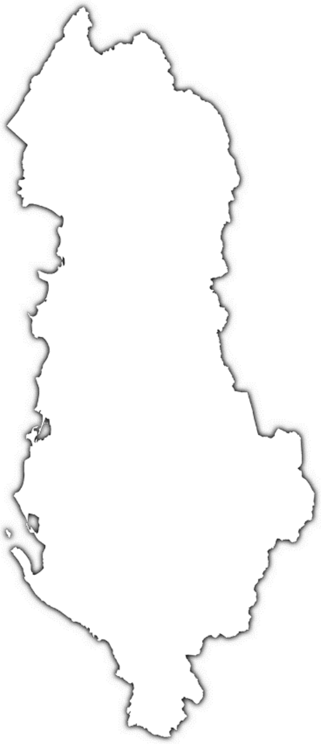
REGIONAL INITIATIVES - EUROPE

READINESS ASSESSMENT REPORT TO ESTABLISH A NATIONAL CIRT IN ALBANIA



Telecommunication Development Bureau

Table of Contents

List of Tables

List of Figures

List of Acronyms and Abbreviations

APTs	Advanced Persistent Threat
CERT	Computer Emergency Response Team
CIIP	Critical information infrastructure protection
CIRT	Computer Incident Response Team
CNIP	Critical National Infrastructure Protection
DDOS	Distributed Denial of Service
FIRST	Forum of Incident Response and Security Teams
GCA	Global Cybersecurity Agenda
GCI	Global Cybersecurity Index
INTERPOL	International Criminal Police Organization
ISP	Internet Service Provider
ITU	International Telecommunication Union
NAECCS	National Authority for Electronic Certification and Cybersecurity
NCS	National Cybersecurity Strategy
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
SSH	Secure Shell
SSL	Secure Socket Layer

Acknowledgement

The International Telecommunication Union (ITU) would like to express sincere gratitude to the representatives from NAECCS (National Authority for Electronic Certification and Cybersecurity) Albania for the support and assistance they provided to the ITU staff. ITU would also like to thank the participants from Albania who showed great enthusiasm and participated well during the assessment workshop.

Executive Summary

This document is a report of a field mission conducted by ITU to TIRANA, Albania to assess Albania's readiness to establish a national Computer Incident Response Team (CIRT). Before producing this report, the expert team consulted and interviewed key stakeholders and also conducted multiple studies and research to gather as many facts as possible regarding the readiness of the country to establish a national CIRT. However, there were times when reasonable assumptions were made due to unavailability of information from the stakeholders.

No national computer security incident response team capabilities are currently established, which poses a challenge to effectively coordinate incident response and management.

No regulation that requires incidents to be reported is in place and Albania lacks a clear mandated authority or protocol to handle such a process.

A list of critical infrastructure (CI) had been already established and the government needs to ensure dissemination of the list and related assets/services to relevant stakeholders.

Communication between the government and CI operators is ad-hoc and therefore coordination is limited. Similarly, risk management exercises or cyber drills are not conducted at a national level.

Based on the assessment carried out, it is timely that the Government of Albania should focus on setting up a Computer Incident Response Team (CIRT), with national responsibility appropriately positioned within the government's institutional and organizational structure as soon as possible.

For the purposes of this report, the proposed national Computer Incident Response Team within NAECCS will hereinafter be referred to as AL-CIRT.

AL-CIRT is the focal point for coordinating the information flow when responding to cyberattacks and will offer remediation of cybersecurity incidents for the whole of Albania. The implementation proposal for AL-CIRT is divided into three phases. In the first phase, the AL-CIRT will offer its services to sectoral CIRTs, government agencies, ministries, law enforcement agencies and regulatory bodies, initially focusing on providing reactive services and some basic levels of proactive services.

As AL-CIRT acquires more experience and based on lessons learned, AL-CIRT can move on to second and third phases accordingly.

It is recommended that AL-CIRT as part of NAECCS, continue to be an executive authority reporting to the Prime Minister's Office.

As the national CIRT for Albania, AL-CIRT would:

a) Develop basic and selected reactive and proactive services in the first phase of establishment

b) Establish a permanent and appropriate space with recommended IT facilities as well as a secured work area and meeting room

c) Function as the coordination center for other CIRTs/CSIRTs within Albania once expected capabilities are met

d) Drive, participate and support the activities of other CIRTs/CSIRTs within the region and globally

e) Cooperate and collaborate with other international CIRTs/CSIRTs for information sharing and coordination.

The readiness assessment shows that Albania is not immune from cybersecurity issues that are being faced by both developed and developing countries. As more and more services are being offered over the Internet, a wider variety of cybersecurity incidents are being reported, ranging from distributed denial of service (DDoS) attacks to Internet frauds. The main stumbling blocks to tackle these incidents are the lack of technical skills and organizational mechanisms at national level.

There are some priority areas that need immediate attention. These include to:

a) Provide training prior to starting the CIRT implementation to improve the skill-sets and competency of the personnel who will be manning the AL-CIRT in areas of cybersecurity as well as to build their confidence in carrying out their duties

b) Conduct a training of trainer's program in Cybersecurity in order to increase the pool of experts who could provide capacity building workshops in Cybersecurity at national level.

c) Improve the overall readiness, availability and reliability of ICT infrastructure and services to the public as well as the private sector

d) Develop applicable policies and regulations for the protection of Critical Information Infrastructure

e) Develop and implement cybersecurity awareness campaigns for the government and the general public

f) Develop, implement and continuously improve cybersecurity legislation.

The development of the above priority areas and the establishment of AL-CIRT can be carried out in parallel.

1 Introduction

1.1 Mission Background

Per the request by the Government of Albania represented by the National Authority for Electronic certification and Cyber Security (AKCESK), ITU is assisting in the assessment of Albania's readiness to implement a national Computer Incident Response Team (CIRT). With the support of the Government of Albania, ITU, conducted a three-day assessment exercise in Tirana, Albania.

The findings and outcomes of the assessment exercise, stakeholder interviews, and additional research form the basis of this report.

1.2 Mission Objectives

The primary objectives of the project were to assess the current capability, resources, and readiness of Albania to implement national CIRT based on input from various stakeholders from both the public and private sector. The overall objectives were to:

a) Study and analyze the current cybersecurity status and needs of Albania

b) Provide high-level recommendations to improve the national cybersecurity posture

c) Provide a project plan for implementing a National CIRT

d) Include the above content and any other information deemed necessary in a report to be submitted in electronic copy to Albania.

1.3 Mission Methodology

The assessment project was initiated by a national CIRT assessment questionnaire being distributed to the government focal point in order for the ITU experts to gain the necessary background information of the ICT and cybersecurity posture of Albania. The offsite research and assessment questionnaire are designed to provide ITU with all the relevant information necessary to ensure a complete analysis of the current context for implementing a national CIRT, a successful realization of the assessment exercise including Albania's cybersecurity maturity review.

The onsite assessment exercise was divided into assessment breakout sessions and cybersecurity capacity building sessions. The breakout sessions were discussions and interviews with key stakeholders that complemented the information gained in the pre-assessment research and served as the foundation for this assessment report. The capacity building sessions assisted the key stakeholders in gaining a basic understanding of the challenges in cybersecurity and the roles, responsibilities and functions of a national CIRT.

For additional data and information collection, the experts also performed a review of relevant documents, past reports, policies, strategies and plans relating to cybersecurity that were provided by the stakeholders during the interviews and meetings. Online websites and publications with information related to ICT and cybersecurity in Albania, such as ITU ICT Eye, ITU

Global Cybersecurity Index, and World Bank Indicators were used to complement the information provided during the assessment exercise.

2 Cybersecurity Context

Today the security of a nation state is not only restricted to its borders and sovereignty but it also extends to protecting against new borderless risks and threats. Globalization and the growth of an interconnected global environment through the Internet have brought immense societal benefits but have also opened up new venues for attacks and threats from governments, criminals, terrorists, private companies, and individuals. The emergence of actors from different locations, with different motives and the desire to challenge the rule of law and international order who can employ readily available tools and operate in a global cyber environment makes it incredibly challenging for nation states to successfully employ protective measures. A breakdown of the main cybersecurity actors, their intention, and threat types can be found in tables 2.1 and 2.2 below.

Governments face a wide range of cybersecurity incidents in their day-to-day reality. There are regular news reports on exploitation of vulnerabilities and disruptions to the ICT infrastructure both in the private and public sector. Even more alarming are the increasing number of targeted attacks through advanced persistent threats (APTs) and attacks on critical infrastructure that could potentially have severe consequences for a nation. The growing number of cyber incidents act as a clear indicator that it is a challenge for governments around the world to put in place effective and timely responses to cyber threats. The current key trends in cybersecurity include:

a) Consumerization, mobile internet and the growth in the number of Internet users are responsible for an incomparable surge in the number of devices connected to the Internet. This development contributes to a more complex management environment and an exponential increase in the number of vulnerable endpoints and users.

b) Digital espionage and cybercrime continue to be the biggest threats for both the public and private sectors.

c) The attackers remain at an advantage. Despite an increased effort from the private industry, governments, and the international community, defenders are still failing to keep up with the complexity, speed, and tools of malicious actors.

d) A significant of portion of cybersecurity incidents could have been resolved through simple and easy to implement preventive measures, highlighting the value of the implementation and auditing of basic security measures as well as cybersecurity awareness and capacity building.

e) Most Internet users and organizations lack the necessary knowledge and skills to adequately protect themselves in the digital environment. As more and more people connect to Internet, especially in the developing world, this will become a more serious concern.

f) Malicious actors take advantage of the long response times from governments and private organizations in implementing security measures and deploying security patches. There is a growing need for increased cooperation and information sharing within the international cybersecurity community to develop and deploy more efficient protective measures.

g) The novelty, variety and complexity of cybersecurity risks and threats require reliable and up-to-date information and situational awareness of the cyber environment.

h) Governments have become increasingly responsible for the coordination of national cybersecurity issues in cooperation with private industry and international actors. National CIRTs have in particular become key cybersecurity actors both nationally and internationally.

The goal of all governments should be to achieve a cybersecurity environment where there is no risk that danger or damage to society or citizens will come from the disruption, loss or abuse of ICTs.

Actor	Intentions	Primary targets	Resources	Prevalence	Visibility
States	Improve position of power	Governments, multinational companies, citizens	High	Medium	Low
Private organizations	Improve information position	Companies	High	Low	Low
Criminals	Monetary gains	Governments, companies, citizens	Average to High	High	Low to Average
Terrorists	Political objectives	Governments, companies, citizens	Few	Low	High
Hacktivists	Ideological objectives	Governments, companies, other groups	Average	Average	High
Script kiddies	Personal interest, to have fun	Governments, companies, citizens, other groups	Low	High	Average
Researchers	Find vulnerabilities	Governments, companies, citizens, other groups	Average	Low	High
Internal actors	Revenge, personal gain	Place of current or former employment	High	Low	Low

Table 1 Cybersecurity Actors and Intentions

	Government	Private organizations	Citizens
States	🟥 Digital espionage	🟥 Digital espionage	🟥 Digital espionage
Private organizations		🟨 Digital espionage	
Criminals	🟥 Disruption as a result of malware, intrusion or spam	🟥 Disruption as a result of malware, intrusion or spam	🟧 Disruption as a result of malware, intrusion or spam
		🟧 Identity fraud	🟧 Identity fraud
	🟨 Blackmail	🟨 Blackmail	🟨 Blackmail
	🟨 Disruption of online services	🟨 Disruption of online services	
Hacktivists	🟧 Publication of confidential data	🟧 Publication of confidential data	🟧 Publication of confidential data
	🟧 Disruption of vital infrastructure	🟧 The disruption of vital infrastructure	
	🟧 Disruption of online services	🟧 The disruption of online services	
	🟨 Hoaxes	🟨 Hoaxes	🟨 Hoaxes
Script kiddies	🟧 Disruption of online services	🟧 Disruption of online services	
Researchers	🟨 Publication of confidential data	🟨 Publication of confidential data	
Internal actors	🟧 Publication of confidential data	🟧 Publication of confidential data	
		🟨 Blackmail	
Not an actor	Fire, water damage and natural disasters	Fire, water damage and natural disasters	
	Failure of power supply	Failure of power supply	
	🟧 Failure and/or absence of hardware and software	🟧 Failure and/or absence of hardware and software	

Table 2 Cybersecurity Actors and Threats Relevance

🟨 Low 🟧 Medium 🟥 High

Ranking	Country	% of attacked users
1	Algeria	32.79%
2	**Albania**	**25.99%**
3	Morocco	25.43%
4	Moldova	24.21%
5	Armenia	23.95%
6	Mauritania	23.95%
7	Belarus	23.49%
8	Philippines	23.48%
9	Venezuela	22.9%
10	Ukraine	22.37%

Table 3 Top 10 countries where users faced the greatest risk of online infection [data for quarter 2 2018][1]

3 Computer Incident Response Teams (CIRTs)

A Computer Incident Response Team (CIRT) is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. Their services are usually performed for a defined constituency such as a corporate, governmental, or educational organization, a region or country, a research network, or a paid client.

There are different types of CERT/CIRT or response teams depending on what type of constituency they serve and what type of services they offer.[2] Similarly, there are also several acronyms used to describe teams providing similar types of services such as CSIRC, CSRC, CIRC, CSIRT, IHT, IRC, IRT, SERT and SIRT.[3]

A CIRT primarily focuses on the response to cybersecurity incidents on behalf of one or more constituents by providing:

a) A single point of contact for reporting incidents and incident coordination

b) Assistance within the constituency and general computing community in preventing and handling computer security incidents

c) Information and lesson learned to its constituents, other CIRT or response teams, as well as other appropriate organizations and international actors.

[1] https://securelist.com/it-threat-evolution-q2-2018-statistics/87170/

[2] CERT is not an acronym; it is a name and a registered service mark of Carnegie Mellon University. The CERT Coordination Centre was the first computer incident response team (CIRT) and although certain CIRT teams have been authorised to use the CERT name by Carnegie Mellon University, the term CIRT is used when referring to general incident response teams.

[3] The definitions are derived from Incident Prevention, Warning, and Response (IPWAR) Manual, USDOE, 205.1-1, Sep 2004 and also Handbook for Computer Security Incident Response Teams (CSIRT), 2nd Edition, April 2003.

In order to provide overarching cybersecurity services to a constituency, CIRTs can also offer a range of reactive, proactive and security quality management services. A more detailed overview of CIRT services can be found in section 6 of this report.

3.1 The Role of a National CIRT

A national CIRT responds to computer security or cybersecurity incidents by providing necessary services to a defined constituency to effectively identify and coordinate threats at the national and regional levels. It also provides information dissemination and acts as the national focal point for matters related to cybersecurity. As of today, there are around 104[4] national CIRTs globally.

The fundamental role of the Government of Albania, to be addressed and managed by the national CIRT, in securing national assets against cyber threats should include to:

a. Provide a national mechanism for incident response, coordination, and resolution

b. Identify and understand current threat landscape and ensure preparedness by adopting appropriate reactive and proactive measures

c. Ensure and maintain the safety and societal wellbeing at all times, particularly in times of crisis

d. Provide appropriate capacity building or training programs to ensure practitioners are able to handle and communicate incidents in a professional manner

e. Protect essential services and ensure continuity of Critical National Information Infrastructure

f. Improve resistance to disruption, breach, damage and loss

g. Implement damage control mechanisms for all national ICT assets

h. Classify sensitive information based on widely adopted information classification system

i. Implement backup, mitigation and recovery plans.

3.2 Benefits of Having a National CIRT

The objective of establishing a strong national CIRT is to establish a trusted focal point of contact within and beyond the national borders for handling cybersecurity matters can provide the following benefits for Albania:

a. A mechanism to identify and manage cyber threats that may have adverse effect on the Government of Albania or the nation itself

b. A mechanism to systematically respond to cybersecurity incidents and take appropriate mitigation actions

c. The ability for the constituency to quickly and efficiently recover from security incidents and minimize loss or theft of information and disruption of services

d. The utilization of information gained during an incident handling activity to better prepare for handling of future incidents and better protect systems and data critical to Albania

[4] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx

e. A mechanism to properly deal with legal issues that may arise during incidents

f. Encouraging knowledge exchange within the constituency and the publication of general security best practices and guidance through publications, websites, and other modes of communications

g. The promotion of education, awareness and training appropriate for a variety of different audiences in Albania

h. Coordination of cybersecurity and CIRT focal points both within Albania and internationally.

As the national and international coordination centers for cybersecurity issues, national CIRTs play a critical role in building a global cybersecurity environment of trust and achieving a safe cyberspace for all countries. The national CIRT within NAECCS should be regarded as a key government authority with a critical role similar to the functions of law enforcement, fire emergency services, and national defense.

Although a developing country like Albania faces several fundamental issues such as the construction of basic infrastructure, it is all the more important that the national CIRT is established before a critical attack occurs. The national CIRT in Albania should be seen as a long-term investment and as a building block on which other cybersecurity projects can be developed.

Figure 3.2.1 below elaborates on how ITU visualizes the roles and responsibilities that a national CIRT can play in protecting its country against cyber threats and also drive other initiatives such as national cybersecurity strategies and policies, cyber forensics services, PKI/digital signature initiatives, governance, legislation, critical information infrastructure protection (CIIP) programs, cybersecurity awareness, training and education, research, international cooperation and security assurance mechanisms.

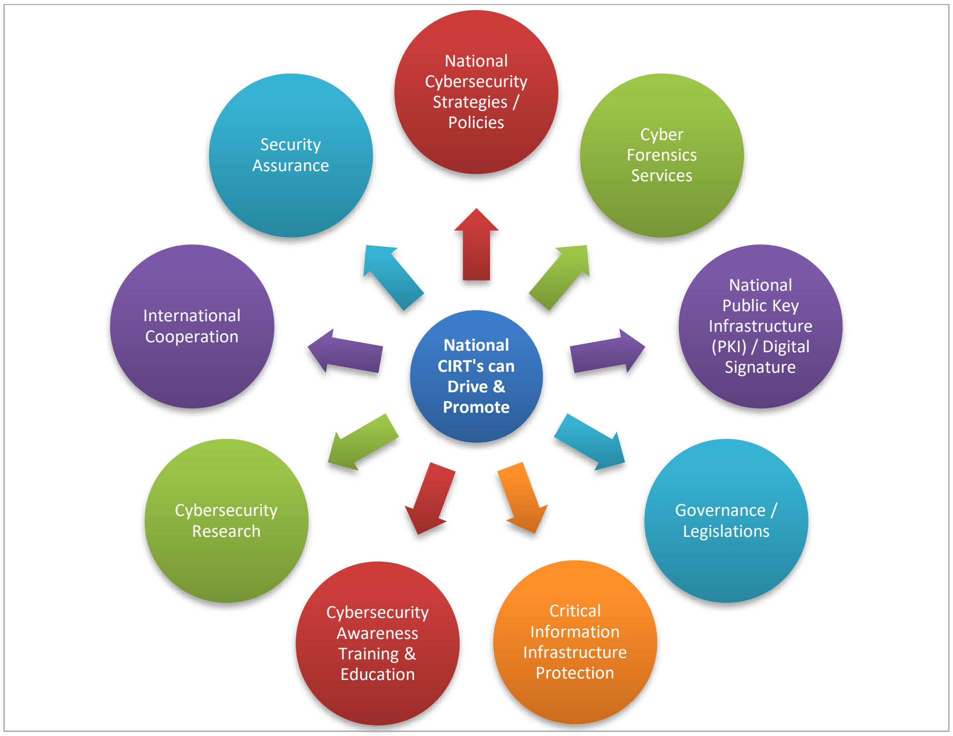

National Cybersecurity Strategies / Policies
Security Assurance
Cyber Forensics Services
International Cooperation
National CIRT's can Drive & Promote
National Public Key Infrastructure (PKI) / Digital Signature
Cybersecurity Research
Governance / Legislations
Cybersecurity Awareness Training & Education
Critical Information Infrastructure Protection

Figure 1The National CIRT as a Cybersecurity Building Block (Source: ITU)

4 Albania Readiness Assessment

This section sets out all the key findings, issues, analysis and recommendations for the enhancement of the current ICT and cybersecurity situation in Albania. These are based on general research and on the information gathered during the onsite assessment and are divided into the following subsections:

1. ICT Landscape
2. Cybersecurity Landscape
3. Cybersecurity Legal Framework
4. Cybersecurity Education and Training

4.1 ICT Landscape

There have been visible improvement in ICT development as a result of the public and private partnerships and their related investments in telecommunications. The dynamism of the policy and regulation of the ICT sector helped to improve the ICT business environment. Nevertheless, the competition is more aggressive in the Mobile/wireless telecommunications market than in the fixed one.

Albania Government's, when defining its Digital Agenda of Albania 2015-2020[5], emphasized the importance to build a robust and modern nationwide network infrastructure to promote and boost the development of an information society in Albania.

4.1.1 Regulatory Landscape

In 2003, the country published its first National ICT Policy Strategy, recognizing the potential of ICTs to enhance economic and social development. The strategy focused on improving access to ICT services but also stimulating demand for ICTs.

This was continued with the 2009-2015 National Strategy on Information Society (NSIS) and the Digital Agenda of Albania 2015-2020, which puts ICTs at the heart of Albania development. The Albania digital agenda aims at increasing investments in ICT infrastructure and boosting policies to provide new digital services. Furthermore, the government is working to improve ICT education and support to outside actors in the ICT sector.

In 2016, an ITU-D report [6]examined the dynamics of the ICT centric innovation ecosystem in Albania and made recommendations to strengthen Albania's ability to integrate ICT innovation in its national development agenda, and leverage the economic and social opportunities provided by innovative technologies.

[5] http://akshi.gov.al/wp-content/uploads/2018/03/Digital_Agenda_Strategy_2015_-_2020.pdf

[6] https://www.itu.int/en/ITU-D/Innovation/Documents/Publications/Albania%20Country%20Review%20Innovation%20June%202016.pdf

4.1.2 ICT development indicators

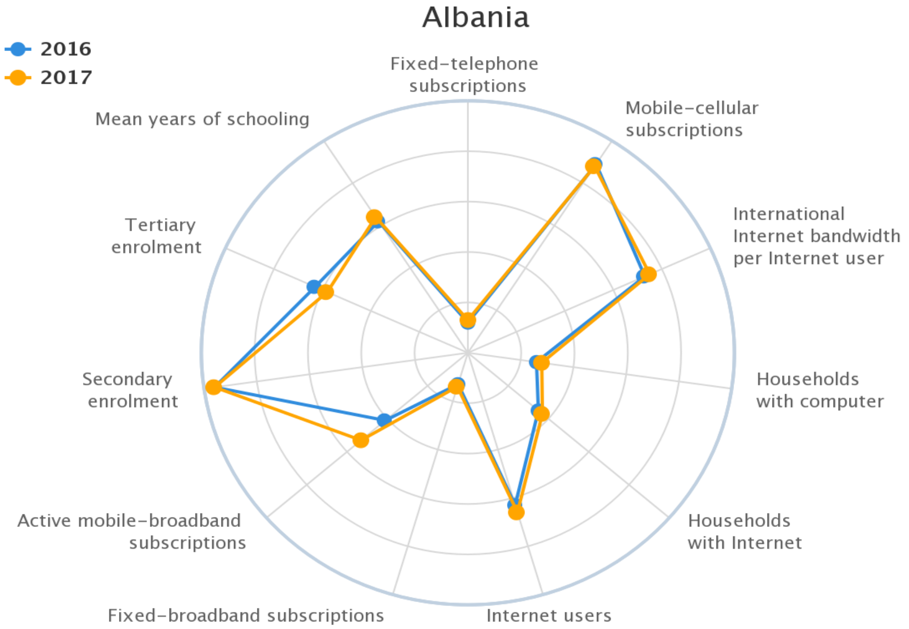


Figure 2 Albania ICT indicators 2017 (Source: ITU)

Fixed Line subscribers at the end of 2016 was about 248 000, while in 2017 it reached about 244 000, which is a 2% decrease. The fixed penetration rate (number of subscribers per 100 subscriptions) at end-2017 reached 8.6%, which is much lower than developed countries (about 40%), about twice lower than the world average (15.2 %), even lower than the average of developing countries (10%).

Fixed network traffic from the Internet reached 85.4 million GB in 2016, which constitutes an increase by several times in the recent years. During 2016, a mobile user has consumed 954 MB per month compared to 541 MB in 2015. Incumbent Operator's active users had the largest consumption of mobile broadband access data at 1.9GB / month

The number of subscribers with broadband access from fixed networks by the end of 2016 has seen an annual growth of about 9%, but only 16.7% of them use a speed of over 10Mbit/s.

The penetration rate per population and household of subscribers with fixed broadband access by the end of 2016 was 9.3% and 33.4% respectively

Mobile broadband continues to grow rapidly. By the end of 2016, this number has grown by almost 30% more than in 2015; increased use of broadband access from 3G/4G mobile networks in recent years may also be noticed by the increase in the volume of data transmitted to mobile networks. In 2014, the annual growth of data traffic in mobile networks was 148%, and this trend continues in 2015 and 2016, with an annual growth of 103% and 110% respectively. During the period 2013-2016, the volume of Internet access data to mobile networks has increased more than 10 times

4.2 Cybersecurity Landscape

The Internet infrastructure in Albania is still at development stage and Internet penetration throughout the country is slightly average, around 66% of the population had access to the Internet in 2017.[7]

Alongside improved Internet performance, Albania has also seen the emergence of various forms of cybercrime of varying scales. Common forms of cybercrime prevalent in Albania include internet banking related fraud such as phishing and spam.

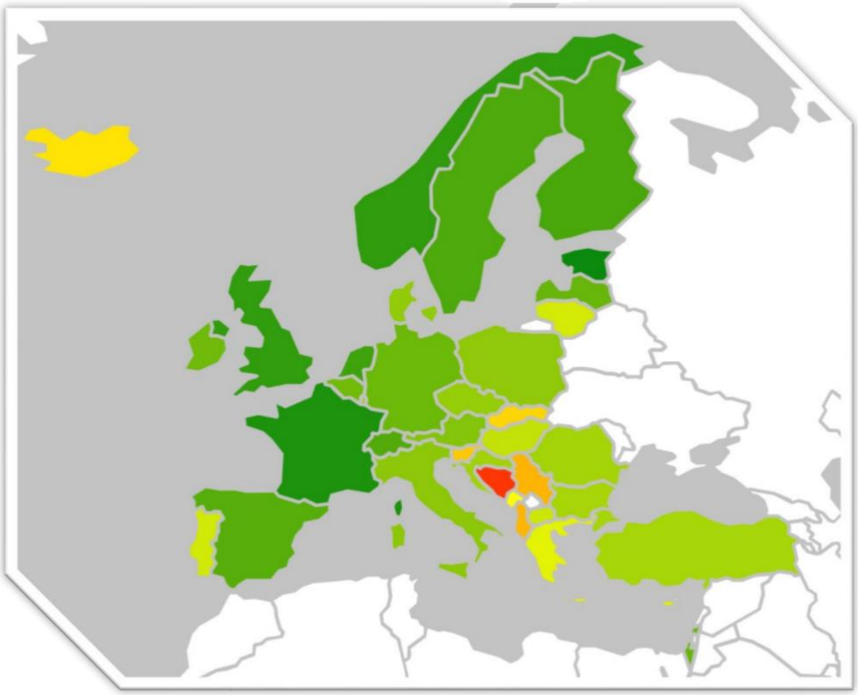
4.2.1 Albania's level of maturity in cybersecurity compared to the Europe region

The Global Cybersecurity Index (GCI) is a survey that measures the commitment of Member States to cybersecurity in order to raise awareness.

The GCI revolves around the ITU Global Cybersecurity Agenda (GCA) and its five pillars (legal, technical, organizational, capacity building and cooperation).

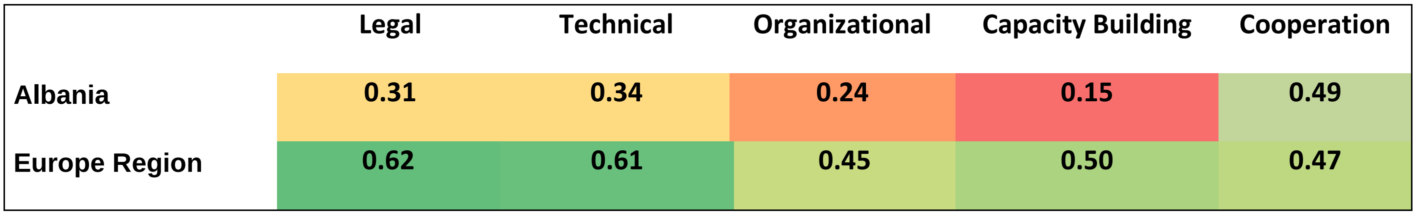
In GCI 2017, Europe region Member States were classified into three categories by their GCI score.

The commitment to cybersecurity of the European region is well illustrated in the heat map above and the table, where most countries are in the leading and maturing stages.



[7] http://www.itu.int/net4/ITU-D/idi/2017/index.html

Leading stage 🟢	Estonia, Latvia, France, Germany, Norway, Ireland, United Kingdom, Belgium, Netherlands, Austria, Finland, Italy, Sweden, Poland, Switzerland, Denmark, Spain, Czech Republic, Israel, Luxembourg.
Maturing stage 🟡	Croatia, Cyprus, Romania, Greece, Turkey, Montenegro, Bulgaria, Malta, Hungary, Iceland, TFYR of Macedonia, Slovakia, Portugal, Slovenia, Lithuania, **Albania**, Serbia.
Initiating stage 🔴	Monaco, Bosnia and Herzegovina, Liechtenstein, Andorra, San Marino, Vatican.



	Legal	Technical	Organizational	Capacity Building	Cooperation
Albania	0.31	0.34	0.24	0.15	0.49
Europe Region	0.62	0.61	0.45	0.50	0.47

Figure 3 Cybersecurity Commitment in ITU Europe region 2017

4.2.2 Cyber threats Affecting Albania

There have been cybersecurity incidents in Albania but they have mainly been dealt with by the organization in which the incident occurred.

Albania does not currently have a mechanism to track and understand the cybersecurity incidents (in national level) and threats that are occurring in the country.

Some of the common types of cybersecurity incidents, based on onsite discussions, are related to:

- Scams
- Phishing
- Viruses and worms
- Frauds (including credit card fraud)
- Web defacement
- Denial of Service

4.3 Critical National Infrastructure Protection (CNIP)

CNIP is a term used by governments to describe information assets that are essential for the functioning of a society and economy.

NAECCS functions according to the bylaw No. 141, date 22.2.2017, “On the organization and functioning of the National Authority for Electronic Certification and Cyber Security” and is the responsible body for applying of the Law no. 2/2017 “On cybersecurity”. NAECCS is the national coordinator and the contact point for the government and CI operators.

The Council of Ministers, with its Decision No. 222, dated 26/04/2018 has clearly defined the list of national CNIP . Standardized policies and procedures for CNIP at the national level, need to be further developed and applied .

There is no defined cybersecurity operational strategy for CNIP in place to manage and mitigate cybersecurity incidents in case of a coordinated cyberattack on critical infrastructure.

4.3.1 Recommendations

The above findings clearly indicate the need for a stronger national CIRT that acts as a focal point in managing incidents and as a coordination center to manage information sharing and information flows so that all relevant parties can report incidents to this central point.

AL-CIRT will also provide knowledge of available good practices that can be shared and implemented on the various networks.

There is also a clear need for the national CIRT to have an adequate cybersecurity situational awareness system in place (to evolve into a threat intelligence capability) so that the CIRT and its constituency are aware of the types of threats and attacks that are happening both domestically and globally and are able to either establish preventive measures or be more reactive in case of breaches.

It is also recommended that following the implementation of AL-CIRT, large organizations that are responsible for the country’s critical national infrastructure should establish their own CIRTs that would collaborate with the AL-CIRT. These would be known as sectoral CIRTs and they would be constituents of the AL-CIRT.

AL-CIRT is formally mandated by the government, and clearly recognized as the empowered entity to deal with incident response and coordination. To this end, according to existing good practices, law or regulation would need improved in line with existing the legislative/regulatory national process.

As Albania has already recognized a large number of critical and highly interdependent nature of - CNI at the moment aims to develop and establish a comprehensive program and a series of measures that will ensure the effectiveness of cybersecurity controls over vital assets. Albania is to ensure that the CNIs are protected to a level that is proportionate to the risks faced.

Outreach programs should be developed to sensitize the public about the dangers associated with cyber threats. Training and education should be conducted to teach users basic steps for dealing with IT security issues.

Ensure the security of communication among stakeholders within the redundant communication network.

4.4 Cybersecurity Legal Framework

A comprehensive national approach to cybersecurity cannot be done by only using technologies and services but has to be coupled with a good and current legal framework to cater for the dynamic nature of the ICT environment and the evolving nature of cyber threats.

There is general awareness from the stakeholders that Albania faces significant threats from cybercrime and other cybersecurity related attacks.

A legal, regulatory framework, which protects against different forms of electronic abuse and crime is essential to creating a trusted environment for electronic communications and transactions. The laws that have aspects relating to Cybercrime

- Law No.7895, dated 27.01.1995, "Criminal Code of the Republic of Albania"
- Law No.2/2017 "On cybersecurity"
- Law No.9918, dated 19.05.2008, "On electronic communications in the Republic of Albania"
- Law No.9887, dated 10.03.2008, "On protection of personal data"
- Law No.8457, dated 11.02.1999, "On classified information"
- Law No.9880, dated 25.02.2008, "On electronic signature"

There is currently no dedicated draft legislation containing substantive and procedural cybercrime provisions also there is limited legislation/ regulation imposing the implementation of cybersecurity measures for the protection of the critical information infrastructure.

4.4.1 Recommendations

Concerned stakeholders should expedite the process of making changes on cybersecurity laws because delays give cybercriminals the chance to exploit legal loopholes.

Development and adoption of a comprehensive legislative framework addressing cybersecurity, cybercrime, human rights online, child online protection, personal data privacy, data protection, consumer protection and intellectual property online is essential to improve national cybersecurity posture.

The development of a more updated legislation should ensure harmonization of national laws with applicable regional work and international good practices.

Where possible accessing, signing, ratifying and implementing regional cybersecurity related instruments, including through the allocation of sufficient resources according to national priorities.

It is important to develop and implement awareness campaigns to educate users, law enforcement and policy makers about cyber laws, the impact of cybercrime and measures of combating it. AL-CIRT can take the lead in the creation of cybersecurity awareness campaigns.

Due to rapid changes in technology there is a need to ensure that laws are technology neutral in order to cater for the dynamic nature of ICT technologies and combat cybercrime effectively.

The Government should take a proactive role in recording complaints and creating a database for reported cybersecurity incidents in collaboration with other relevant agencies like the AL-CIRT, INTERPOL, banks, ISPs and so forth that will help tracking cybercriminals and combating cybercrime both domestically and globally.

While there is a definite need for an AL-CIRT, the need for cybercrime legislation is also a pressing requirement. Relevant cybersecurity legislation should be developed in tandem with the development and implementation of AL-CIRT. Without cybersecurity laws, a national CIRT cannot perform its duties effectively.

4.5 Cybersecurity Education and Research

Human resources with adequate skill-sets and qualifications in cybersecurity has proven to be one of the toughest challenges for developing countries in terms of implementing a national CIRT and improving the overall national cybersecurity situation. It is key that the Government of Albania can ensure a sufficient level of cybersecurity education and research to sustain the domestic need for cybersecurity professionals.

There are some high level university [8]degrees being offered in cybersecurity and there are no cybersecurity research initiatives in Albania.

All stakeholders and constituent organizations recognized that there is a high need for training individuals in cybersecurity. There are individuals with IT and networking background in some stakeholder organizations that could be eligible to undertake cybersecurity courses.

There is a lack of a common approach in educating government staff and the public on the need for safer practices and awareness of cybersecurity.

4.5.1 Recommendations

The most pressing activity is the establishment of AL-CIRT and acquiring the right technical expertise to operate it. This can be achieved by sending the identified candidates for appropriate training and seminars be it locally (if available) or abroad.

To establish the national CIRT, the stakeholders should conduct a talent search to identify the right people with adequate qualifications to operate the CIRT. A training needs assessment should also be conducted to identify the right set of courses that the identified personnel should partake in.

Relevant ministries such including the Ministry of Education, Sport and Youth and the proposed national CIRT can develop cybersecurity specific syllabus that can be made available to local colleges and universities to produce skilled job ready talented pool of cybersecurity professionals locally.

The national CIRT should conduct awareness programs in public organizations and government offices to increase the awareness level.

[8] There is a master degree on Information Security in the Economic Faculty at the University of Tirana, as well as a recently open the same MD about Cyber Security in the University College Luarasi

To impart the culture of cybersecurity, stakeholders can also embark on activities such as research programs relevant to cybersecurity areas with tertiary students. The research programs can be coupled with rewards such as scholarships or employment opportunities to encourage additional participation.

Through partnerships and Memorandums of Understanding (MoUs), the Government can bring in various cybersecurity training providers and make courses accessible in Albania. Scholarship programs can also be offered to encourage professionals in Albania to venture into cybersecurity areas.

It is strongly recommended that in parallel with the establishment of the National CIRT, the national authority for electronic certification and cybersecurity conduct a training of trainer's program in Cybersecurity in order to increase the pool of experts who could provide capacity building sessions in the Cybersecurity filed at national level.

5 Action Plan to Establish AL-CIRT

Based on the assessment exercise it is recommended that the Government of Albania proceeds with the implementation of the national CIRT, AL-CIRT, as soon as possible.

ITU recommends that AL-CIRT ideally should be would be as it is, part of NAECCS reporting directly to the Prime Minister's Office

It was highlighted above that the key strength of a CIRT is the competency of its staff. Thus, for each phase identified below, a training needs and suitable tools assessment must be conducted that will lead to the identification of appropriate training programs for the staff so that adequate competencies can be achieved.

In addition to human capacity, it is also important to set up the network infrastructure, hardware and software for the CIRT, which needs to be done in the first phase before the start of any training programs. This is a critical requirement so that the trained personnel can immediately apply their knowledge on the daily CIRT routines.

ITU proposes a holistic three-phased approach to establish AL-CIRT. In order for AL-CIRT to effectively deliver its services in accordance to the phases identified, several key requirements are identified in this section. Most important of all is human capacity development.

The figure below gives an overarching view of the timelines for each of the phases involved.

The identification of the main components of the CIRT, such as its positioning, the constituency (the clients) the service that the CIRT will deliver, the technology requirements, the premises, the human resources, as well as the processes and related procedures will be done during the design phase.

However, general indications are provided in the below chapters.

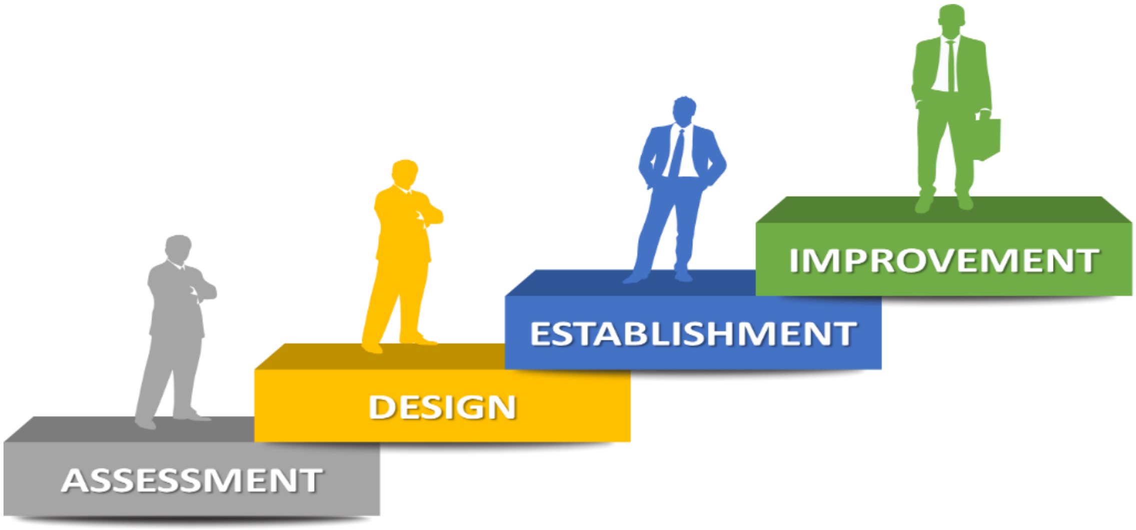


Figure 4 Proposed AL-CIRT Implementation Phases (Source: ITU)

5.1 Design (Phase 1)

This phase will develop a blueprint of the National CIRT project, with the related implementation processes. The key deliverables of this phase are the CIRT design document and implementation plan.

Design	
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

Table 4 Design Phase

5.2 Establishment (Phase 2)

A basic set of solutions with some technical components such as an incident management system, mailing list, public portal and advisories will be needed to operate the CIRT. The AL-CIRT staff (analysts and manager) will also need training in CIRT management, tools and technologies.

Other freely available resources can also be acquired such as membership with the Forum of Incident Response and Security Teams (FIRST). Membership with FIRST enables incident response teams to have more effective reactive and proactive reactions to security incidents.

The establishment phase will include the following activities:

Establishment	
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

Table 5 Implementation Phase

5.3 Enhancement (Phase 3)

The enhancement phase will focus on setting up advanced CIRT services and include the following activities.

Improvement	
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

Table 6 Enhancement Phase

6 CIRT Services

The service model and related services will be properly identified during the design mission.

Good practices show a sort of a common approach in structuring the services that a CIRT would provide to its constituency.

Below the service structure that would be adopted for AL-CIRT. To be noted that this structure is taken from the current work undertaken by the Forum for Incident and Security Response Team (FIRST)[9], which represent the biggest incident response community globally.

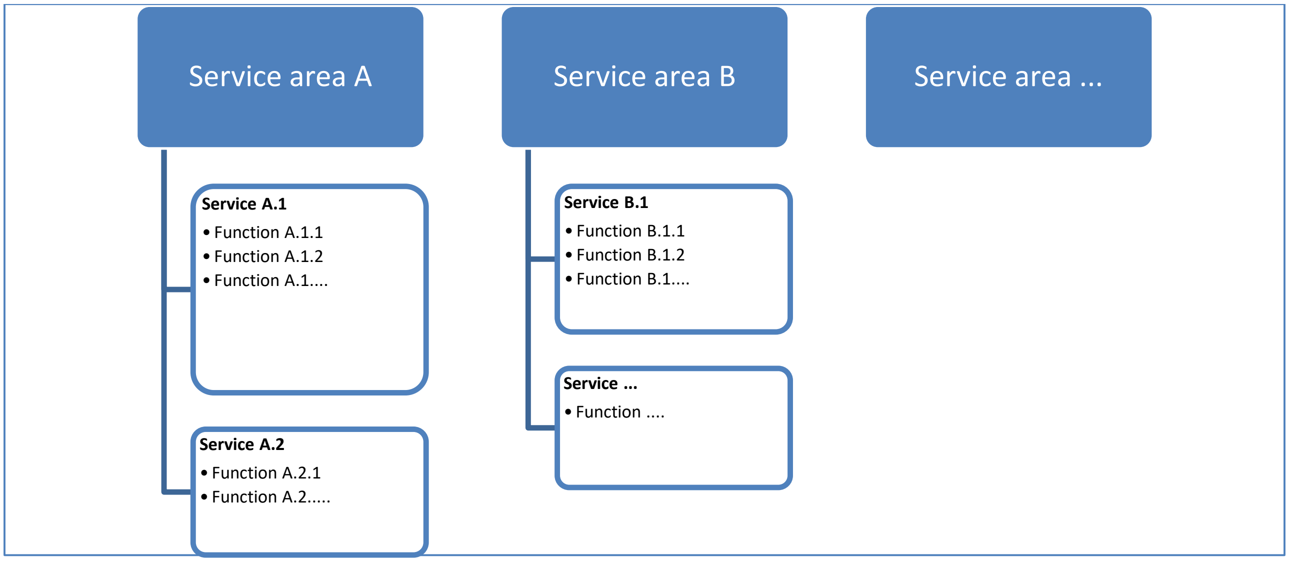


Figure 5 CIRT Service Structure

Service area represent group if services related to a common aspect. They help to organize the services along a top-level categorization in order to facilitate understanding. A Service is the set of recognizable, coherent actions towards a specific result on behalf of or for the stakeholder of an incident response team. In addition, functions are specific tasks of a specific service used to implement the service.

6.1 Potential Service model of AL-CIRT

The following picture highlights the potential set of services that AL-CIRT would be made available. The list of services has been identified talking account the information gathered during the assessment mission.

[9] https://www.first.org/education/CIRT_service-framework_v1.1

The final list of services would be agreed during the design phase.

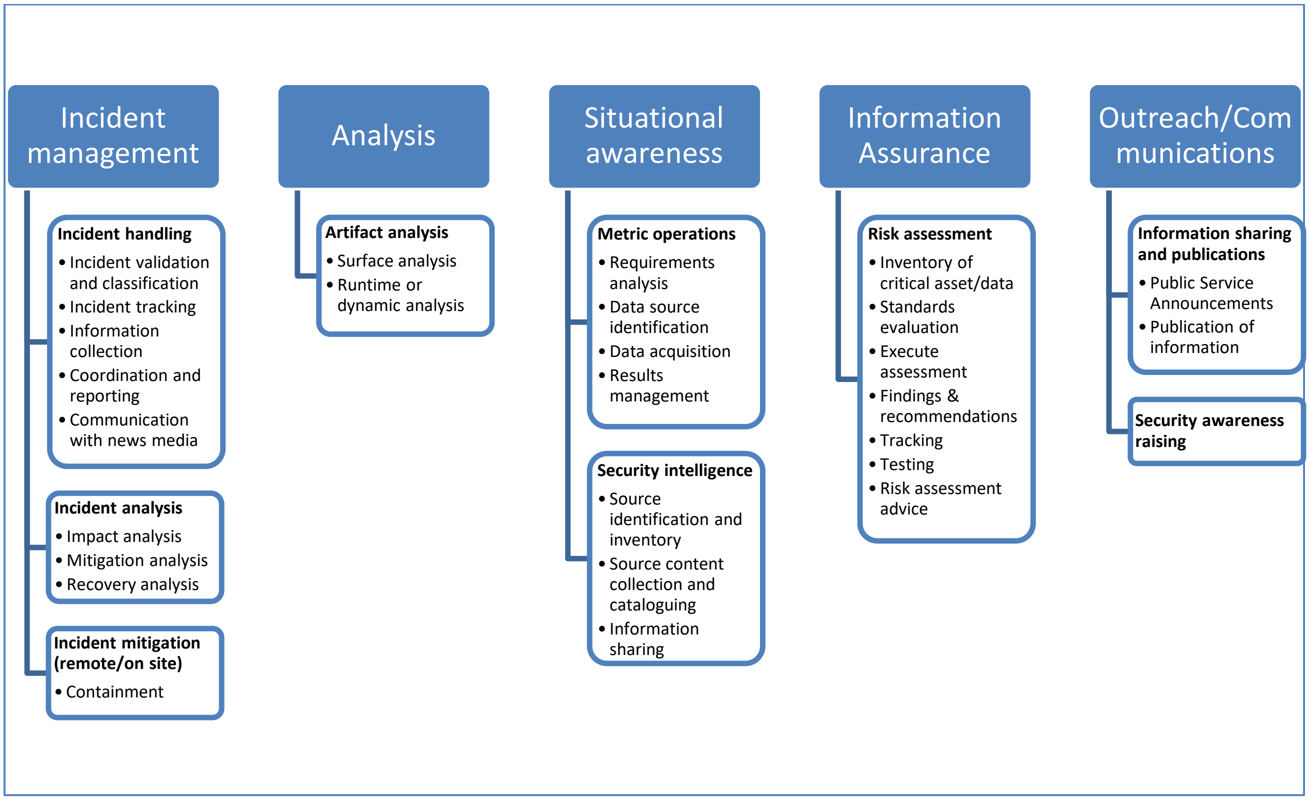


Figure 6 CIRT Potential Services

A phased approach would be adopted for the development of the services. Typically a National CIRT would start with Incident Management and Outreach and communication (defined as reactive services). Once these services are well consolidated and the related processes and procedures well established, the development and availability of additional services to the constituency would follow; in this specific example, Analysis (such as forensic) Situation awareness (such as threat intelligence), and Risk assessment.

6.2 Service parameters

According international best practice[10] each service will have the following parameters to be properly documented in the service catalogue.

Attribute	Description
Objective	Purpose and nature of the service

[10] Handbook for Computer Security Incident Response Teams (CIRTs), CMU/SEI-2003-HB-002, Carnegie Mellon Software Engineering Institute

Attribute	Description
Definition	Description of scope and depth of service
Service level	The conditions under which the service is available: to whom, when, and how
Quality assurance	Quality assurance parameters applicable for the service. Includes both setting and limiting of constituency expectations
Interactions and information disclosure	The interactions between the CIRT and parties affected by the service, such as the constituency, other teams, and the media. Includes setting information requirements for parties accessing the service, and defining the strategy with regard to the disclosure of information (both restricted and public).
Interfaces with other services	Define and specify the information flow exchange points between this service and other CIRT services it interacts with.
Priority	The relative priorities of functions within the service, and of the service versus other CIRT services.

Table 7 Service Parameters

7 Technology and infrastructure

AL-CIRT will require a dedicated IT infrastructure to ensure adequate data separation for its investigations and coordination work.

Generally, AL-CIRT should retain control of its own network border firewall, this means that the following assets should remain under the exclusive control of AL-CIRT:

- Network border firewall
- Primary computing hardware for AL-CIRT operational data
- Backup equipment for AL-CIRT data.

AL-CIRT should control access to its ICT infrastructure either within its secure perimeter or another secure space within the data center of its building.

A lockable server rack will be required for the machines and the rack must be located in a secure storage room similar to that for the AL-CIRT office. The network design of AL-CIRT should be kept as simple as practically possible.

The figure below shows a potential network topology for AL-CIRT.

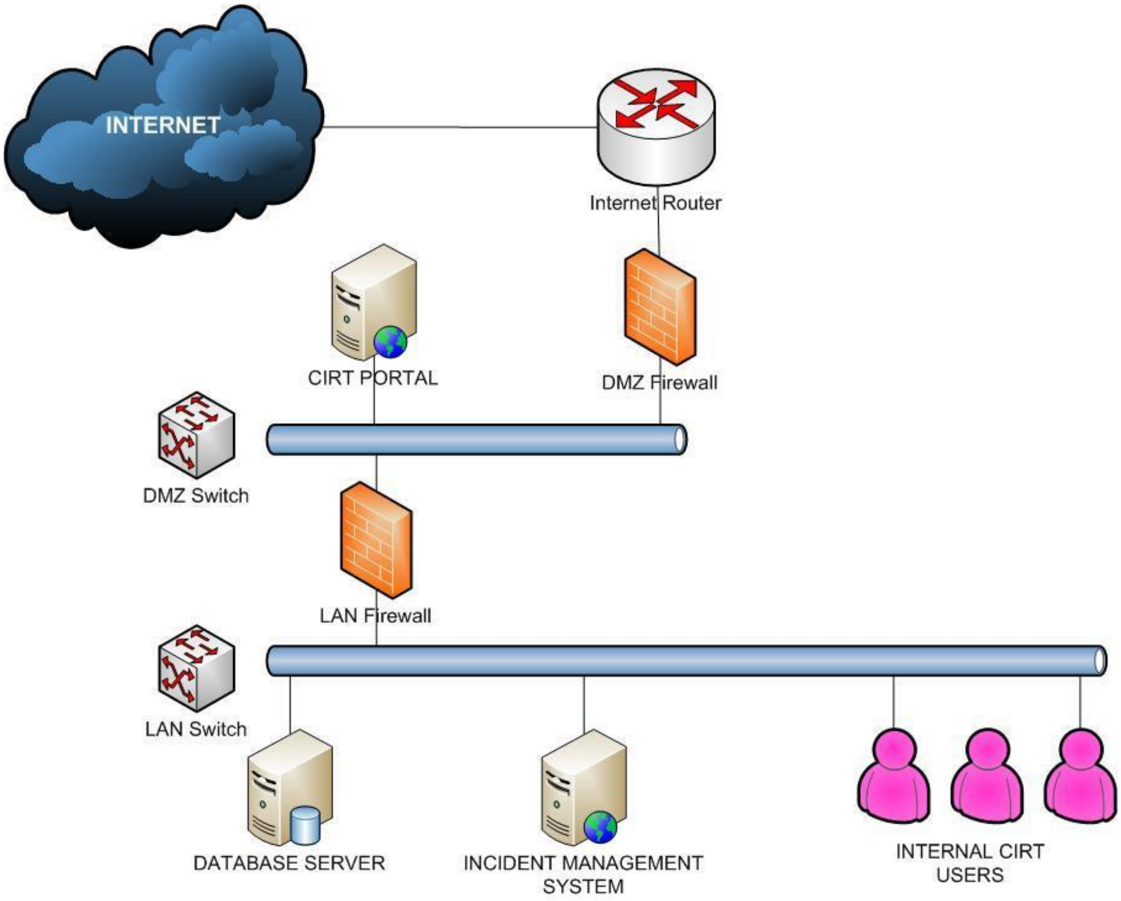


Figure 7 Potential Network Topology

The table below summarizes the list of the essential hardware that is required to operate the CIRT, according to the above network topology.

To be noted that the below identified hardware will be sufficient to provide basic CIRT services (as described in section 6.1).

The more mature the CIRT becomes the more investment in HW and SW will be needed.

The exact list of the equipment and the technical specifications will be finalized during the Design phase.

Type	Role	Quantity
Router	Connection to the ISP	1

Firewall	DMZ and LAN Firewall	2
Switch	DMZ and LAN Layer 2 Switching	2
Web Server (Apache, PHP) Server	Web server for the CIRT Portal and Mailing List solution	1
Mail Server Server	Mail server for email communication between the CIRT and the public	1
Database Server	Database server for Incident Management System running on RTIR	1
Laptops & desktops	User workstations (incident management, normal office activities)	3 Laptops 3 Desktops
Printer	Networked Laser Printer for general purposes tasks	1

Table 8 Potential Equipment List

8 Premises

The nature of operations of AL-CIRT makes it necessary for the CIRT premises to have a high level of security. To ensure separation of function, a physical security perimeter will be necessary and this will entail a separate office space for the AL-CIRT.

The premises should have the following characteristics:

- a separate reception/waiting room for visitors
- an operations center where the analysts conduct day-to-day activities and other functions
- an office for the general manager, large enough to accommodate private meetings
- a path from the reception area to the office that does not transit the operations center
- a meeting room, ideally with a viewing gallery for the operations center
- a data storage area for documents and network equipment, which could incorporate the rack space for AL-CIRT infrastructure (see Section 7 on Technology and infrastructure).

The figure below depicts a potential setup for the premises.

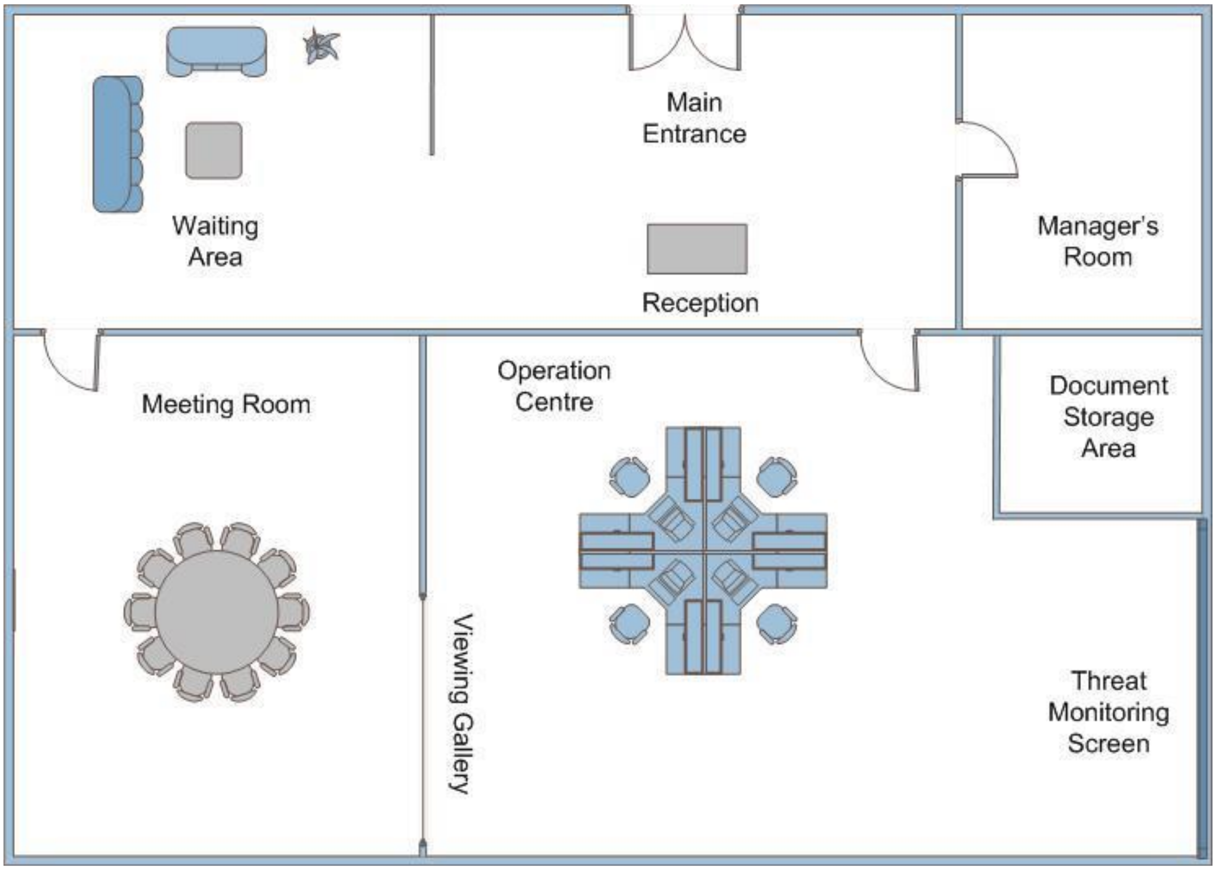


Figure 8 Potential setup of premises

9 Human Resources

It is recommended that AL-CIRT be staffed by a minimum of five people; a CIRT Manager and three analysts and one communication officer.

The CIRT Manager will supervise the three technical staff. Three analysts are necessary to ensure that operations may continue with one staff member is absent due to ill-health, leave or other CIRT related matters such as training, workshops or conferences.

It is also essential that the identified resources CIRT operations have an opportunity for constant learning and development. Hence, regular trainings should be provided and the members should be given exposure to international cyber security events and conferences.

The exact number of staff would be identified during the design phase, as it may vary according to the nature and number of services that the CIRT will make available as well as the magnitude of the constituency (client base) to be covered.

The below tables are provided as examples of the skillset that might be required for the AL-CIRT staff.

CIRT Manager
Qualifications and Experience • Bachelor’s Degree and Master’s Degree in Computer Science/ ICT/ Engineering – Electronics, Telecommunications or any other relevant area • MBA or MSC in Management will be considered an advantage • Professional certification in one or more relevant information/cyber security fields such as: CISA/CISM/CCISO/CISSP/CEH/GCIH • At least five (5) years of working experience in relevant field. • At least three (3) years of experience in team management and coordination of relevant work • Very Good oral and written command of English
Technical Competence • An active knowledge in information and cyber security, and trends • Deep understating in various information and cyber security frameworks like ISO27001, NIST CSF, including security related EU directives, regulations and national laws • Basic working knowledge of a broad range of IT technologies, platforms, operating systems • Knowledge in information security risk assessments • Strong writing skills required for preparation of documents and reports
Personal Competence • Leadership • Management and decision making • Coordination • Conflict management • Analytics • Stress resistant
Responsibilities/Tasks • Oversees, supervises and supports the entire operations and workforce of the CIRT • Strategic CIRT direction within applicable EU directives and national laws • Liaises with national and international authorities/organizations, represents team within CIRT community • Owns and executes CIRT strategy (governance, services / processes establishment, human resources, and technologies; develops, implements and maintains processes, procedures and guidelines to improve and increase the effectiveness of the operations of the CIRT)

• Lead yearly acquisition plan, purchasing and tendering processes • Setups, maintains and controls service level parameters • Manage CIRT human resources • Coordinates cross-institutional activities in cyber security, including crisis management • Coordinates, produces yearly, quarterly and ad-hoc reports • Complies with and ensures compliance with CIRT policies, procedures and guidelines.
Suggested trainings profile for technical competence • Official training courses for CISM, CISA, CISSP, CCISO, including certification • ISO/IEC 27001 Information Security Management System (ISMS) training course • Information Security Management Systems (ISMS) Auditor/Lead Auditor Training Course • TERENA TRANSITS-I / II trainings • FIRST Basics of incident handling course

Table 9 CIRT Manager Skillset

Incident manager
Reports to: • CIRT Manager
Qualifications and Experience • Bachelor’s Degree in Computer Science/ ICT/ Engineering – Electronics, Telecommunications or any other relevant area • Preferable Master’s Degree in Computer Science/ ICT/ Engineering – Electronics, Telecommunications or any other relevant area • Professional certification in one or more relevant information/cyber security fields such as: CISA/GCIH/GIAC/CHFI/CCNA Security • At least five (5) years of working experience in relevant field. • Very Good oral and written command of English
Technical Competence • Incident handling: containment, evidence handling, recovery and remediation steps • In-depth understanding of how the Internet infrastructure functioning • Fundamental knowledge of at least the following protocols: IRC, DHCP, FTP, SMB, SNMP, ICMP • Detailed knowledge of application layer protocols commonly used by Trojan malware, namely TCP, UDP, HTTP[S], SMTP, and DNS

- IP networking (IPv4 and IPv6, TCP, UDP and ICMP, network address translation, security implications of shared media, switched media and VLANs, IP Subnets, IP Routing), network traffic capture, network configuration security issues, firewalling techniques
- Knowledge of common classes of tools used to perform intrusion analysis and reverse engineering
- Host, operating system and application fingerprinting techniques
- Encryption and encoding, symmetric / asymmetric encryption, encryption algorithms: DES, 3DES, AES, RSA, RC4
- Applications of cryptography: SSL, IPsec, SSH, PGP
- Data sources and network log sources
- Command and control channels
- Identification and access management
- Security vulnerabilities and prevention techniques
- Strong writing skills required for preparation of documents and reports

Personal Competence

- Coordination
- Communication
- Analytics
- Stress resistant

Responsibilities/Tasks

- To plan, execute, assess and monitor all tasks related to Incident management service, including assurance of agreed service level, incident response coordination when major incidents occur, escalation activities
- Team coaching and directing about how to handle cyber security incidents
- To plan, execute, assess and monitor all tasks assigned by the Team Leader
- Supervise or lead important cyber investigations
- Represent team within CIRT community
- Ensure balance of incident assignments with incident handlers and duty officers
- Preparing informational products for constituency
- Prepare technical part of terms of references while tendering
- To develop training modules and technical documentation
- To conduct knowledge sharing sessions for other technical personnel on lessons learned or new findings.
- Complies with and ensures compliance with CIRT policies, procedures and guidelines

Suggested trainings profile for technical competence

- CERT games, cyber exercises, and investigation challenges

• Computer hacking forensic investigator training course • FIRST Basics of incident handling course

Table 10 Incident Manager Skillset

10 Estimated effort

The below table provides an indication of the potential effort needed to implement the project.

To be noted that during the design phase, some adjustment might be needed to reallocate time and resources, according to the specific needs identified.

Also the estimated effort does not take into account the Improvement phase, as more mature proactive services might not be needed in the first period of operations. (See Figure 5.1)

Phase	Activities	Location	Estimated man days
DESIGN	1. CIRT positioning	Off-site	3
	2. Identify CIRT services	Off-site	2.5
	3. Identify processes and related workflows	Off-site	4.5
	4. Identify policies and procedures	On-site	4.5
	5. Relationship with constituency and communication strategy	Off-site	7.5
	6. Technology	Off-site	7.5
	7. Premises	Off-site	4.5
	8. HR	Off-site	5.5
	9. On-site Visit	On-site	15
	10. Finalization	Off-site	6
Subtotal			**60.5**
ESTABLISHMENT	1. Capabilities development	Off-site	38
	2. Capabilities deployment and testing	Off-site	29
	3. Customization, fine tuning and training	On-site	26
	4. Operations	Off-site	30
	5. Handover and closure	Off-site	6.5
Subtotal			**129.5**
GRAND TOTAL			**190**

Table 11 Potential Project Implementation Effort

11 Financials

The cost for the establishment varies greatly in function of several conditions and dependencies, such as the level of expertise of the CIRT staff, the availability of existing IT equipment, the availability of physical premises, and above all the services that the CIRT intends to provide to its constituency.

The below cost is an indicative estimation calculated according to the results of the assessment performed on-site. A more accurate estimation will be provided, once Albania will commit to go ahead with the project. At that time, further interactions will be needed with the identified national focal point in order for ITU to accurately identify the needed budget.

Notes on estimated cost – Service

- The efforts are expressed in number of days taking into account the usage of one resource full time. The indicative cost of such resource is estimated based on the standard ITU staff cost.
- The project team will be composed by more than one resource, with different qualifications and expertise.
- The expenses related to the procurement of the necessary Hardware (HW) and Software (SW) licenses are included. The possible procurement of the HW and SW is responsibility of the ITU is coordination with Albania
- ITU will manage the bidding process on behalf of Albania, through an international call for bid. The timing for the conclusion of the bid and the acquisition of the material mighty vary according to the import procedures in Albania in case the material is acquired outside the country.

Note on the estimated cost - Missions

- The Daily Subsistence Allowance (DSA) for Albania (Tirana) is 147 USD.
- The flight tickets are not included in the costing as might greatly vary. As such the mission costs will vary according to the timing and the current rates of flight tickets.

Note on the overall cost

- A 7.5% of the below estimates (including flight tickets) must be added as Administrative Fee for the ITU, who will manage all procurement, project management, and general oversight of the project.

Annex –References

A generic national Framework for CIIP	www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf
A step-by-step approach on how to setup a CSIRT	www.enisa.europa.eu/act/cert/support/guide/files/csirt-setting-up-guide
Benefits of national CERTS	www.cert.org/archive/pdf/nationalCSIRTs.pdf
Computer Security Incident Handling Guide (NIST)	csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf
COP Guidelines	www.itu.int/osg/csd/cybersecurity/gca/cop/index.html
CSIRT Services	www.cert.org/csirts/services.html
Implementation of WSIS Action Line C5	www.itu.int/wsis/c5/index.html
ITU Activities related to Cybersecurity	www.itu.int/cybersecurity/
ITU Global Cybersecurity Agenda	www.itu.int/osg/csd/cybersecurity/gca/
ITU ICT Eye	www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
ITU ICT Development Index (IDI) 2017	www.itu.int/net4/ITU-D/idi/2017/
ITU Global Cybersecurity Index 2017	www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
National Cybersecurity Guide	www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx
World Bank Indicators	data.worldbank.org/indicator/