International
Telecommunication
Union

ORGANISATION
INTERNATIONALE DE
la francophonie

AfricaCERT
United in promoting cyber security in Africa

CIRT Creation Stages

INTRODUCTION

WHAT IS A CIRT

- CIRT Computer Incident Response Team
- CSIRT Computer Security Incident Response Team
- CERT Computer Emergency Response Team
- CIRC Computer Incident Response Capability
- IRC   Incident Response Center or Incident Response Capability
- IRT   Incident Response Team
- SERT Security Emergency Response Team
- SIRT Security Incident Response Team

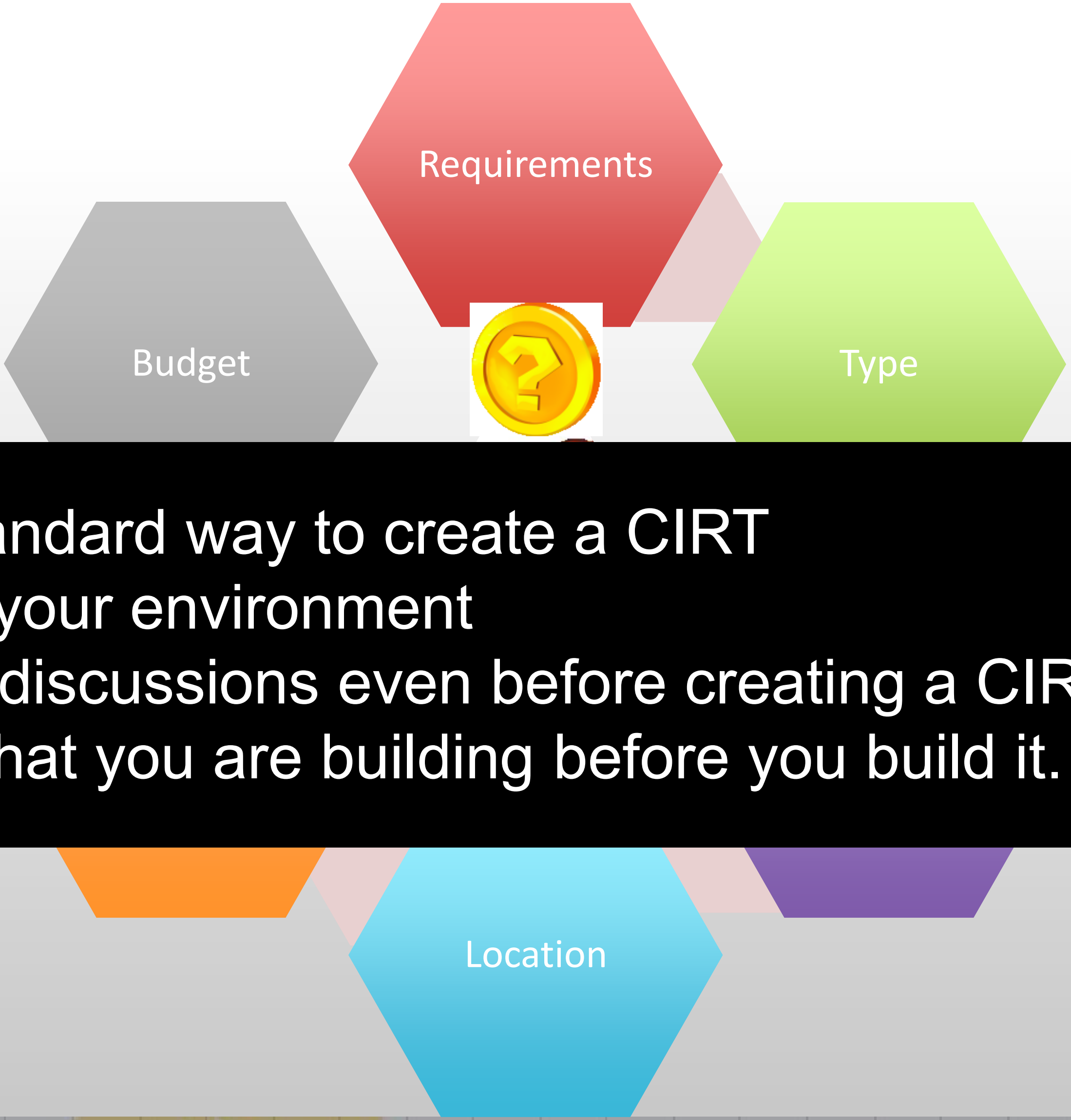
There are different types of CERT/CIRT or response teams
It could be for a government/private/organisation/region
The constituency/mission contributes to the services offered

TYPE OF INCIDENT RESPONSE TEAM

- National Incident Response Team
- Organizational Incident Response Team
  - Governmental CIRT
- Multi-Organizational Incident Response Team
  - UN-CSIRT , CERT-EU
- Sectorial Incident Response Team
  - Financial Institution CIRT
- Regional Incident Response Team
  - AfricaCERT, APCERT , OIC-CERT

INTRODUCTION

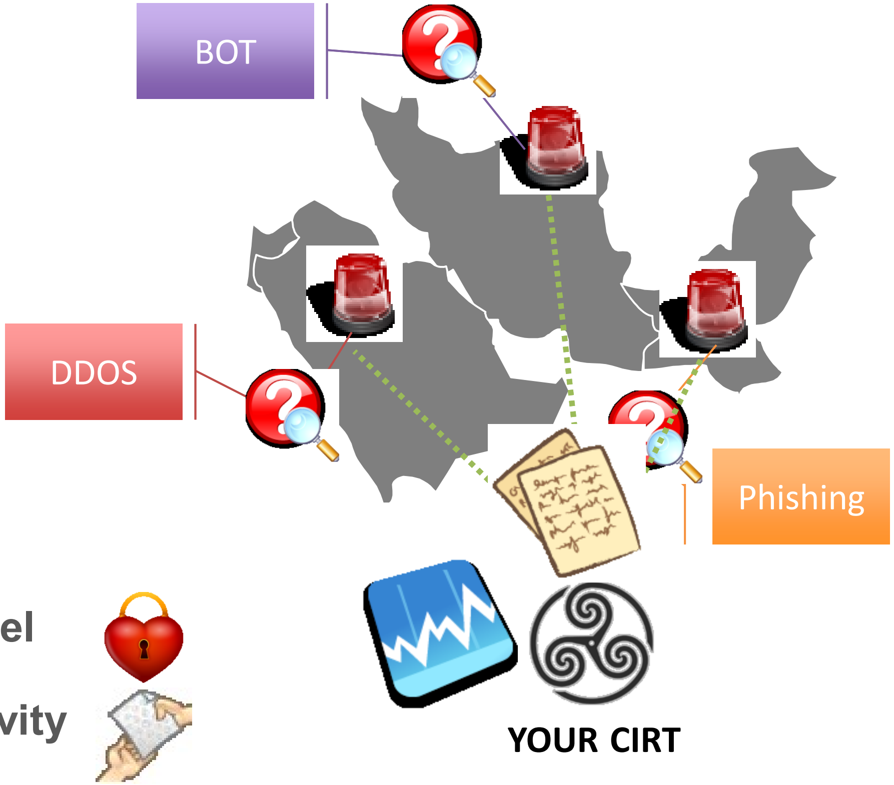
PROBLEMS



There is no standard way to create a CIRT
It depends on your environment
It is crucial for discussions even before creating a CIRT
Get to know what you are building before you build it.

INTRODUCTION

MECHANISMS



Provide early warning

Detect & Identify the activity

Develop mitigation & response strategies

Establish a trusted communication channel

Share data and Information about the activity

Track and monitor information

Determine Trends & Long Term Remediation plans

Needed Mechanisms

INTRODUCTION

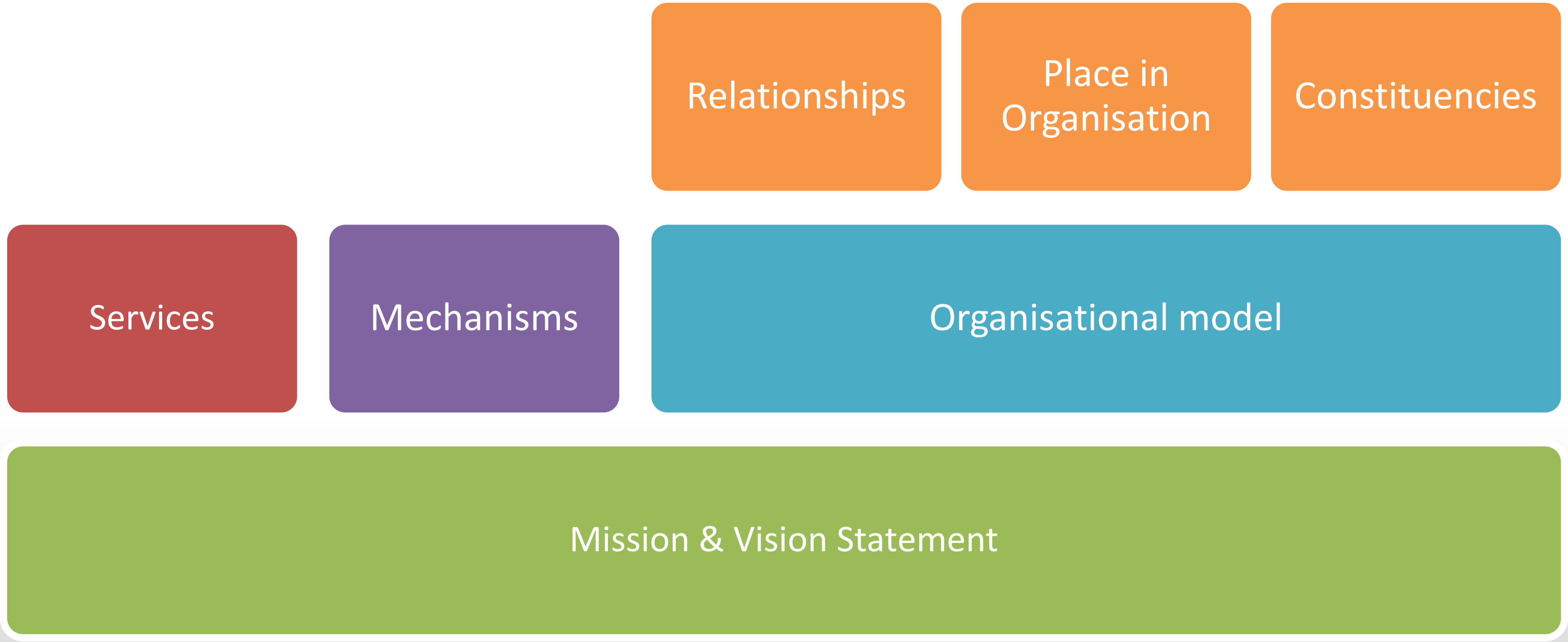
BENEFITS OF A NATIONAL CIRT

YOUR CIRT

- Serve as a trusted focal point
- Develop a capability to support incident reporting.
- Develop an infrastructure for coordinating response.
- Conduct incident, vulnerability & Artifact analysis.
- Participate in cyber watch functions.
- Help organizations develop their own incident management capabilities.
- Make security best practices & guidance available.
- Provide awareness, education & trainings

CREATING A CIRT

BASE PLAN



Relationships

Place in Organisation

Constituencies

Services

Mechanisms

Organisational model

Mission & Vision Statement

- MISSION & VISION STATEMENT
- CREATING A CIRT

CREATING A CIRT

MISSION STATEMENT

- Must be clear to **establish the policies and services**
- Must **complement** the **mission of the organization**.
- It should **reflect what is really important** for that **specific organisation**.
- **Be pragmatic** – it is not realistic to say ‘prevent any incident from happening’, or ‘resolve any incident within an hour’
- An ideal statement could include references to:
  - Protecting and maintaining the security
  - Coordinating incident response activities
  - Minimizing damage
  - Educating the constituency
- It should naturally also **state what community the CERT cares for**

CREATING A CIRT

MISSION STATEMENT

Sample Mission Statement:

1. X-CIRT’s mission is to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the nation while protecting the constitutional rights of the nationals.
2. Y-CIRT will maintain a trusted contact network of computer security experts in its region to improve the region's awareness and competency in relation to computer security incidents through:
   - Enhancing regional and international cooperation on information security;
   - Jointly developing measures to deal with large-scale or regional network security incidents;
   - Facilitating information sharing and technology exchange, including information security, computer virus and malicious code among its members;
   - Promoting collaborative research and development on subjects of interest to its members;
   - Assisting other CERTs and CSIRTS in the region to conduct efficient and effective computer emergency response;
   - Providing inputs and/or recommendations to help address legal issues related to information security and emergency response across regional boundaries.

CREATING A CIRT

VISION STATEMENT

- Must be clear to **project the end goal of the CIRT**
- Must **complement** the **mission statement of the CIRT**.
- It should **reflect what the CIRT aims to attain**.
- **Be realistic**

CREATING A CIRT

VISION STATEMENT

Sample Vision Statement:

1. X-CIRT's vision is to be a trusted global leader in cybersecurity - collaborative, agile, and responsive in a complex environment.
2. Y-CIRT will work to help create a safe, clean and reliable cyber space in its Region through global collaboration

- CONSTITUENCY
- CREATING A CIRT

CREATING A CIRT

CONSTITUENCY

For incident management you must define the constituency you work for or with – the constituency is the organisation (or group of organisations) and/or people whose incidents you handle (or co-ordinate).

- ENISA

CREATING A CIRT

CONSTITUENCY

	HELPFUL	HARMFUL
INTERNAL ORIGIN	**Strength** • There is some knowledge within the company • They like the plan and are willing to cooperate • Support and funding provided by the Mgmt. Board	**Weaknesses** • Not much internal communication • No coordination with ICT Incidents • Lots of ‘little departments’
EXTERNAL ORIGIN	**Opportunities** • Huge flood of non structured vulnerability information • Strong need for coordination • Reducing losses due to incidents • Lot of open ends on the matter of ICT security • Educating the staff on ICT security	**Threats** • Not much money available • Not much staffing • High expectations • Culture

SWOT Analysis

CREATING A CIRT

CONSTITUENCY

PEST Analysis

Political

- Ecological / environmental issues
- Current legislation home market
- Future legislation
- European/International legislation
- Regulatory bodies and processes
- Government Policies
- Government term and change
- Trading policies
- Funds, grants and initiatives
- Home market lobbying/pressure groups
- International pressure groups

Economic

- Home economy situation
- Home economy trends
- Overseas economy and trends
- General taxation and issues
- Taxation specific to product/services
- Seasonality/weather issues
- Market and trade cycles
- Specific industry factors
- Market routes and distribution trends
- Customer/end-user drivers
- Interest and exchange rates

Social

- Lifestyle Trends
- Demographics
- Consumer attitudes and opinions
- Media views
- Law charges affecting social factors
- Brand, company, technology image
- Consumer buying patterns
- Advertising and publicity
- Major events and influences
- Buying access and trends
- Ethnic/religious factors

Technological

- Competing technological development
- Research Funding
- Associated/dependent technologies
- Replacement technology/solutions
- Maturity of technology
- Manufacturing maturity and capacity
- Information and communications
- Technology legislation
- Innovation potential
- Technology access, licensing, patent
- Intellectual property issues

- PLACE IN THE ORGNISATION
- CREATING A CIRT

CREATING A CIRT

PLACE IN ORGANISATION

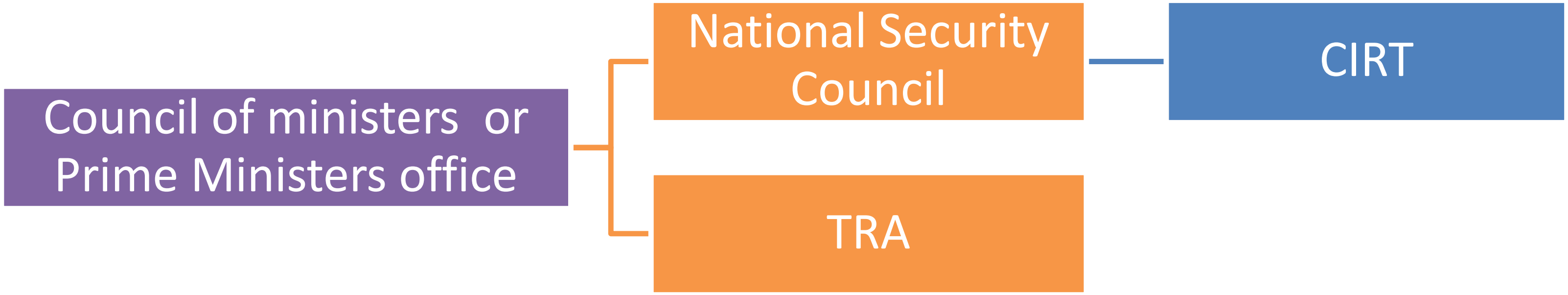
- Define the position of the CIRT
- The role of CIRT, played in overall risk management in the context of its organization
- Highest position possible
- Depends on the authority and type of services offered

Whom does the CIRT report to?

1. Security Council?
2. TRA?
3. Ministry?
4. Council of Ministers?
5. CIRT Management Body?
6. University?
7. etc.

CREATING A CIRT

PLACE IN ORGANISATION


Council of ministers or Prime Ministers office
National Security Council
CIRT
TRA

- Sample structure

- RELATIONSHIPS
- CREATING A CIRT

CREATING A CIRT

RELATIONSHIPS

- The realm of a CIRT is a big as the internet.
- CIRT can expect to have both domestic and international relationships.
- CIRT would have to device a proper plan for:
  - Establishing contacts

A CIRT can’t operate effectively without gaining trust & respect from constituency

  - Ministry of Justice
  - Other CIRTs/CERTS/CSIRT
  - CIRT Constituencies
  - Industry Partners
  - Other international organisations/agencies

CREATING A CIRT

RELATIONSHIPS

A CIRT must consider co-operation and co-ordination as the key elements for its day to day activities.

It would be ideal to have

- Communication Plan
- Liaison
- Templates / Drafts
- Contact database

CREATING A CIRT

RELATIONSHIPS

- CIRT have to inter-operate to get their job done
- Consider joining the regional / global community (FIRST)
- FIRST: Forum of Incident Response and Security Teams
  - Foster coordination in incident prevention, detection and response
  - Strives for excellence and improvement to ensure integrity, quality, performance and mutual respect among other CIRTs
  - Provides a trusted mechanism to share sensitive incident information amongst response teams

- SERVICES
- CREATING A CIRT

CREATING A CIRT

SERVICES

What does a CIRT do?

- Provides a single point for reporting incidents
- Assists the organizational constituency and general computing community in preventing and handling computer security incidents
- Share information and lesson learned with other CIRT / response teams and appropriate organizations and sites.

REMEMBER!

No single team can be everything to everyone!

CREATING A CIRT

SERVICES

We can distinguish 4 kind of services:

1. Reactive Services
2. Proactive Services
3. Artifact Handling
4. Security Quality Management

CREATING A CIRT

SERVICES

In the beginning stage a CIRT should ideally focus on the following services:

1. Alerts & Warning
2. Incident Handling
3. Incident Analysis
4. Incident Response Support/Coordination
5. Announcement
6. Awareness & Capacity Building

CREATING A CIRT

SERVICES

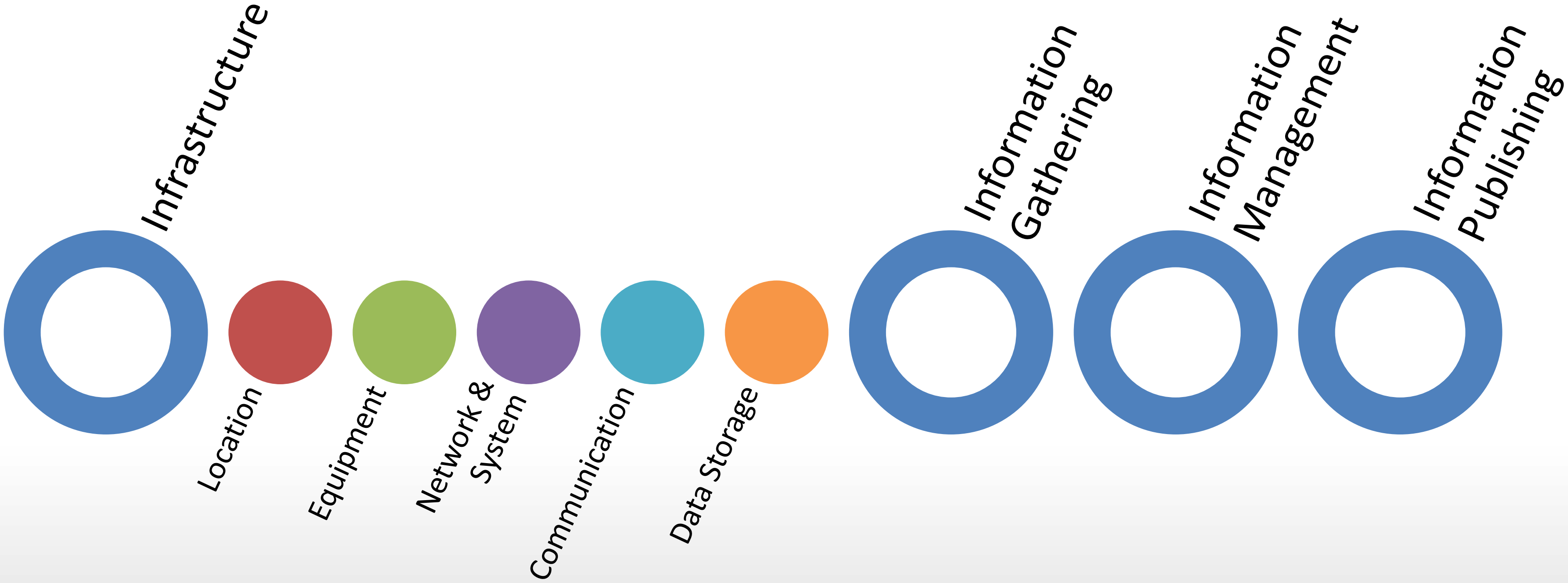
Reactive Services	Proactive Services	Artifact Handling
Alerts & Warnings	Announcements	Artifact Analysis
Incident Handling	Technology Watch	Artifact response
Incident Analysis	Security Audits	Artifact response coordination
Incident response support	Security Assessments	**Security Quality Management**
Incident response coordination	Configuration & Maintenance of Security	Risk Analysis
Incident response on site	Development of Security Tools	BC and Disaster Management
Vulnerability Handling	Intrusion detection services	Security Consulting
Vulnerability Analysis	Security related information dissemination	Awareness Building
Vulnerability Response		Education/Training
Vulnerability Response Coordination		Project Evacuation or Certification

- MECHANISMS
- CREATING A CIRT

CREATING A CIRT

MECHANISMS

CIRT relies on a number of mechanisms for its operations. Some of them being:



CREATING A CIRT

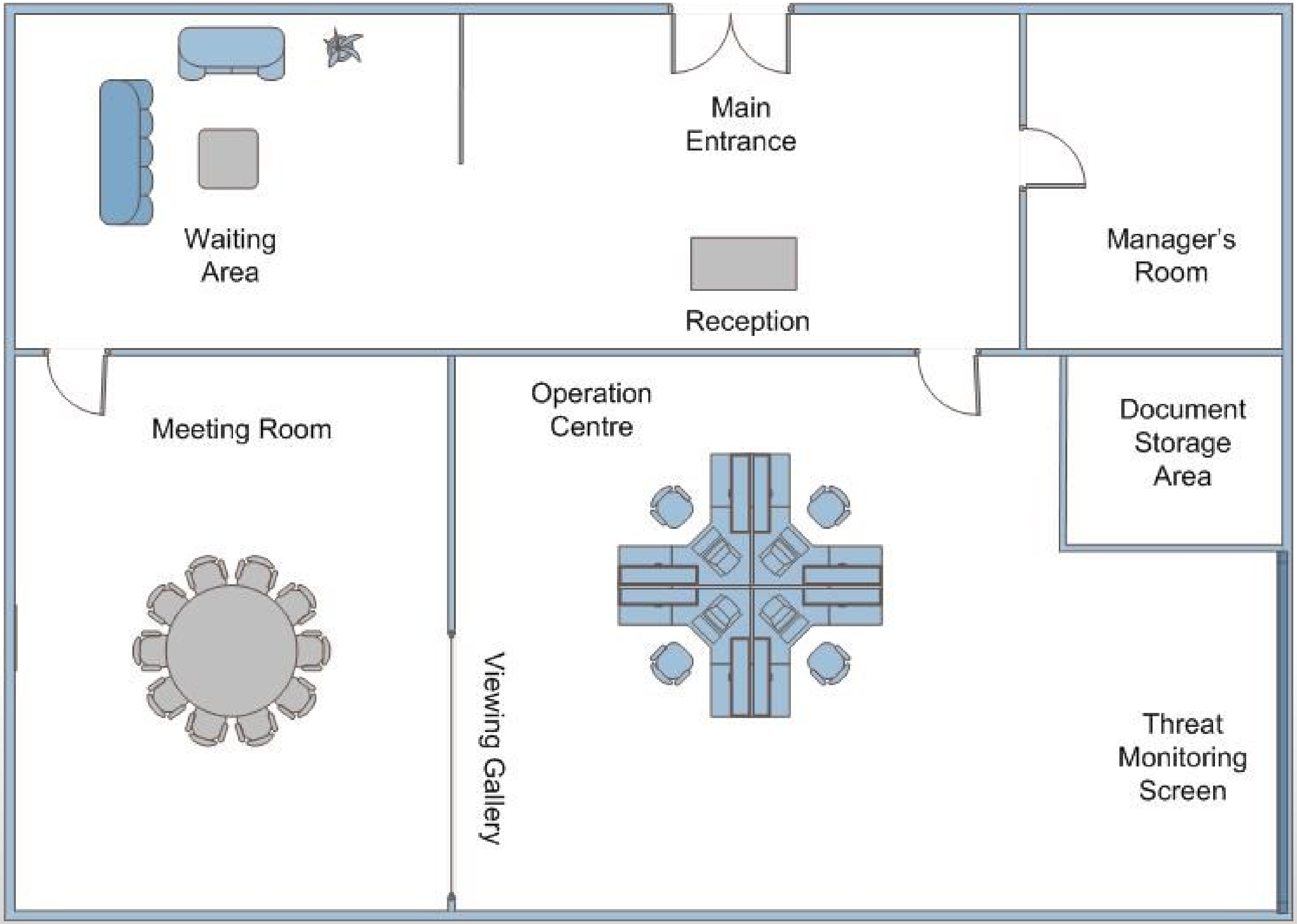
MECHANISMS: LOCATION

- Must be secure physically
- Incident data and sensitive data must be highly protected. Depending on:
  - Legal requirement
  - Constituency expectation
  - Business necessity
  - Potential intruder threat

- A working space alone is not enough:
  - General office area
  - Secure physical area for meetings and incident work
  - Lab or test network area

CREATING A CIRT

MECHANISMS: LOCATION



CREATING A CIRT

MECHANISMS: EQUIPMENT

- For CIRT staff
  - Need access to basic computing and communications systems
- For secure online data
  - File server
  - Laptop PC
  - Physical network wiring and data connections
  - Wiring closets
  - Routers and firewalls
- Printing Mechanisms
  - Sensitive data should be printed in a secure area
  - Fax machines too
- Shredding
  - Shred classified information. Secure storage prior to shredding

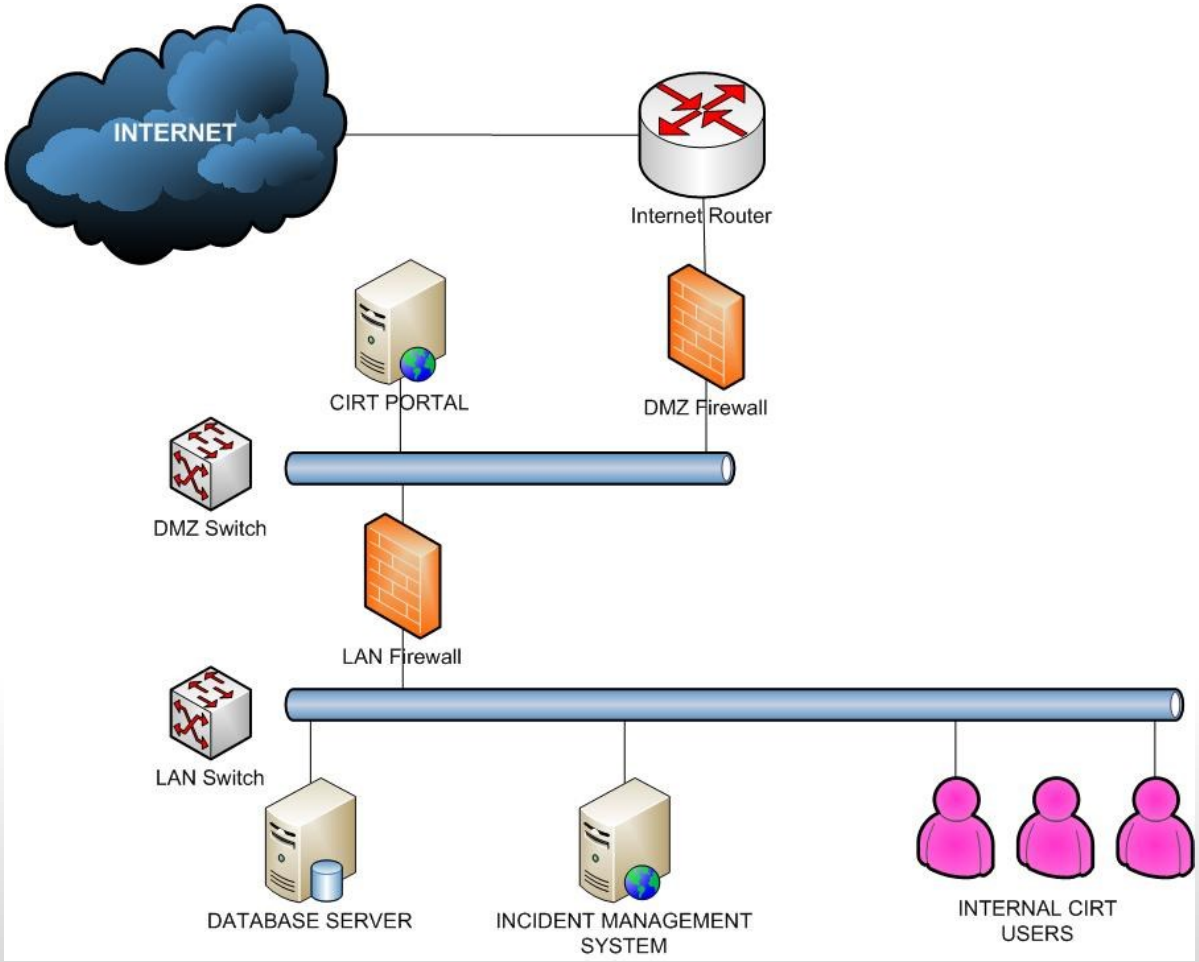
CREATING A CIRT

MECHANISMS: NETWORK & SYSTEM

- Separate CIRT network
- Separate email, web, DNS, and other server and services
- Up-to-date and consistent software
- Secure network and system configurations
- Method for updating software on staff devices
- Guidelines on appropriate software to use and not to use
- Test network, lab or devices
- Secure intranet for CIRT staff

CREATING A CIRT

MECHANISMS: NETWORK & SYSTEM



CREATING A CIRT

MECHANISMS: COMMUNICATION

- Remote Access
  - SSH
  - VPN
- Encrypting or decrypting email
  - PGP
  - GPG
  - Digital certificates
  - S/MIME
- Secure telephone
  - STU phones

CREATING A CIRT

MECHANISMS: DATA STORAGE

- Trouble ticket or help desk system
- Relational database
- Query and analysis tools
  - What data will you collect
  - What reports or analysis will you do or do you need?
  - How is data reported (automatically / data entry)?
  - Is the data consistent? Can it be used with data mining and decision support tools?

CREATING A CIRT

MECHANISMS: INFORMATION GATHERING

- Public monitoring
  - Watch security related websites everyday
  - Like: Security Focus, Secunia, SANS, other CIRTs…
- International CIRTs and other organizations
  - Trusted relationship is needed
  - Secure communication channel
  - NDA or MOU is highly recommended
- Domestic companies and other organizations
  - ISPs / ASPs
  - Developers / Manufacturers
- Reporting
  - Official reporting framework
  - Consumers?

CREATING A CIRT

MECHANISMS: INFORMATION MANAGEMENT

How to store data?

- Relational Database
- Tracking system
- Excel

Prioritizing

- How to evaluate it?
- Scoring system?

CREATING A CIRT

MECHANISMS: INFORMATION MANAGEMENT

Who needs to know the information?

- Very restricted staff.
- Only for people to take actions.

How to manage it?

- Any secure way to share
- E-mail is not secure enough
- Telephone / fax may not be secure

Will the information be published?

- When?
- Information update
- Update? Need to notify?

CREATING A CIRT

MECHANISMS: INFORMATION MANAGEMENT

Accuracy

- Can you trust reporters?
- Evidence such as log information

Other considerations

- Can you handle the information freely?
- Information control restriction

Personal / private information issues

- Confidentiality issues
- Need to encrypt?

How to determine if a person is the right person to tell the information?

CREATING A CIRT

MECHANISMS: INFORMATION PUBLISHING

What kind of information?

- Technical Alert
- Technical Document
- Research Report
- Others

For whom?

- IT Pro
- Consumer
- Government
- Industry
- International

How?

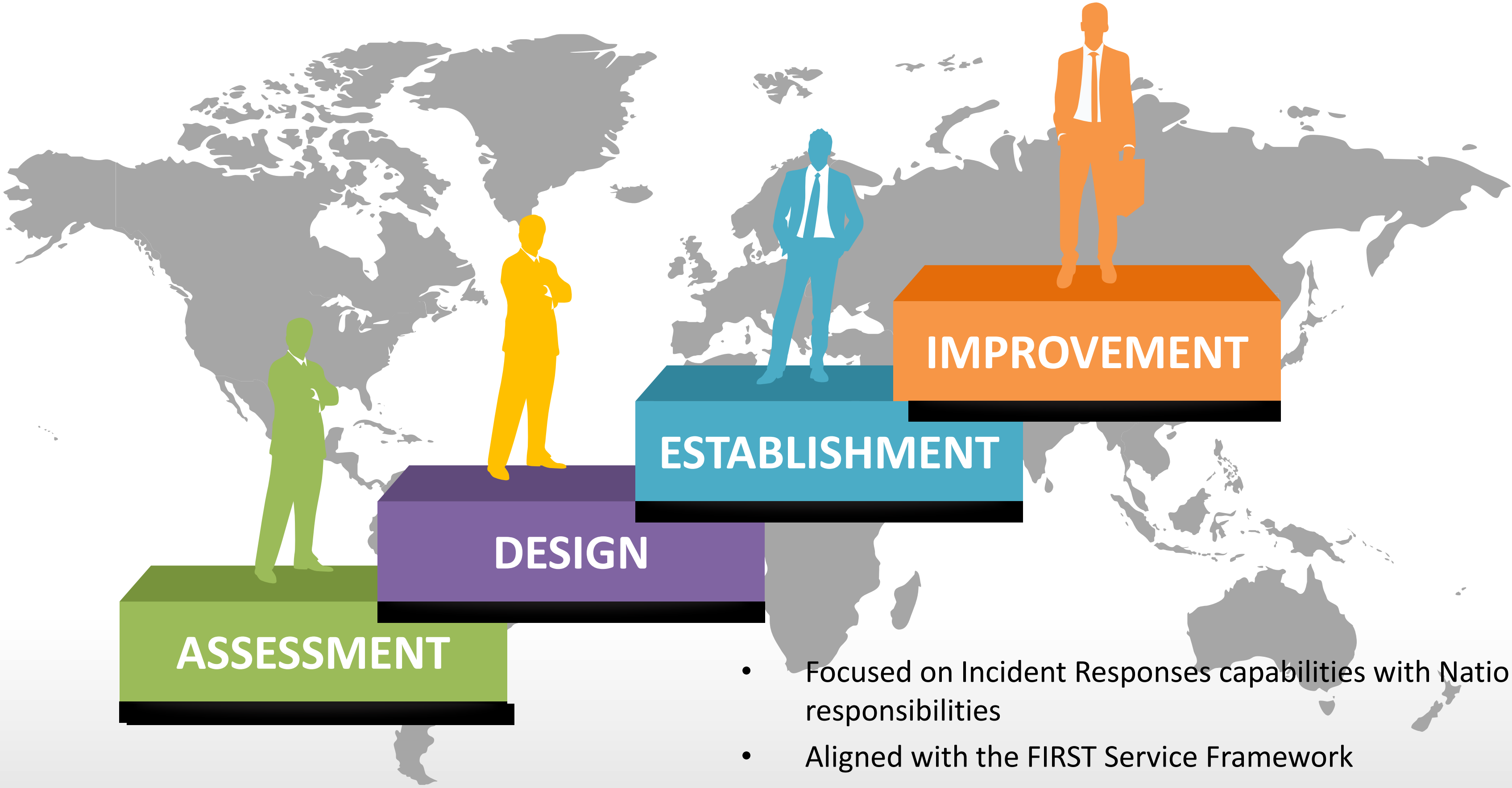
- Mailing list
- Website

We will focus on

NATIONAL CIRT

CIRT Framework

ITU CIRT Framework



- Focused on Incident Responses capabilities with National responsibilities
- Aligned with the FIRST Service Framework

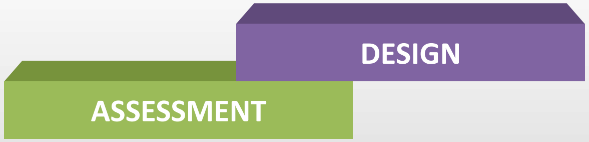
ITU CIRT Framework Explained

Assessment Service	
Description	Review the current incident response capabilities present at the national level
Activities	- Administering CIRT questionnaire - Analyzing response - Performing on-site visit for review and finalization
Key Deliverables	Assessment report
Modality	Off-site and On-site
Finance	Covered by ITU

ASSESSMENT

ITU CIRT Framework Explained

Design Service	
Description	Develop a blueprint of the National CIRT project, with the related implementation processes
Activities	- CIRT positioning - Identify CIRT Services - Identify processes and related workflows - Identify policies and procedures - Relationship with constituency and communication strategy - Technology - Premises - HR
Key Deliverables	CIRT design document and implementation plan
Modality	Off-site and On-site
Finance	Covered by the country



ITU CIRT Framework Explained

Establishment Service	
Description	Execute the project as agreed with the Member States and based on the outcomes of the Design Service's deliverables
Activities	▪ Capabilities development ▪ Capabilities deployment and testing ▪ Customization, fine tuning and training ▪ Operations ▪ Handover and closure
Key Deliverables	▪ SOPs ▪ Operating manuals ▪ Training material ▪ Tools
Modality	Off-site and On-site
Finance	Covered by the country

Typical services that the CIRT will provide to the constituency

- Incident handling
- Incident analysis
- Outreach and communication

ESTABLISHMENT

DESIGN

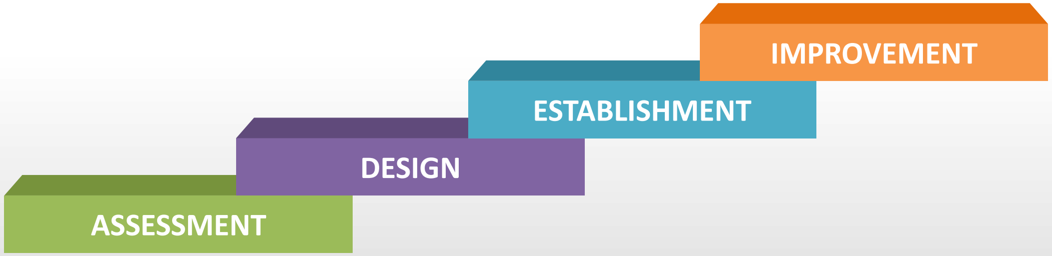
ASSESSMENT

ITU CIRT Framework Explained

Improvement Service	
Description	Enhance Existing CIRT capabilities and operation
Activities	▪ Environment Analysis ▪ Capabilities deployment and testing ▪ Customization, fine tuning and training ▪ Operations ▪ Handover and closure
Key Deliverables	▪ SOPs ▪ Operating manuals ▪ Training material
Modality	Off-site and On-site
Finance	Covered by the country

Typical services that the CIRT will provide to the constituency

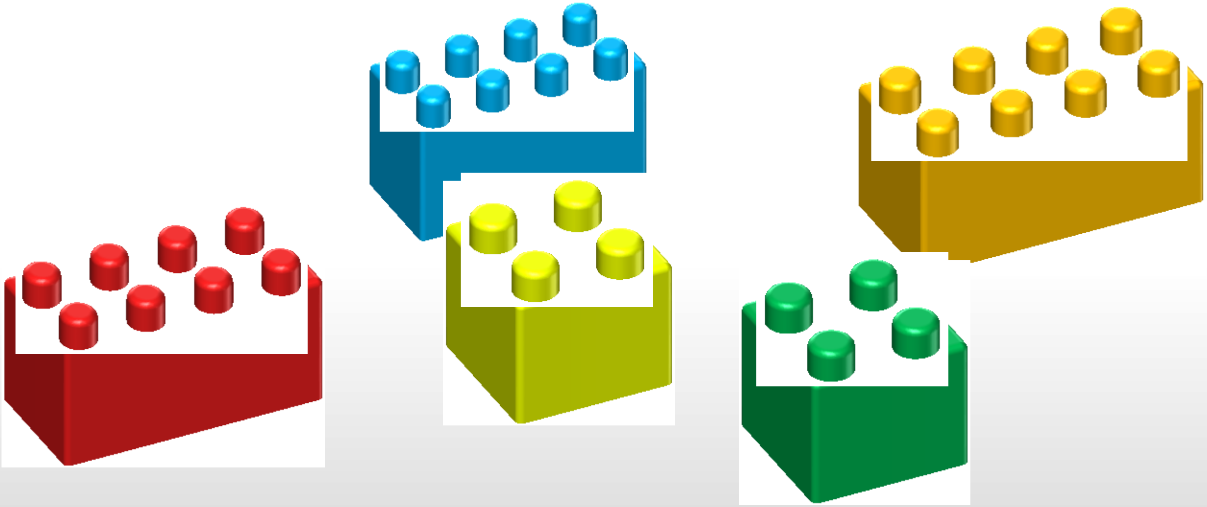
- Digital Forensic
- Situational Awareness
- Basic CTI



Notion of building blocks

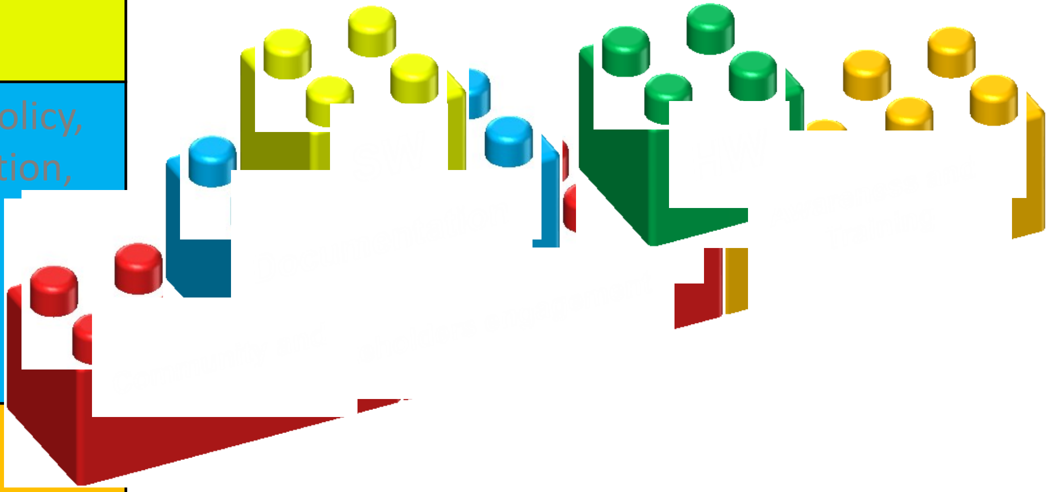
- A building block is an atomic element (piece of HW, document, training course, etc.) that can be used to produce a deliverable

- Building blocks are cross cutting to all processes used to provide assistance as well as to the services that the CIRT will provide to the constituency

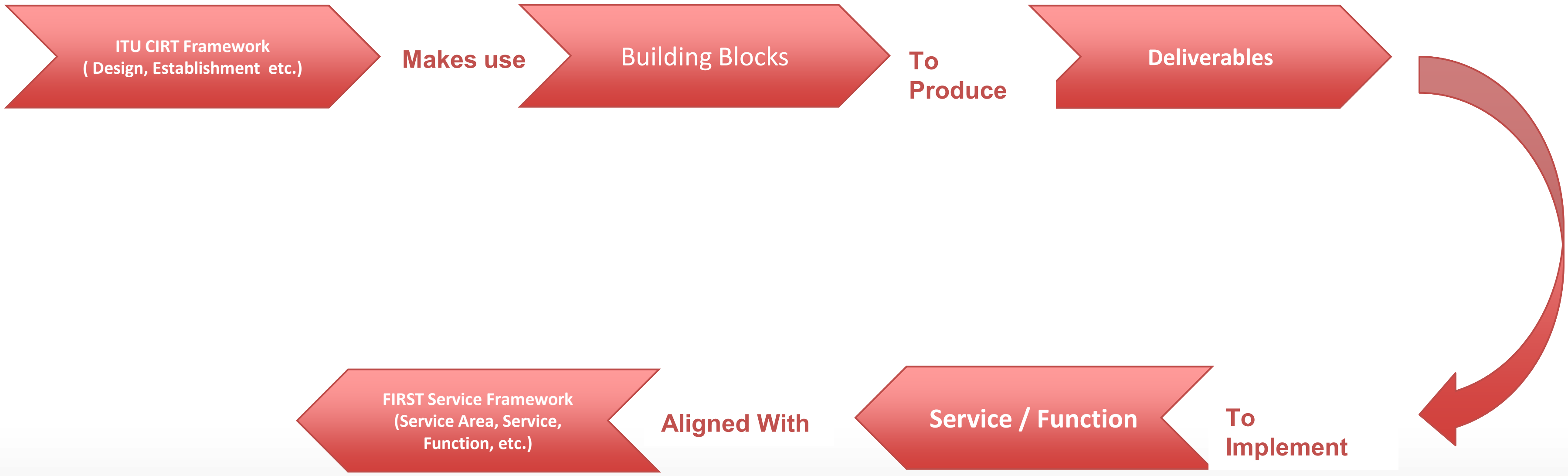


Typology of Building Blocks

HW	Appliances Network devices Desktops, laptops Cables
SW	RTIR Tools for malware analysis Office automation tools
Documentation	Policies (Internal security policy, data and incident classification, Org Charts, job profiles) Templates Manuals Communication material
Awareness and training	Presentations Books Training lab Manuals Communication material
Community and stakeholders engagement	FIRST Membership Outreach plan Announcement plan



ITU CIRT Framework applied


ITU CIRT Framework
(Design, Establishment etc.)

Makes use

Building Blocks

To
Produce

Deliverables

To
Implement

Service / Function

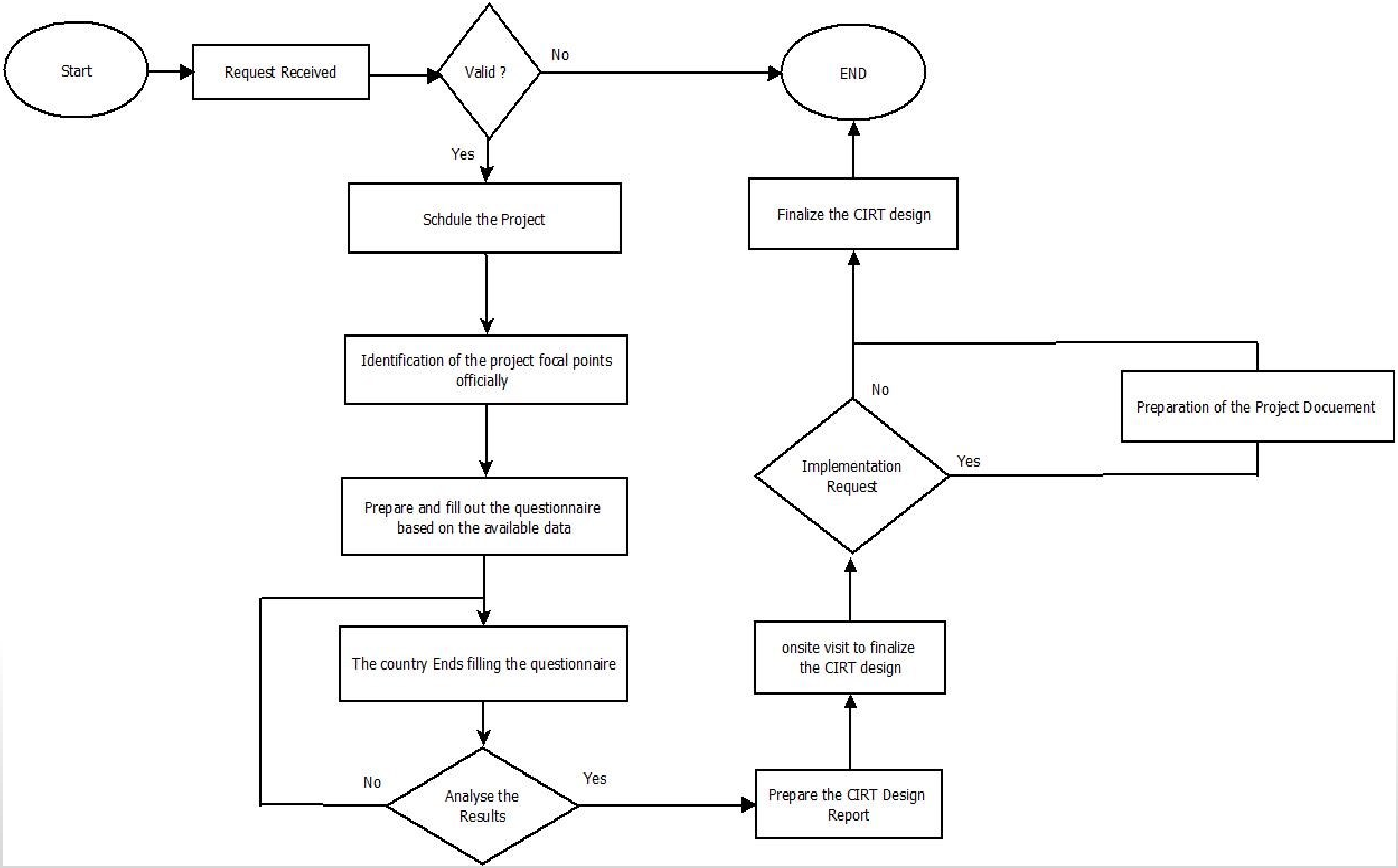
Aligned With

FIRST Service Framework
(Service Area, Service,
Function, etc.)

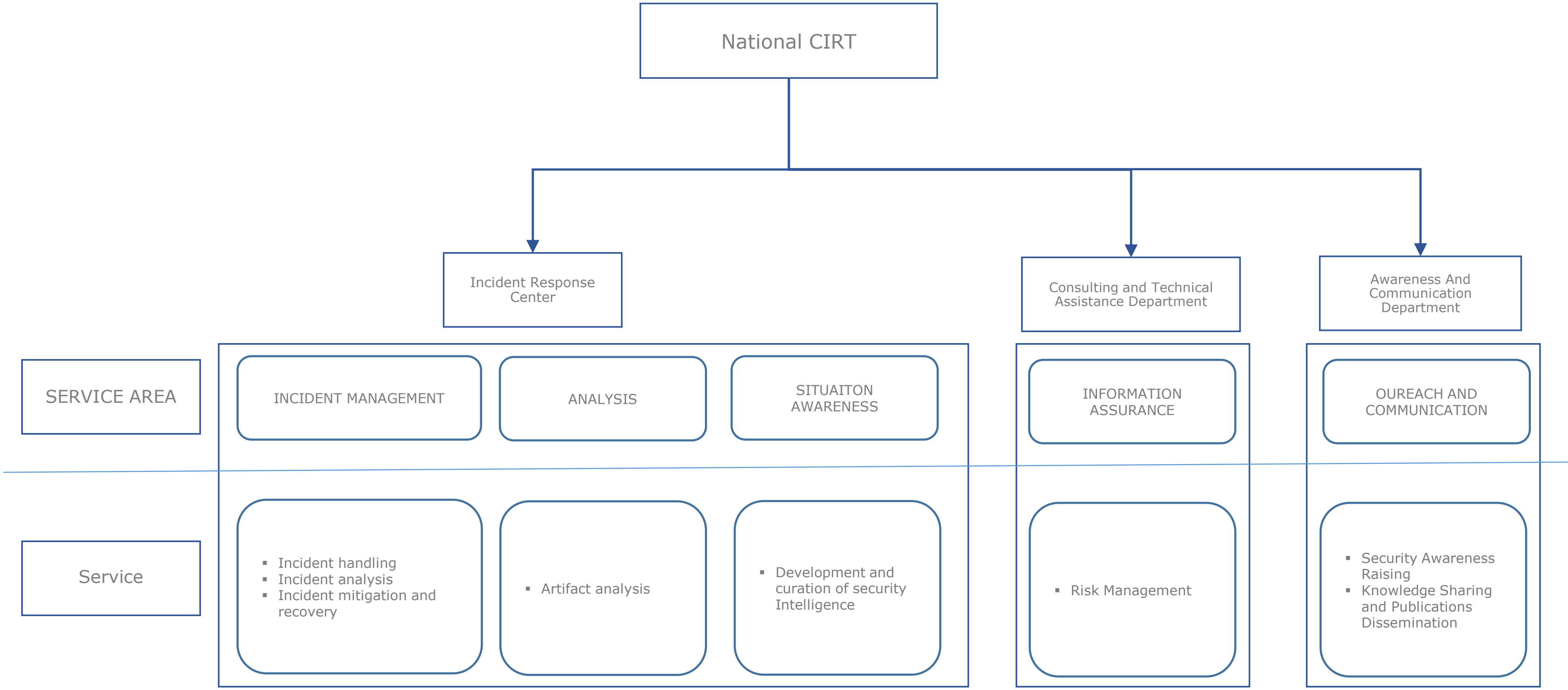
ITU CIRT Framework Applied

Example of Design and Establishment

Design Process


Start
Request Received
Valid ?
No
END
Yes
Schdule the Project
Finalize the CIRT design
Identification of the project focal points officially
No
Preparation of the Project Docuement
Implementation Request
Yes
Prepare and fill out the questionnaire based on the available data
The country Ends filling the questionnaire
onsite visit to finalize the CIRT design
No
Analyse the Results
Yes
Prepare the CIRT Design Report

The Basic Services Offered by a National CIRT


National CIRT

Incident Response Center

Consulting and Technical Assistance Department

Awareness And Communication Department

SERVICE AREA

INCIDENT MANAGEMENT

ANALYSIS

SITUAITON AWARENESS

INFORMATION ASSURANCE

OUREACH AND COMMUNICATION

Service

- Incident handling
- Incident analysis
- Incident mitigation and recovery

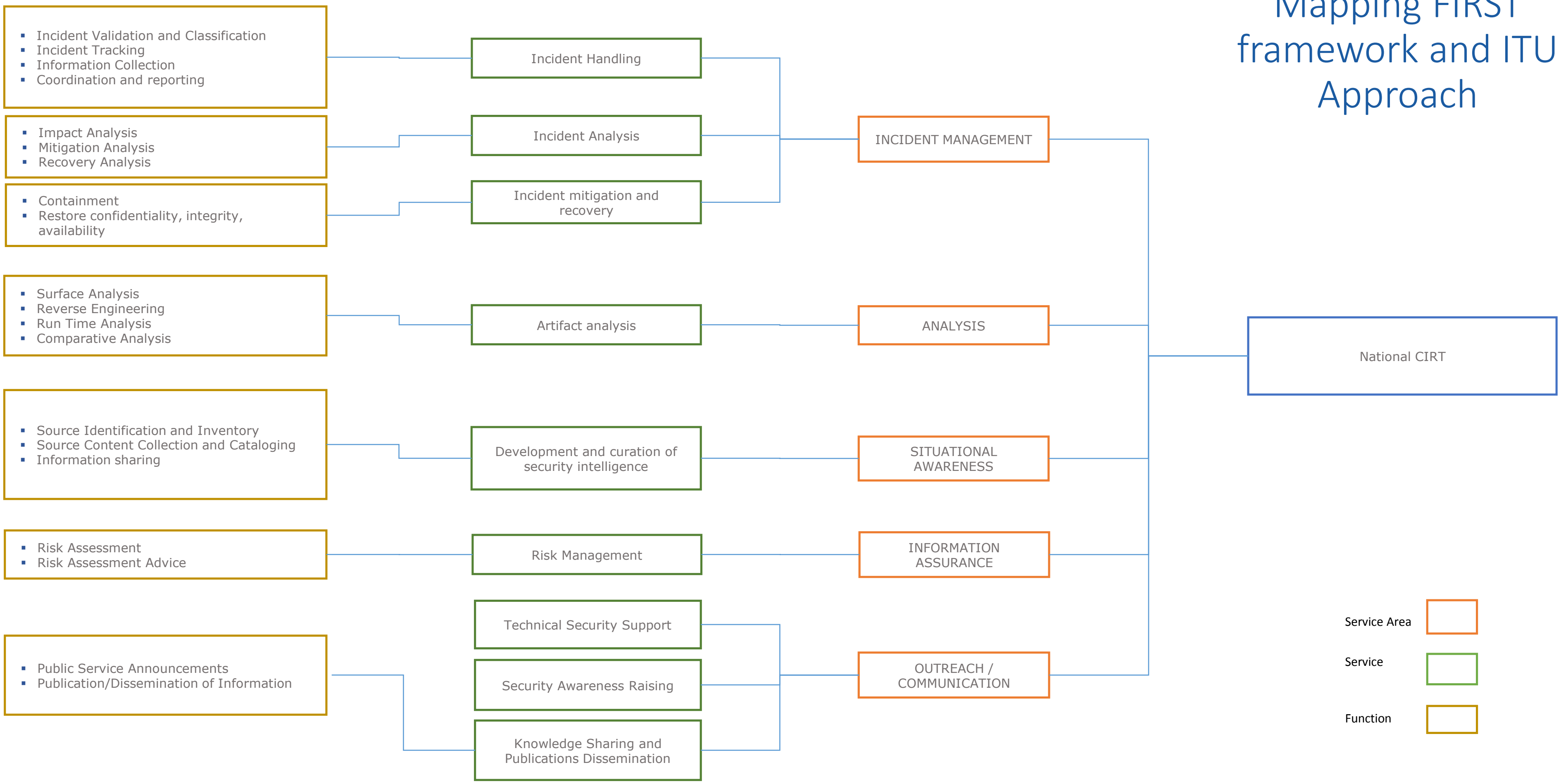
- Artifact analysis

- Development and curation of security Intelligence

- Risk Management

- Security Awareness Raising
- Knowledge Sharing and Publications Dissemination

Mapping FIRST framework and ITU Approach



- Incident Validation and Classification
- Incident Tracking
- Information Collection
- Coordination and reporting

Incident Handling

- Impact Analysis
- Mitigation Analysis
- Recovery Analysis

Incident Analysis

- Containment
- Restore confidentiality, integrity, availability

Incident mitigation and recovery

INCIDENT MANAGEMENT

- Surface Analysis
- Reverse Engineering
- Run Time Analysis
- Comparative Analysis

Artifact analysis

ANALYSIS

National CIRT

- Source Identification and Inventory
- Source Content Collection and Cataloging
- Information sharing

Development and curation of security intelligence

SITUATIONAL AWARENESS

- Risk Assessment
- Risk Assessment Advice

Risk Management

INFORMATION ASSURANCE

Technical Security Support

- Public Service Announcements
- Publication/Dissemination of Information

Security Awareness Raising

Knowledge Sharing and Publications Dissemination

OUTREACH / COMMUNICATION

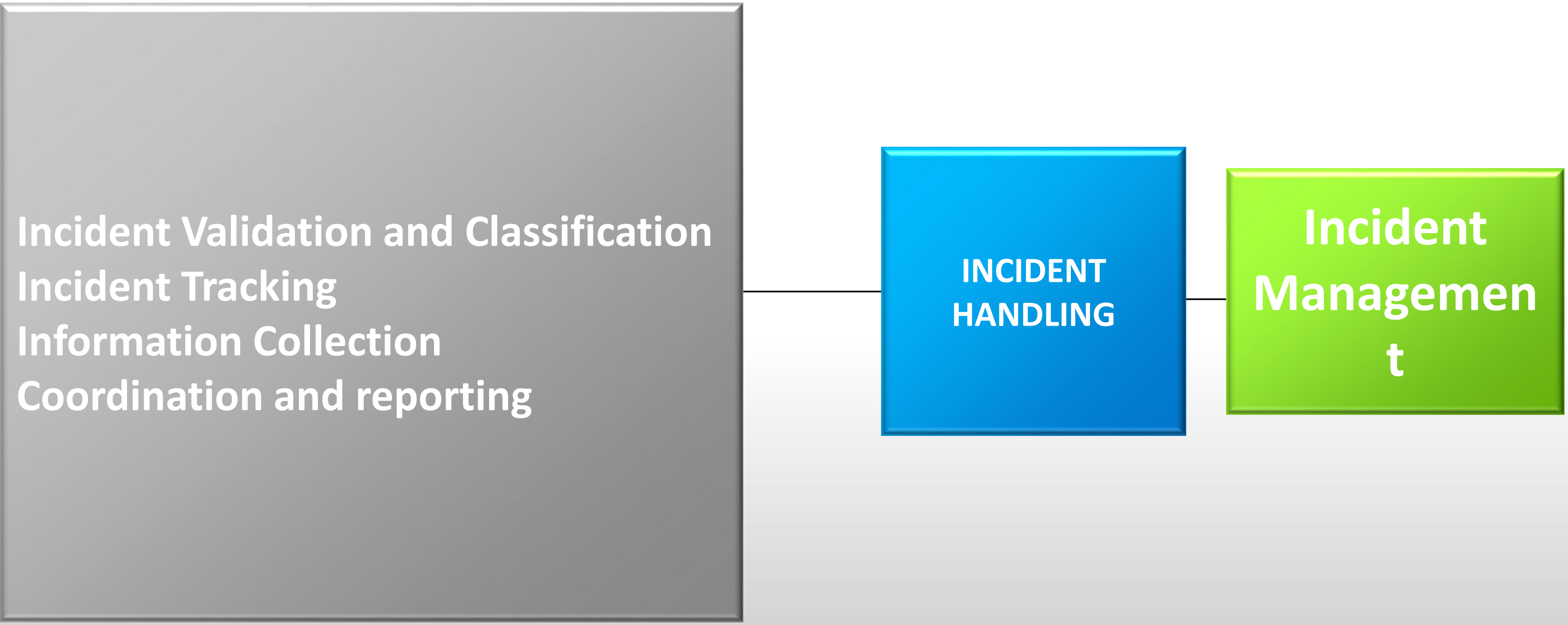
Service Area 🟧

Service 🟩

Function 🟨

Example

INCIDENT MANAGEMENT



Incident Validation and Classification
Incident Tracking
Information Collection
Coordination and reporting

INCIDENT HANDLING

Incident Managemen t

Design Phase

Service	Description	Documents	Trainings		Tools	
			Duration	Title	Open Source	Commercial
INCIDENT HANDLING	Services related to the management of a cyber-event, to include alerting constituents and coordinating activities associated with the response, mitigation, and recovery from an incident. Incident handling is dependent upon analysis activities, which are defined in the “Analysis” section. Functions : • Incident Validation and Classification • Incident Tracking • Information Collection • Coordination and reporting	- Incident Management Process - Standard Operational Procedures : . Worm Infection . Windows Intrusion . Unix/Linux Intrusion Detection . DDOS . Malicious NetworkBehaviour . Website-Defacement . Windows Malware Detection . Blackmail . Smartphone Malware . Social Engineering . Information Leakage . Insiderabuse . Phishing . Scam . Trademark infringement . Ransomware - Technical Guidelines for the Administration of the Incident Management System - Job description for : . Incident Response Manager . Incident Response Analyst	1 Day 5 Days	- RTIR Incident Management & System Administration - Incident Management Training : . Incident Response Framework . Exercises in the use of the SOP . Incident Management Process Improvement	• RTIR • OTRS	• IBM The Integrated Incident ManagementTivoli • HPE for Incident Management
INCIDENT ANALYSIS	Services related to identifying and characterizing information about events or incidents such as scope, affected parties, involved systems, timeframes (discovery, occurrence, reporting), status (ongoing versus completed). Functions : • Impact Analysis • Mitigation Analysis • Recovery Analysis					
INCIDENT MITIGATION AND RECOVERY	Services related to reducing the impact of an incident and working to restore business functions within the constituency. Functions : • Containment • Restore confidentiality, integrity, availability					

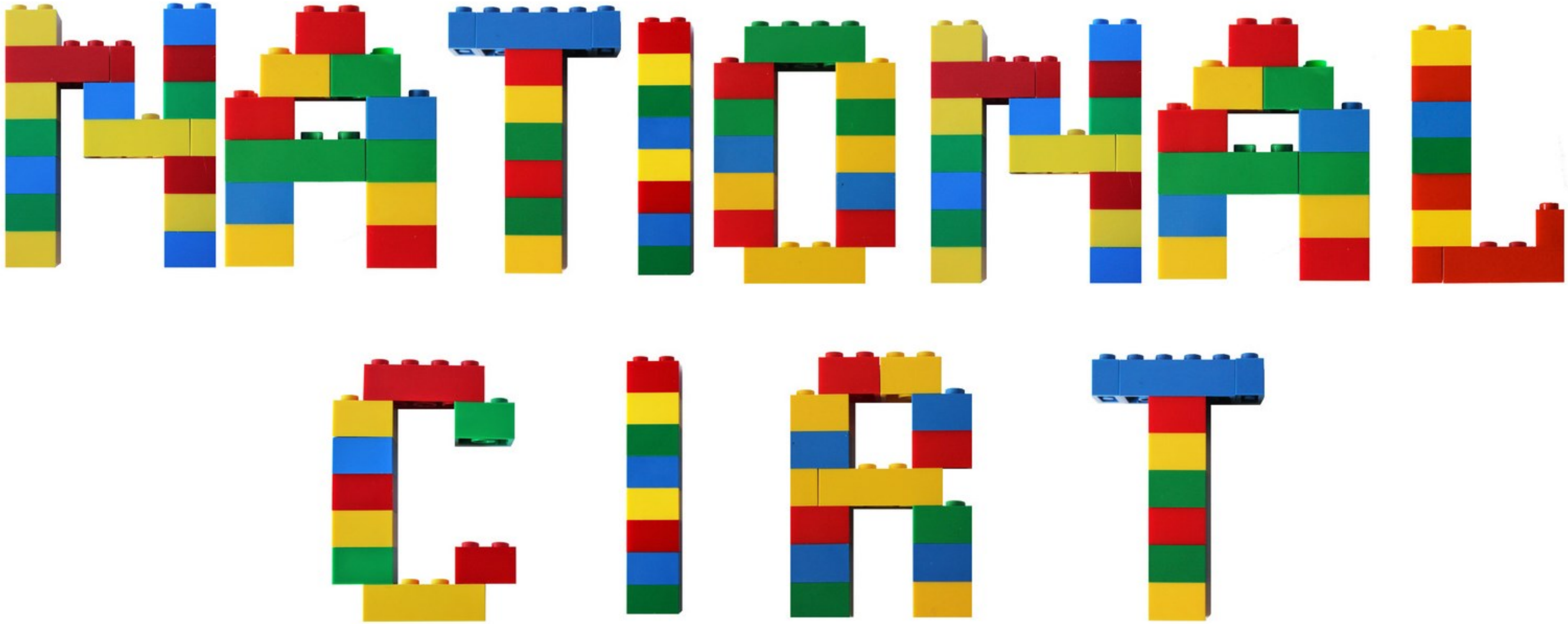
Deliverables

Document N.	Document Title	[illegible]	Category
D1.1	Incident Management Process	Incident Management	Operational Processes
D1.2	Artifact Analysis Process	Incident Management	Operational Processes
D1.3	Alerts and Warnings Process	Incident Management	Operational Processes
D1.4	Standard Operational Procedures : . Worm Infection . Windows Intrusion . Unix/Linux Intrusion Detection . DDOS . Malicious Network Behavior . Website-Defacement . Windows Malware Detection . Blackmail . Smartphone Malware . Social Engineering . Information Leakage . Inside abuse . Phishing . Scam . Trademark infringement . Ransomware	INCIDENT MANAGEMENT	SOP
D1.5	Technical Guidelines for the Administration of the Incident Management System	Incident Management	Technical Guidelines
D1.6	Job description for : . Incident Response Manager . Incident Response Analyst	Incident Management	Job Description
D1.9	RTIR Incident Management & System Administration	Incident Management	Training Materials
D1.10	Incident Management	Incident Management	Training Materials

Training N.	Training Title	Unit	Number of Days
T1.1	RTIR Incident Management & System Administration	Incident Management	1
T1.2	Incident Management Training	Incident Management	5

Tool N.	Tool Name	Unit
L1.1	RTIR	Incident Management

…ETC


NATIONAL
CIRT

CREATING A CIRT

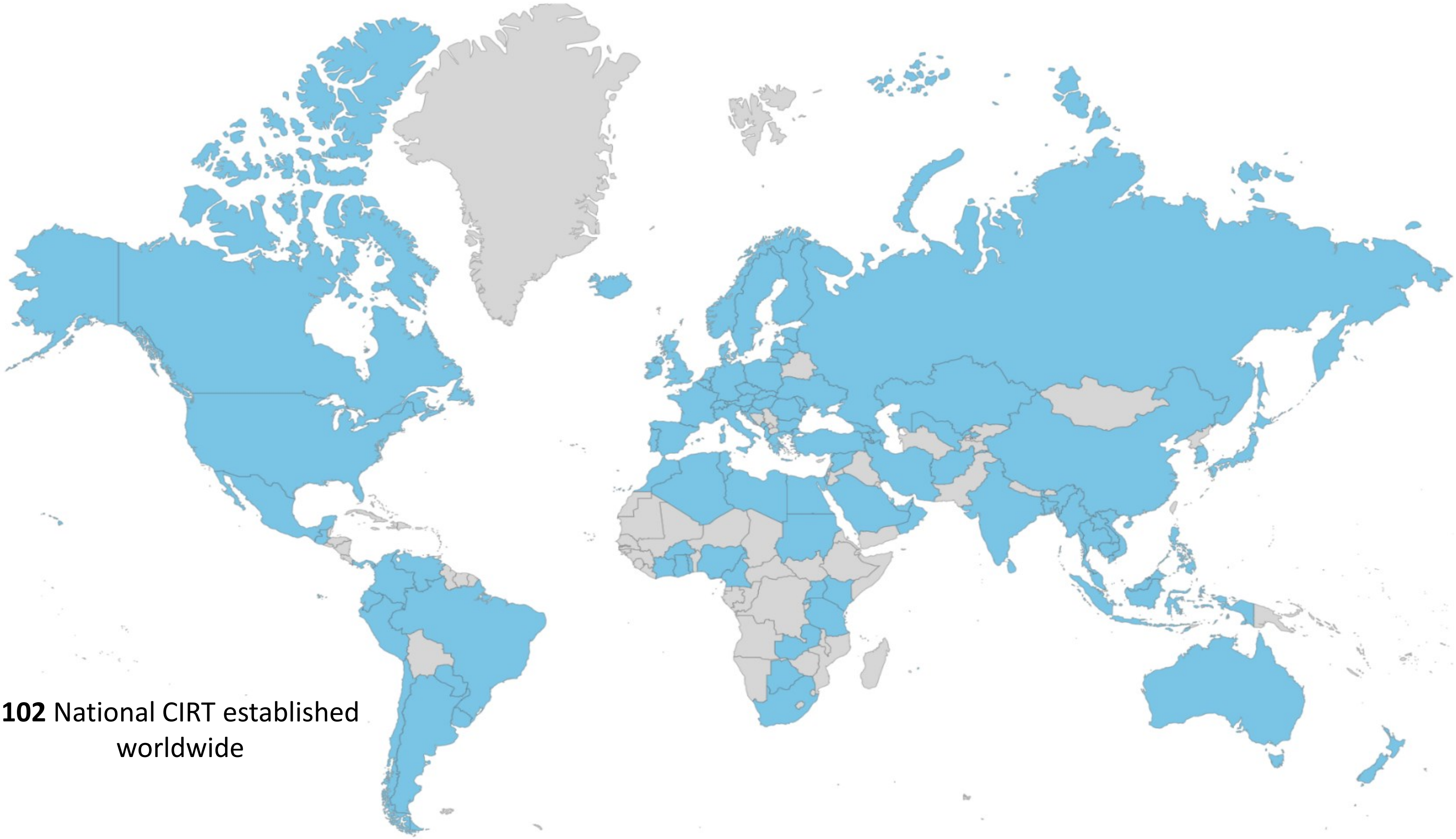
SUMMARY

CREATING A CIRT

CHOOSING THE RIGHT APPROACH

1. Define a communication approach to your constituents
2. Define the mission statement
3. Make a realistic implementation/project plan
4. Define your CSIRT services
5. Define the organizational structure
6. Define the Information Security policy
7. Hire the right staff
8. Utilise your CSIRT office
9. Look for cooperation between other CSIRTs and possible national initiatives

Current status at the global level



102 National CIRT established worldwide

ITU current efforts

65 National CIRT ASSESSMENT

Africa: Angola, Botswana, Burkina Faso, Burundi, Cameroon, Chad, Congo (Dem Rep), Congo (Republic), Côte d'Ivoire, Gabonese Republic, Gambia, Ghana, Kenya, Lesotho, Liberia, Niger , Nigeria, Rwanda, Senegal, Swaziland, Tanzania , Togolese Republic, Uganda , Zambia, Zimbabwe

Americas: Anguilla, Antigua, Barbados, Bolivia, Dominica , Dominican Republic , Ecuador, Grenada, Honduras, Jamaica , St Kitts & Nevis, St Lucia, St Vincent & The Grenadines, Suriname, Trinidad and Tobago

Arab region: Comoros, Djibouti, Jordan, Lebanon, Mauritania , Palestine, Sudan

Asia & Pacific: Afghanistan, Bangladesh , Bhutan, Cambodia, Fiji, Laos, Maldives , Myanmar, Nepal , Vanuatu, Vietnam

Europe & CIS: Albania , Armenia, Cyprus, Macedonia, Monaco, Montenegro, Serbia

14 National CIRT designed and established

1. Barbados
2. Burkina Faso
3. Cote d'Ivoire
4. Cyprus
5. Ghana
6. Jamaica
7. Kenya (+ Enhancement in progress)
8. Montenegro
9. Tanzania
10. Trinidad and Tobago
11. Uganda
12. Zambia
13. Burundi (in progress)
14. Gambia (in progress)

In the Pipeline we've 14 Requests for design and Establishment of a National CIRT:

1. Mozambique
2. Guatemala
3. Mali
4. Senegal
5. Sierra Leone
6. Madagascar
7. DR Congo
8. Uganda
9. Zimbabwe
10. Namibia
11. Grenada
12. Saint Vincent and Grenadines
13. Djibouti
14. State of Palestine

TIME TO PLAN