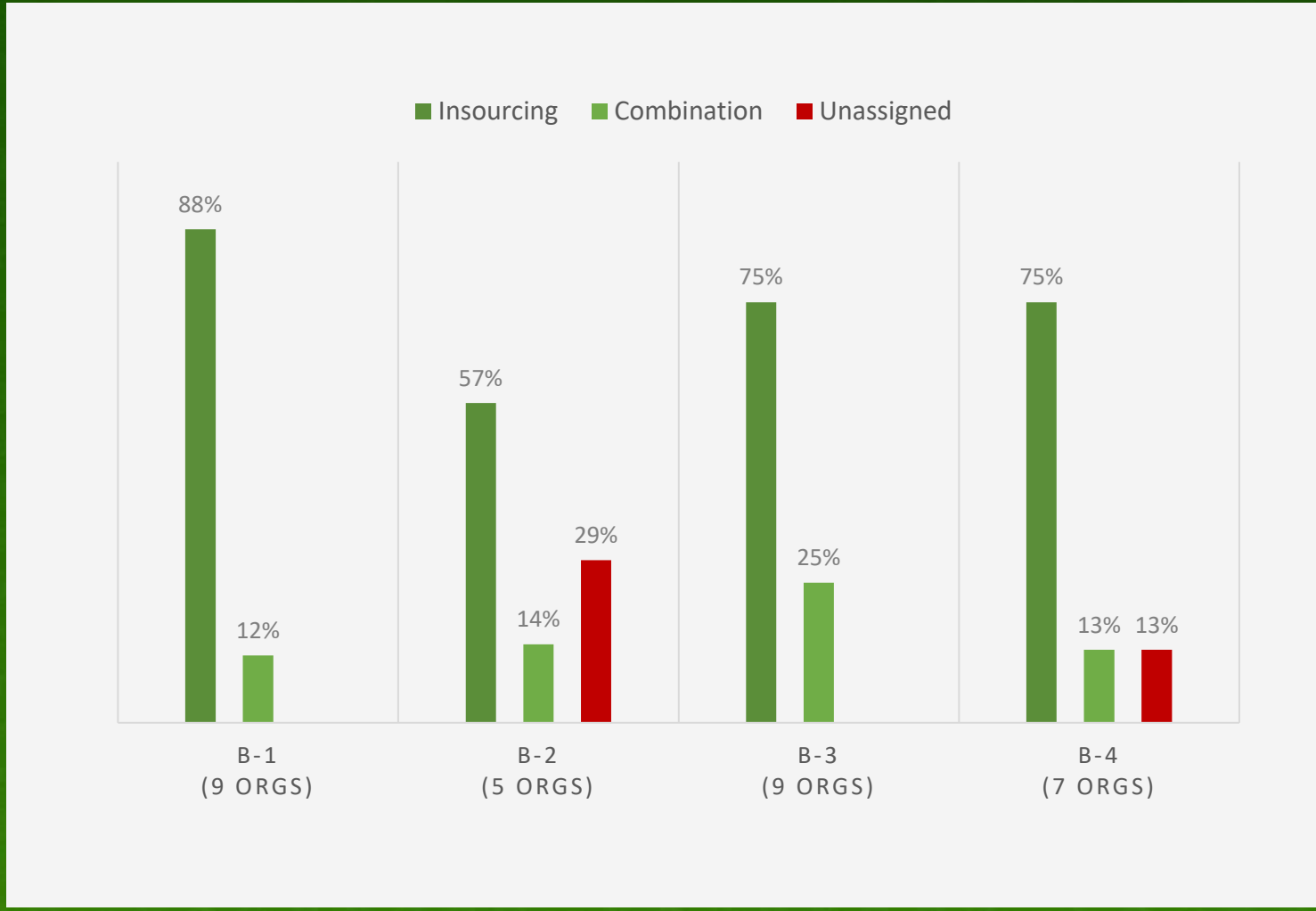
Constantly monitors and analyses logs and data from various systems, such as network devices, servers and security products.

B-1: Real-time asset monitoring

B-2: Event data retention

B-3: Alerting & warning

B-4: Handling inquiry on report



Category B: Real-Time Analysis
Observations from the Respondent Organizations

- B-1 and B-3 are the most implemented services (by 9 orgs each) while B-2 is the least implemented (by 5 orgs)
- Insourcing is preferred CDC service assignment (majority for all services):
  - 52% of respondents (avg) documented operation authorized by CISO or other organizational director with appropriate responsibilities (service score “+5 points”)
- None of the respondent organizations exclusively outsource real-time analysis
  - 53% of respondents (average) choose not to implement outsourcing (service score “N/A”)
- Combination of insourcing and outsourcing assigned for all services and two services (B-2, B-4) are unassigned

CDC Service Category C

Incident response

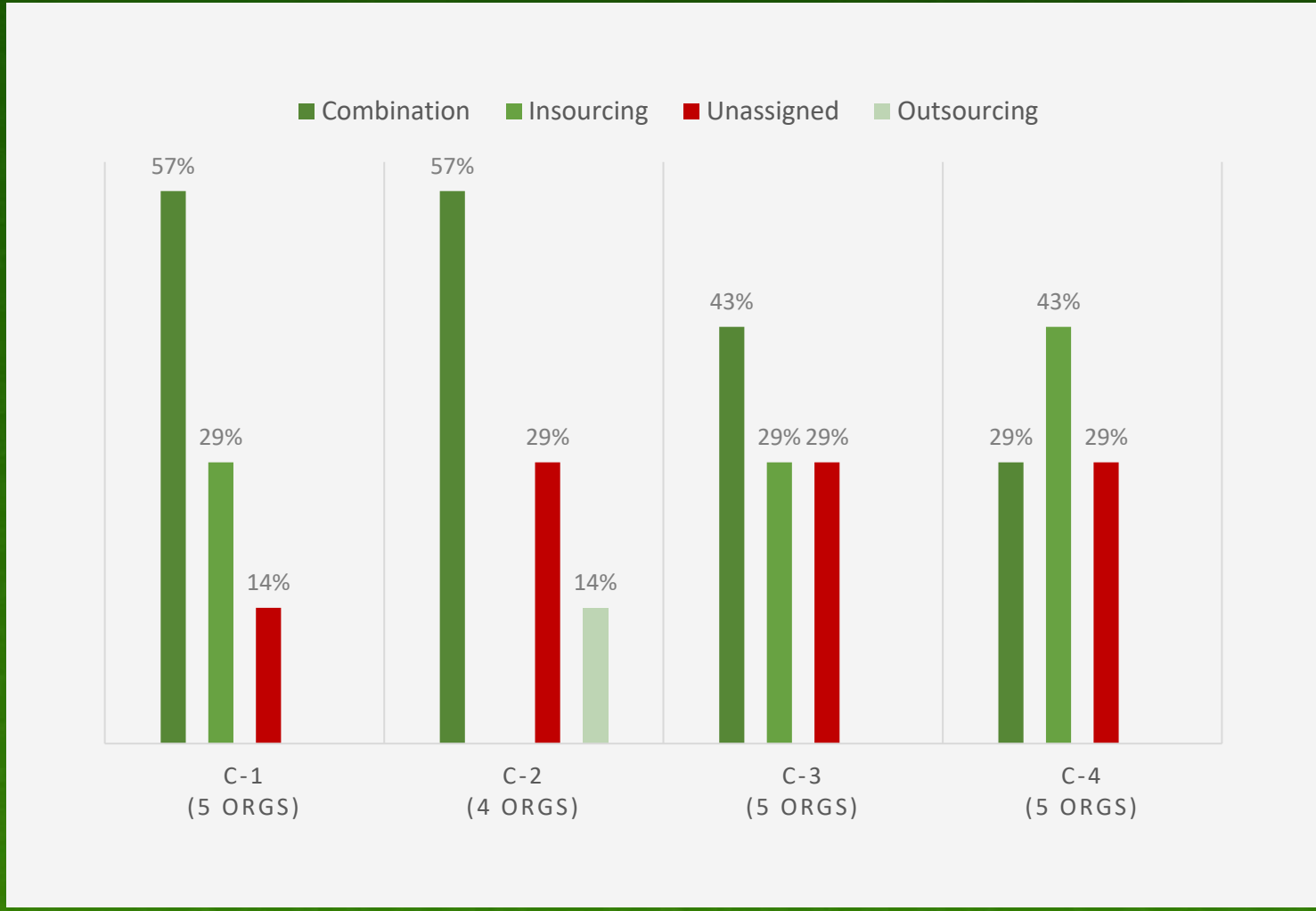
Related to the incident, reviewing the compromised data, and analysing the tools and methods used in the attack.

C-1: Forensic analysis

C-2: Malware sample analysis

C-3: Tracking & tracing

C-4: Forensic evidence collection



Category C: Deep Analysis

Observations from the Respondent Organizations

- C-1, C-3 and C-4 are the most implemented services (by 5 orgs each)
- Combination of insourcing and outsourcing is observed in C-1, C-2 and C-3 (majority)
- Outsourcing only applied in C-2 (malware sample analysis)
  - However, for outsourcing, 72% of respondents (avg) have documented operation authorized by CISO or other organizational director with appropriate responsibilities (service score “+5 points”)
- None of the respondent organizations exclusively insource C-2 (malware sample analysis)
- In 29% of respondent organizations, C-2, C-3 and C-4 are unassigned

CDC Service Category D

Deep Analysis

Takes specific actions based on the results of real-time analysis and threat information to deter and eliminate threats

D-1: Incident report acceptation

D-2: Incident handling

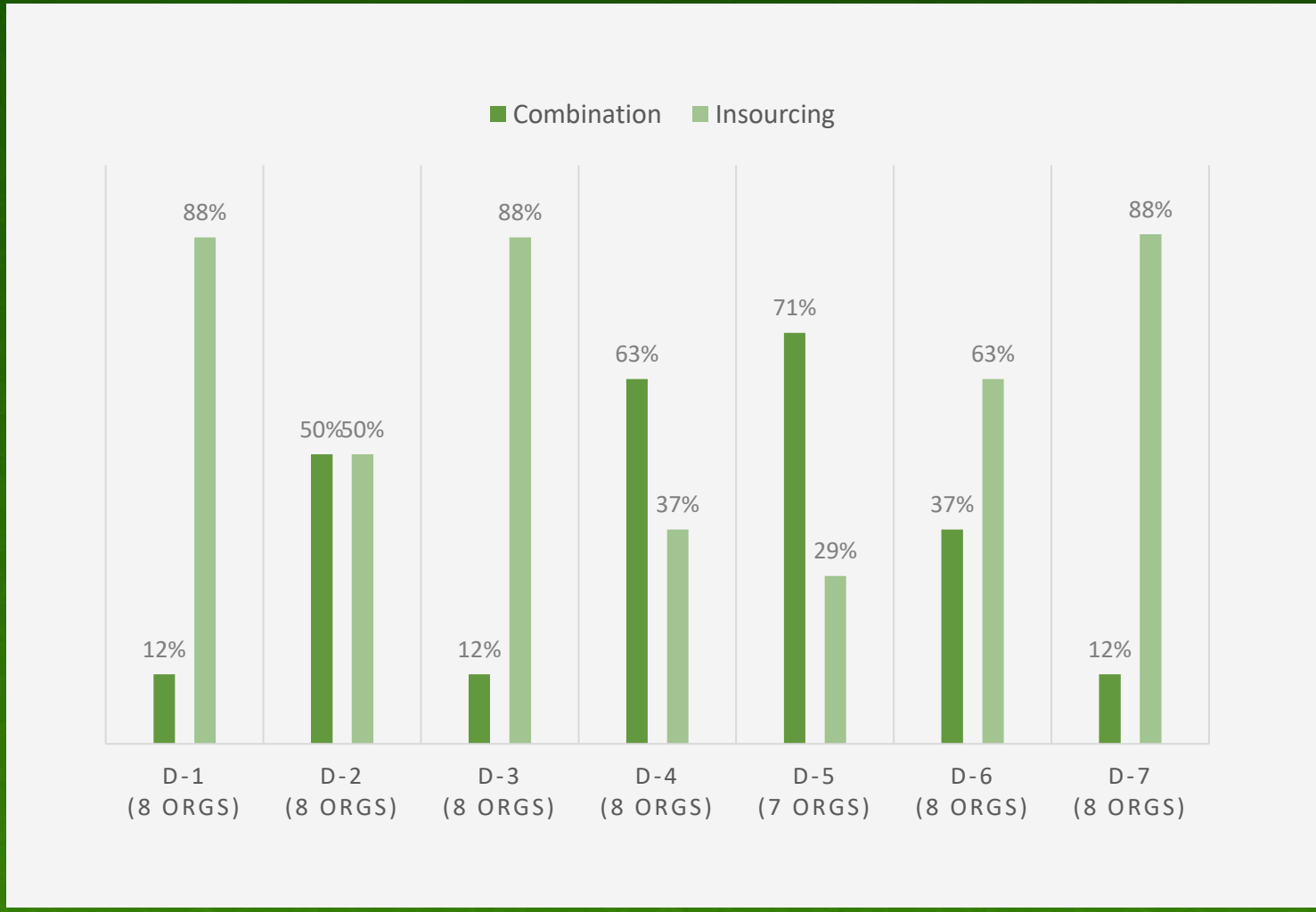
D-3: Incident classification

D-4: Incident response & containment

D-5: Incident recovery

D-6: Incident notification

D-7: Incident response report



Category D: Deep Analysis

Observations from the Respondent Organizations

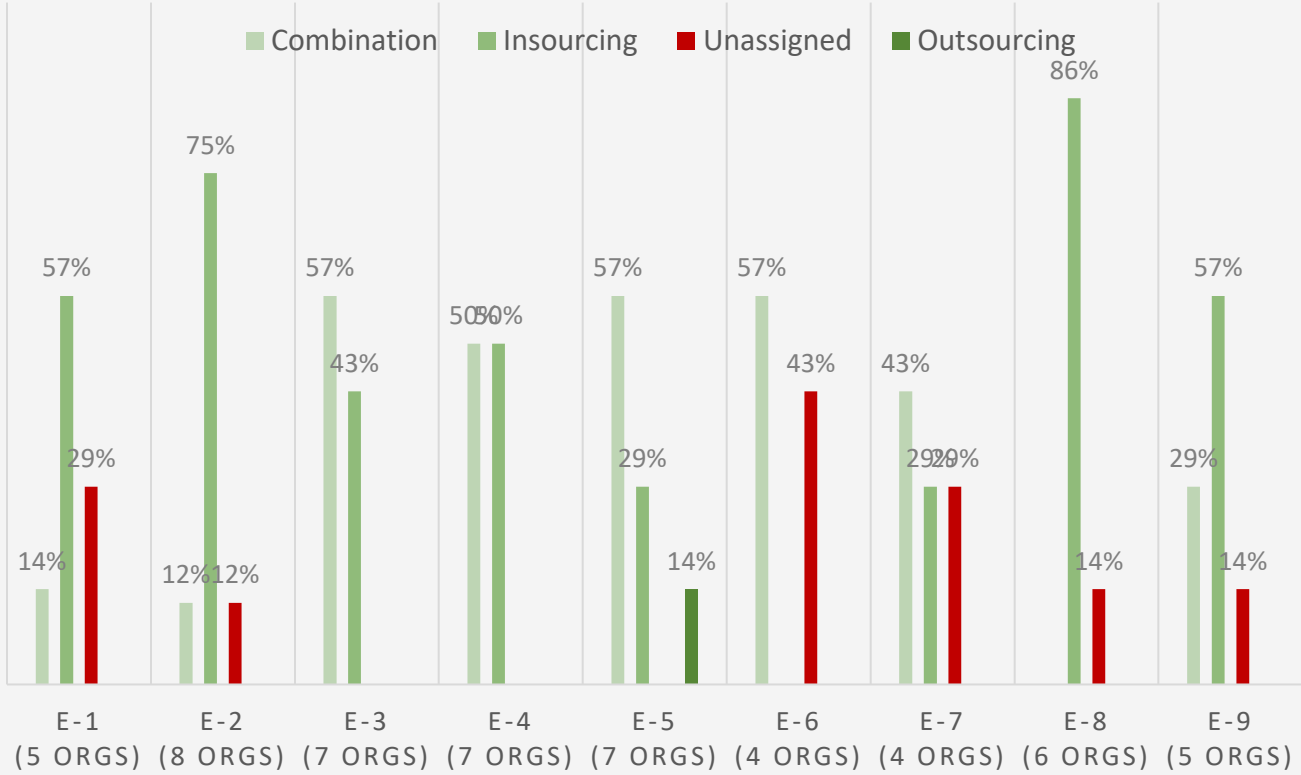
- 63% of respondent organizations (avg) apply insourcing for incident response
  - D-1, D-3 and D-7 services are each implemented by 88% of the respondents using insourcing
- Insourcing is preferred CDC service assignment for D-4 (incident response and containment) and D-5 (incident recovery)
  - 70% of respondents (avg) document their insourcing operations:
  - 23%, operation is authorized by CISO or other director with appropriate responsibilities (service score “+5 points”)
- 47%, others can play the role of existing operator (service score “+4 points”)
- None of the respondent organizations exclusively outsource
  - 50% of respondents (avg) choose not to implement outsourcing (service score “N/A”)

CDC Service Category E

Checking and evaluation

For vulnerability assessment of systems to be protected, and incident response training and its evaluation

E-1: Network information collection
E-2: Asset inventory
E-3: Vulnerability assessment
E-4: Patch management evaluation
E-5: Penetration test
E-6: Defence capability against APT attack evaluation
E-7: Handling capability on cyber attack
E-8: Policy compliance
E-9: Hardening



Category E: Checking and evaluation
Observations from the Respondent Organizations

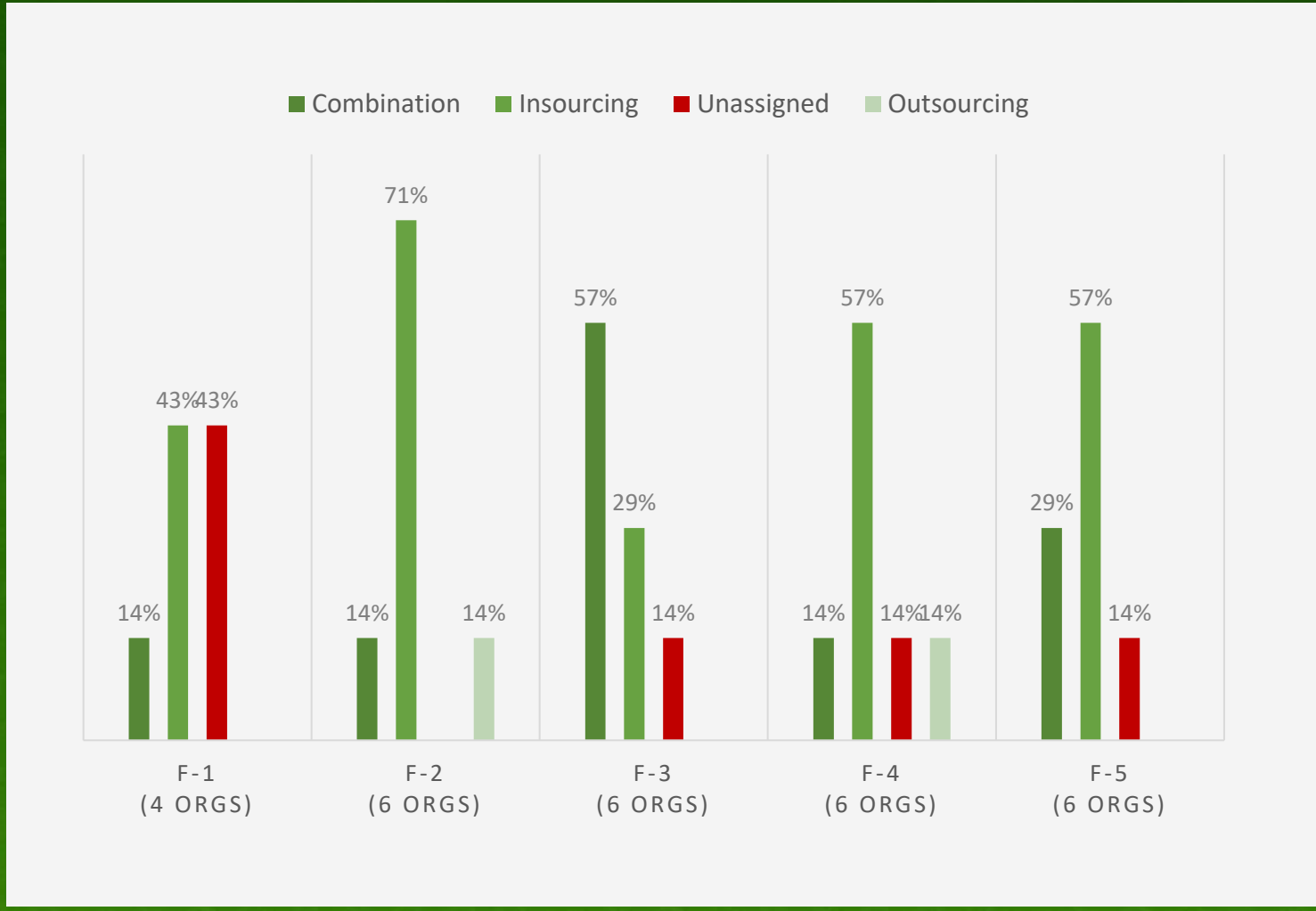
- E-2 is the most implemented service (by 8 orgs) and E-6; E-7 are the least implemented (by 4 orgs)
- While insourcing is preferred CDC service assignment for E-8 (in 86% of respondents), it is not used for E-6
  - 53% of respondents (avg) document operations and others play the role of existing operator (service score “+4 points”)
- Combination of insourcing and outsourcing used for all services except E-8
- 53% of respondents (average) choose not to implement outsourcing (service score “N/A”)
- Outsourcing only applied in E-5 by 14% of respondents
  - However, for outsourcing, 65% of respondents (avg) have documented operation authorized by CISO or other organizational director with appropriate responsibilities (service score “+5 points”)

CDC Service Category F

Collection, analysis and evaluation of threat intelligence

Collects threat information on vulnerabilities and attacks (external intelligence) that is available on the Internet and handles information on real-time analysis and incident response (internal 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



Category F: Checking and evaluation

Observations from the Respondent Organizations

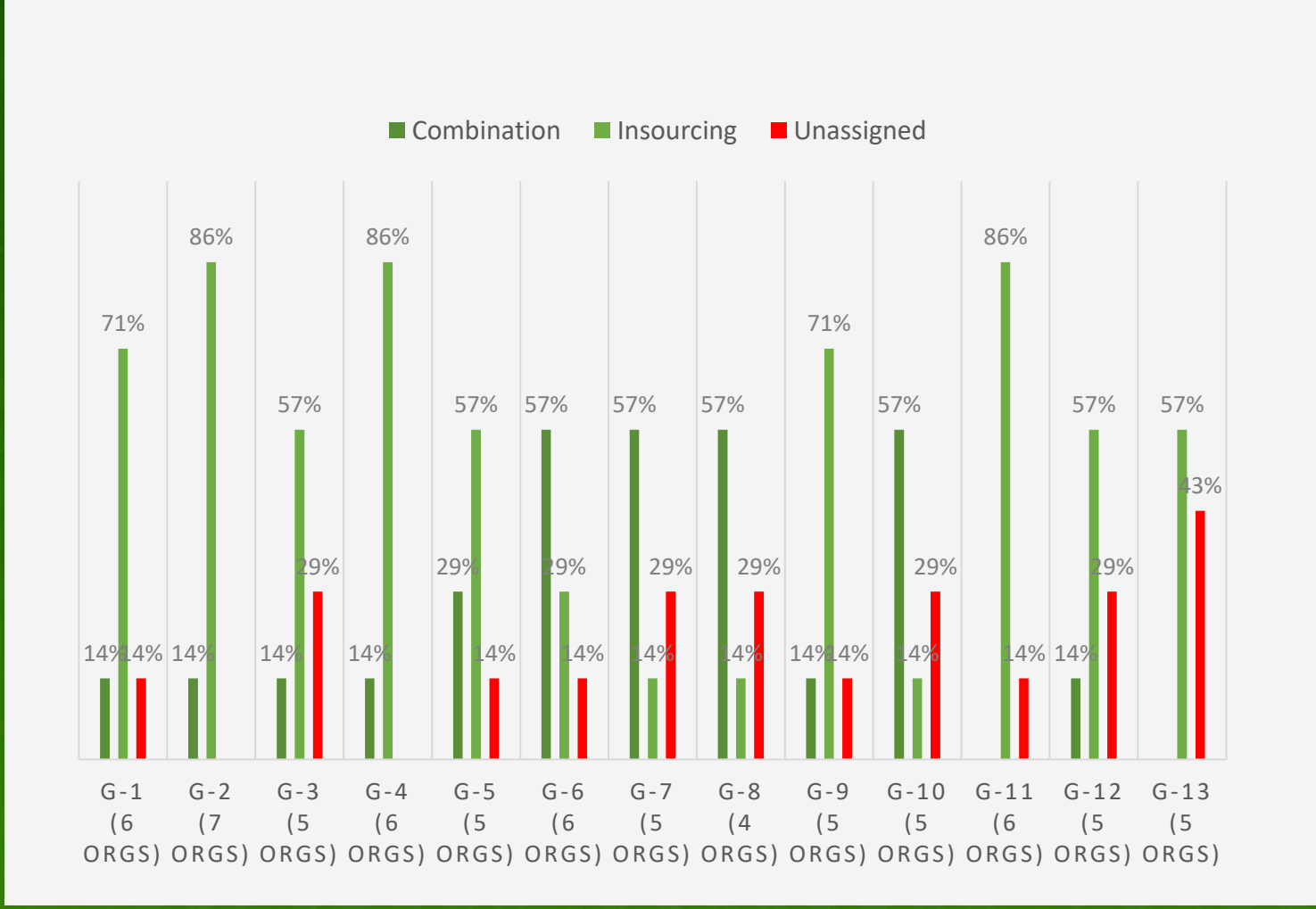
- F-2; F-3; F-4 and F-5 are the most implemented (by 6 orgs) and F-1 is the least implemented (by 4 orgs).
- Insourcing is preferred CDC service assignment for category F
  - Majority service assignment for 3 out of services (F-2, F-4 and F-5)
  - 47% of respondents (avg) document operations and others play the role of existing operator (service score “+4 points”)
- Combination of insourcing and outsourcing used for all services by the respondent organizations
- Outsourcing only applied in F-2 and F-4:
  - 42% of respondents have documented operation authorized by CISO or other organizational director with appropriate responsibilities (service score “+5 points”)
  - 47% of respondents choose not to implement outsourcing (service score “N/A”)
- F-1 is the most common unassigned service with 43% of respondents

CDC Service Category G

Development and maintenance of CDC platforms

Manages, improves or develops new systems that are necessary for security response.

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



Category G:

Observations from the Respondent Organizations

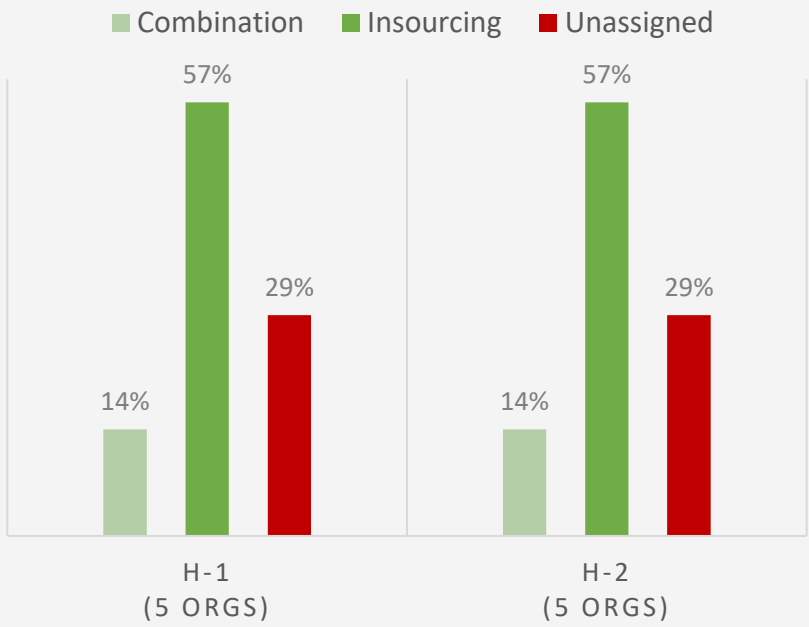
- G-2 is the most implemented (by 7 orgs) while G-8 is the least implemented (by 4 orgs).
- Insourcing appears to be preferred CDC service assignment (majority in 9 out of 13 services):
  - 52% of respondents (avg) have documented operation authorized by CISO or other organizational director with appropriate responsibilities (service score “+5 points”)
- Combination of insourcing and outsourcing used for all services except G-11 and G-13
- G-13 is the most common unassigned service with 43% of respondents
- None of the respondent organizations exclusively outsource
  - 58% of respondents (avg) choose not to implement outsourcing (service score “N/A”)

CDC Service Category H

Support of internal fraud response

Manages, improves or develops new systems that are necessary for security response.

H-1: Internal fraud response and analysis support
H-2: Internal fraud detection and reoccurrence prevention support



Category H: Support of internal fraud response

Observations from the Respondent Organizations

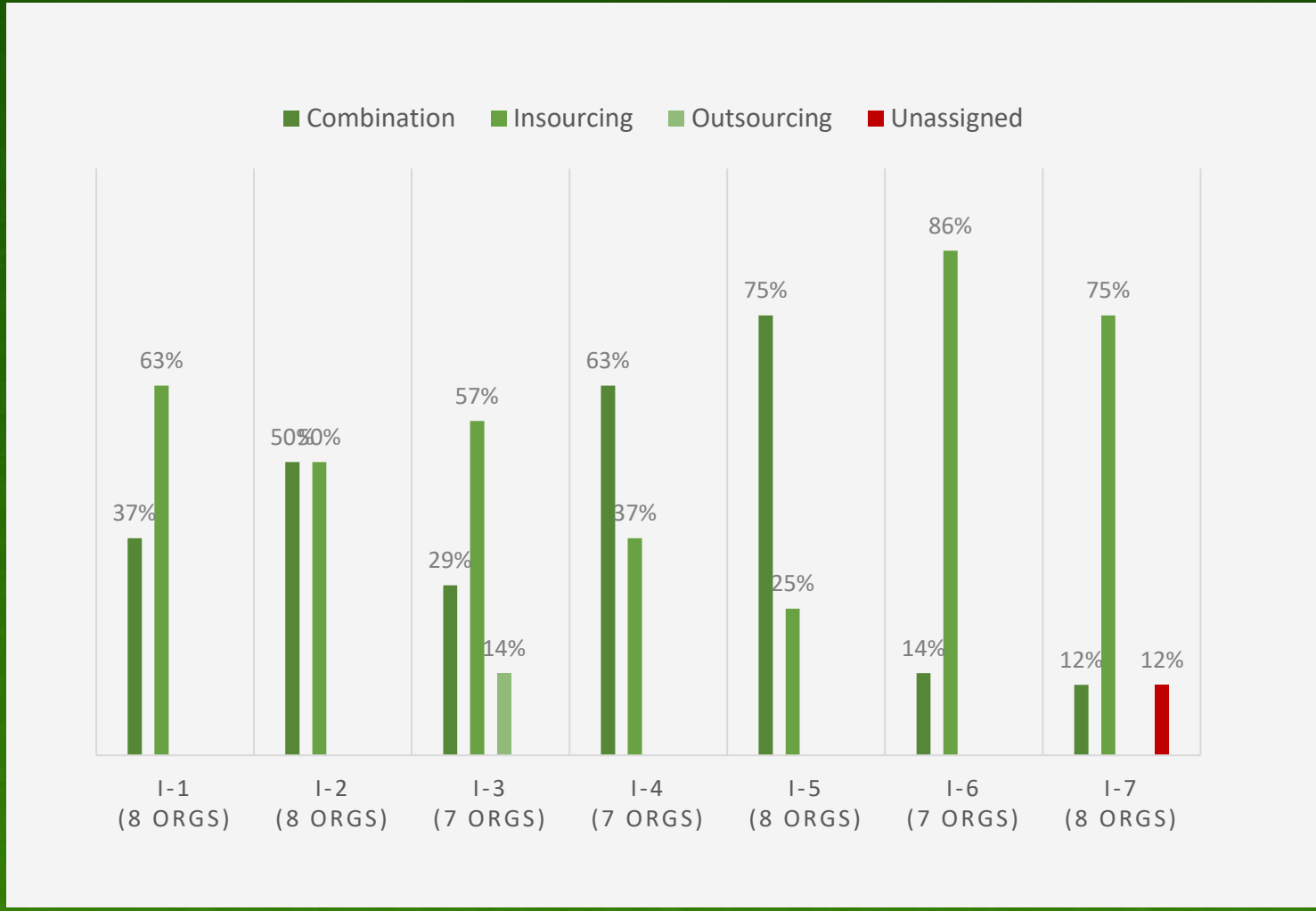
- H-1 and H-2 implemented using an identical approach in 5 organizations
- Insourcing appears to be preferred CDC service assignment for category H
- 80% of respondents (avg) document their insourcing operations:
  - 40%, operation is authorized by CISO or other director with appropriate responsibilities (service score “+5 points”)
  - 40%, others can play the role of existing operator (service score “+4 points”)
- Combination of insourcing and outsourcing used for all services
- None of the respondent organizations exclusively outsource
  - 75% of respondents (avg) choose not to implement outsourcing (service score “N/A”)

CDC Service Category I

Active relationship with external parties

Manages, improves or develops new systems that are necessary for security response.

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



Category I: Active relationship with external parties

Observations from the Respondent Organizations

- H-1 and H-2 implemented using an identical approach in 5 organizations
- Insourcing appears to be preferred CDC service assignment (majority in 4 out of 7 services):
- 42% of respondents (avg) have documented operation authorized by CISO or other organizational director with appropriate responsibilities (service score “+5 points”)
- Combination of insourcing and outsourcing appears to be most preferred for I-4 and I-5
- Outsourcing only applied in I-7:
- However, 41% of respondents (avg) have documented operation authorized by CISO or other organizational director with appropriate responsibilities (service score “+5 points”)
- I-3 is the only unassigned service

CDC service portfolio evaluation

- For evaluation, the difference between the current score and targeted score should be determined to help an organization to identify what needs to be improved.
- The survey collected data on both the targeted and current scores of each CDC service and the supplementary slides display the data collected on the targeted scores.
- The CDC evaluation process, however, is a self-evaluation i.e. each organization assesses the performance of their CDC services - what is required is a gap analysis on the service scores per organization and per service
- However, the objective of collecting the targeted scores was unclear:
  - Is the intention to evaluate each respondent organization's CDC service portfolio?
  - Is the data intended to be used to develop some benchmarks?
  - Is the purpose just to have a general view of existing target service scores?
- Analysis of these target scores is recommended after clarification on the objectives of collecting data on the target scores is provided

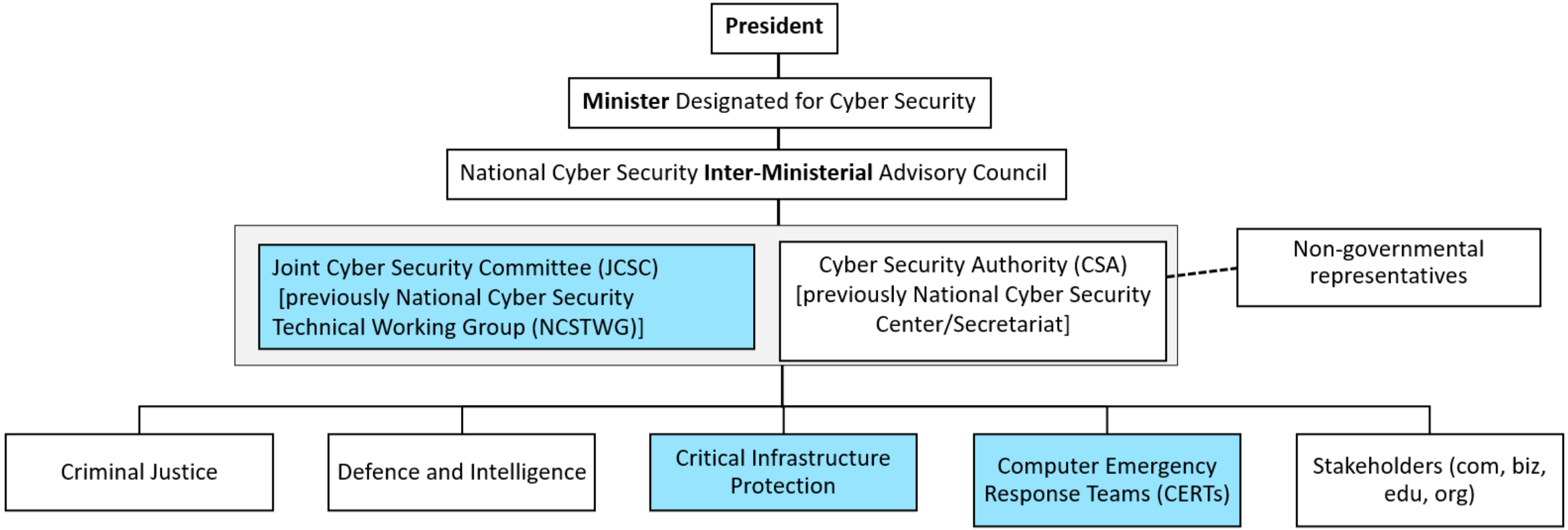
CDC service portfolio evaluation

- For evaluation, the difference between the current score and targeted score should be determined to help an organization to identify what needs to be improved.
- The survey collected data on both the targeted and current scores of each CDC service and the supplementary slides display the data collected on the targeted scores.
- The CDC evaluation process, however, is a self-evaluation i.e. each organization assesses the performance of their CDC services - what is required is a gap analysis on the service scores per organization and per service
  - However, the objective of collecting the targeted scores was unclear:
    - Is the intention to evaluate each respondent organization’s CDC service portfolio?
    - Is the data intended to be used to develop some benchmarks?
    - Is the purpose just to have a general view of existing target service scores?
  - Analysis of these target scores is recommended after clarification on the objectives of collecting data on the target scores is provided

Suggestions for the way forward

- Understanding of Context
  - Concerns, issues or suggestions including interests in ITU-T SG17
- Awareness of ITU-T SG 17
  - Awareness of CDC
  - Stakeholders identifies and engaged/targeted (appropriate respondents)
- Utilization of X.1060 and Survey
  - Expand on Survey (content, interviews, discussions)
  - Improve the tool to improve usefulness and quality of responses
- Participation
  - Engage more stakeholders on participation of activities relating SG 17 and workshops such as this one
- Contribution
  - Discussions, Interviews and Exercises
  - Feedback from stakeholders (all of us) to add to X.1060 use (e.g. supplements), lessons sharing

Cyber Security Ecosystem in Ghana



Critical Sectors in Ghana

- Public Sector (Government)
- Banking and Financial
- Telecommunication
- Energy and Utilities
- Military
- National Security
- Academic
- Health
- Transportation
- others

WSIS FORUM 2022
Starting on 15 March
Final week 30 May - 3 June

Thank You

www.wsis.org/forum