المـركز العـربي الإقليـمي للأمن السـيبراني

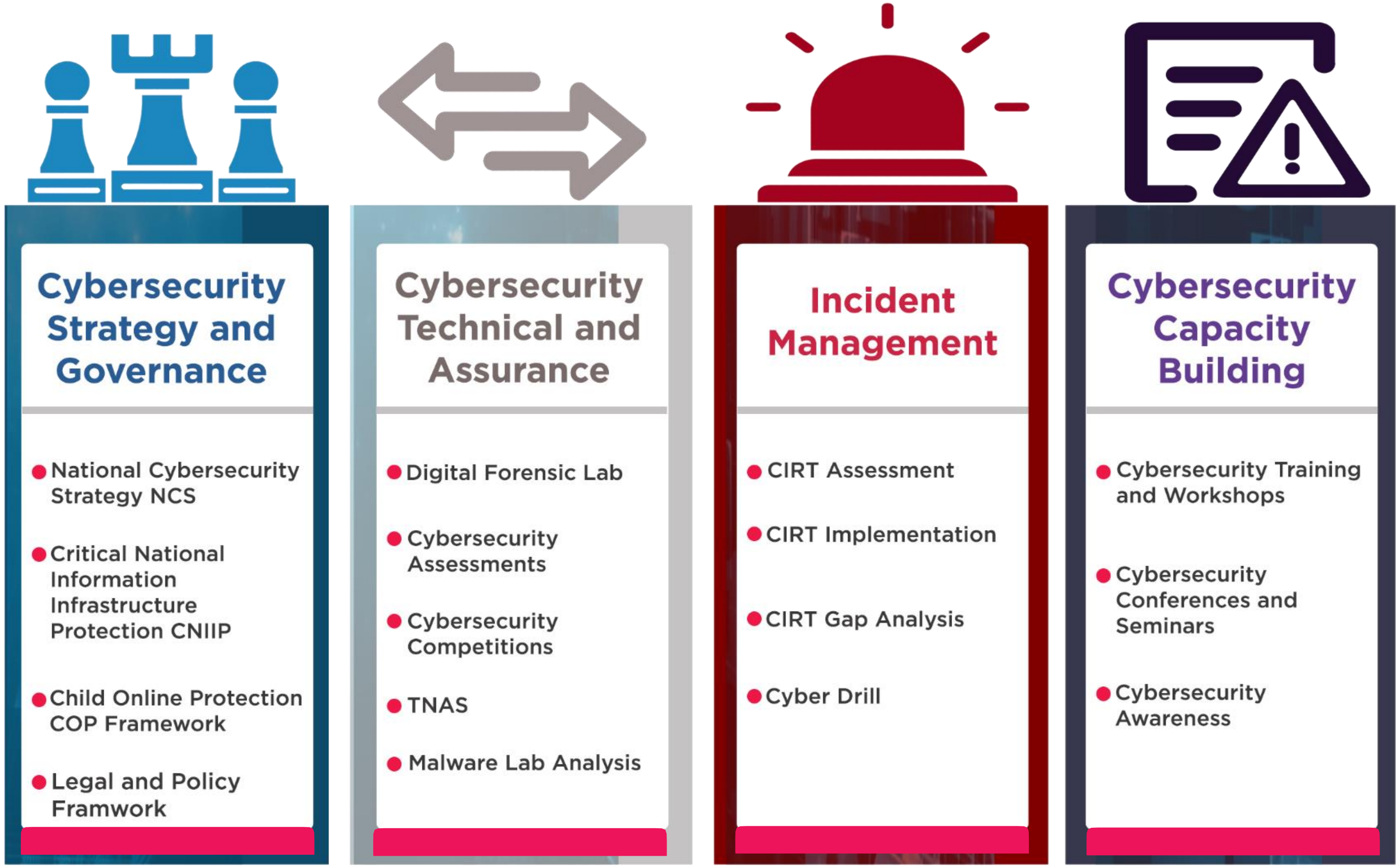
ITU - ARAB REGIONAL CYBERSECURITY CENTER

ITU Arab Regional Cybersecurity Center

Service Catalogue

Service Catalogue Diagram

ITU-ARCC services offer a variety of cybersecurity services to meet the difficult challenges of fighting cyber threats and to support the center's aim. These services align and agree with ITU Global Cybersecurity Agenda (GCA), which intends to enhance the confidence and security in the information society. The GCA was launched on 17 May 2007 for international cooperation and strategies to improve cybersecurity posture in global. ITU-ARCC provides the following services:



Cybersecurity Strategy and Governance

- National Cybersecurity Strategy NCS
- Critical National Information Infrastructure Protection CNIIP
- Child Online Protection COP Framework
- Legal and Policy Framwork

Cybersecurity Technical and Assurance

- Digital Forensic Lab
- Cybersecurity Assessments
- Cybersecurity Competitions
- TNAS
- Malware Lab Analysis

Incident Management

- CIRT Assessment
- CIRT Implementation
- CIRT Gap Analysis
- Cyber Drill

Cybersecurity Capacity Building

- Cybersecurity Training and Workshops
- Cybersecurity Conferences and Seminars
- Cybersecurity Awareness

Cybersecurity Strategy and Governance

Cybersecurity Strategy and Governance

ITU-ARCC experts work closely with governments and public sectors to develop national cybersecurity strategies with clear accountabilities and responsibilities. The cybersecurity strategy includes robust programs to enhance the cybersecurity capabilities and to fill the gaps in the cybersecurity environment.

National Cybersecurity Strategy (NCS)

legal and Policy Framework

Child Online Protection (COP) Framework

Critical National Information Infrastructure Protection (CNIIP)

National Cybersecurity Strategy (NCS)

Introduction

ITU-ARCC experts in close cooperation with governments and public sectors will develop a national framework to drive the adoption of a national cybersecurity strategy. The cybersecurity strategy includes robust programs to enhance the cybersecurity capabilities and to fill the gaps in the cybersecurity environment.

Objectives

The main objectives of a national cybersecurity strategy are to:

- Study and analyze the country's current cybersecurity status, needs and risk management methodologies.
- Study institutional and organizational requirements, and arrangements for developing a comprehensive National Cybersecurity Strategy.
- Provide high-level recommendations to improve the cybersecurity posture of the country in order for the implementation of the NCS.
- Conduct training to impart the necessary knowledge on key concepts surrounding National Cybersecurity such as its development and production, as well as its implementation and long-term sustainability

Deliverables

National Cybersecurity Strategy workshop. High-level report shows the key findings recommendations of the way forward for the establishment or enhancing of National Cybersecurity Strategy.

Critical National Information Infrastructure Protection (CNIIP)

Introduction

Succeeding in the government sector is as important as succeeding in the Critical National Infrastructure as their prosperous would robust the national economy similar to their incapacitation or destruction would have a debilitating effect to the national economy.
ITU-ARCC experts extends its services and work closely with the Critical Information Infrastructure department to help secure, enhance and strengthening the regional cybersecurity capabilities by developing and assisting the organizational model of the CIIP sectors, policy, process and procedures related to CNIIP.

Objectives

The main objectives of the CNII protection framework are to:

- Assess the country’s current critical IT/OT infrastructure on the national as well as sectorial level.
- Study and evaluate the current, processes, organizational bodies and other establishments, if any put in place as the national cybersecurity framework.
- Address the immediate concerns by carrying out a gap analysis with each identified critical sector and how best they can contribute in CNIIP plan.
- Assess the need to establish a centralized platform, which address the risk for the critical information infrastructure of the country at a national level.

Deliverables

A comprehensive report showing the key findings and recommendations.

Child Online Protection (COP) Framework

Introduction

Child Online Protection (COP) is an initiative, which is established by International Telecommunication Union (ITU) in 2008 as a multi-stakeholder effort within the Global Cybersecurity Agenda (GCA) framework. COP is an international collaborative network to protect children worldwide against cyber threats by providing legal, technical & procedural, organizational, capacity Building, and international cooperation measures.

Objectives

The main objectives of COP are as follows:

- Identification of risks and vulnerabilities to children in cyberspace.

- Creation of awareness among policymaker industry, parents and educators as well as the children.

- Development of practical tools to help minimize risk.

- Sharing knowledge and experience to establish safe cyber space.

Deliverables

COP framework providing a global platform for national or regional contexts on protection of children online.

Legal and Policy Framework

Introduction

An integral component of any national Cybersecurity strategy is the adoption of appropriate legislation against the misuse of ICTs for criminal purposes – which is harmonized with regional and international policy and practices. To help ensure a safe, secure and equitable internet – and combat cybercrime – ITU-ARCC is assisting ITU Member States in implementing appropriate cybersecurity legislation and harmonizing the legal and policy framework.

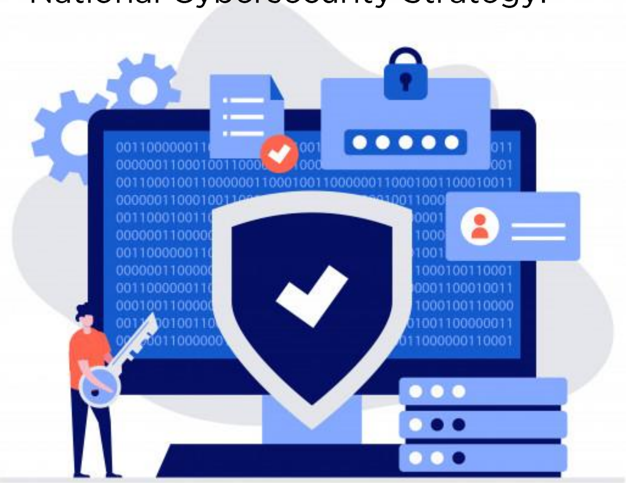
Objectives

The main objective of legal and policy framework is to assess the following concern areas and benchmarks country's legal initiatives against international best practices.

- Legal Measures and response
- Cybercrime and restrictions to the use of certain technology
- Data protection and Intellectual property
- Digital investigations and electronic evidence
- Electronica services and signatures

Deliverables

National Cybersecurity Strategy workshop. High-level report shows the key findings recommendations of the way forward for the establishment or enhancing of National Cybersecurity Strategy.



Cybersecurity Technical and Assurance

Cybersecurity Technical and Assurance

Cybersecurity Technical and assurance services aim to offer cybersecurity Technical and compliance measures. ITU-ARCC experts use the best of technical benchmarks and international standards such as ISO 27001 to support ITU member states for determining areas for enhancement.

- Digital Forensic Lab
- Cybersecurity Assessments
- TNAS
- Cybersecurity Competitions
- Malware Lab Analysis

Digital Forensics Lab

Introduction

Computer forensics can be defined as the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law.

Objectives

The main objectives are to:

- Facilitate the deployment of a Digital Forensic Centre (DFC).
- Equip the CIRT with digital forensic capability.
- Improve services the national CIRT offers to its constituents on identification, prevention, response and resolution of cybersecurity incidents.

Deliverables

Development of documentation for digital forensic, Installation of Hardware and solution, Digital forensic training

Cybersecurity Assessment

Introduction

The overall aim of cybersecurity assessment is reviewing and evaluating the level of risk associate with an application in terms of its cyber vulnerabilities and the potential disclosure of sensitive information for the country infrastructure. ITU-ARCC experts follows an appropriate and comprehensive methodology when conducting a cybersecurity assessment. The assessment conducted under controlled environment to ensure the availability of country production systems is not impacted during the testing.

Objectives

The main objectives of the cybersecurity assessment are to:

- Perform cybersecurity assessment review for the constituency
- Identify the vulnerabilities in the country's existing ICT infrastructure and applications.
- Evaluate the effectiveness of existing security controls in protecting the ICT infrastructure against attack;
- Provide remediation or mitigation plan of the identified risks to minimize country's ICT infrastructure risk exposure, which will improve the overall security posture.

Deliverables

Cybersecurity Assessment Report, which include key findings and recommendations.

Cybersecurity Competitions

Introduction

These exercises are offering technical participants with a chance to elevate their skills to different level by conducting ethical hacking activities against cybersecurity competitions. The aim is to allow the National advanced Cyber Threat team to carry out an urgent vulnerability assessment or pen testing for online services infrastructure to identify the existing vulnerabilities and to suggest critical remediation to reduce the overall risk exposure.

Objectives

The main objectives of the cybersecurity competitions are to:

- Practice real life ethical hacking experience for the talented participants.
- Allow organization to discover the issues and vulnerabilities in their environments.
- Encourage the teamwork and knowledge transfer between the experts.

Deliverables

Trainings, Advisories about threats and vulnerabilities.

Threats and Notifications Alert Service (TNAS)

Introduction

ITU-ARCC through Oman national CERT provide this service to disseminate information that describes an intruder attack, security vulnerability, intrusion alert, computer virus, or hoax, and providing any short-term recommended course of action for dealing with the resulting problem.

The Threats and Notifications Alert Service is sent as a reaction to the current problem to notify constituents of the activity and to provide guidance for protecting their systems or recovering any systems that were affected.

Objectives

Disseminate timely information regarding imminent threats and vulnerabilities.

Deliverables

Email alerts, with detailed information on threats and vulnerabilities

Malware Lab Analysis

Introduction

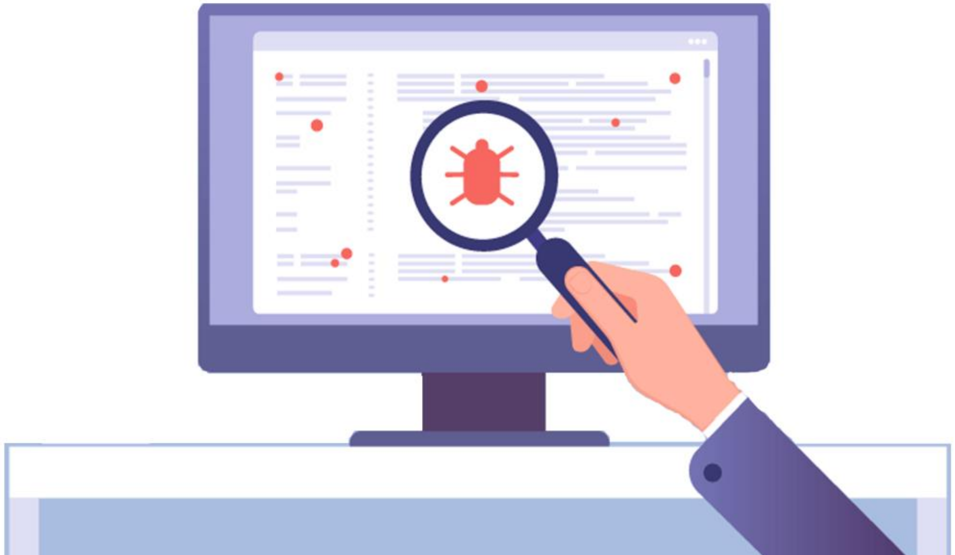
ITU-ARCC through Qatar national CERT provide analysis of binary files to identify potential threats or evidence of harmful content. Such binary files may be collected as evidence and submitted for analysis.These may be recovered from exploits involving cyber attacks, corporate espionage or compromise of information infrastructure.

Objectives

The main objective is to collect and analyze of cyber threats to determine the effect of such threats to the nation.

Deliverables

A comprehensive report showing the effect of the binary file on the infected information assets and resources.



Incident Management

Incident Management

ITU-ARCC work team with their partners to assist and encourage ITU member states to establish its national CIRT (Computer Incident Response Team) with nationwide responsibility and to serve as a trusted, central coordination point of contact for cybersecurity. In addition, the computer incident response service is designed to assess governments and public sectors CIRTs capabilities to identify the gaps and propose roadmap to improve their CIRTs.

- CIRT Assessment
- CIRT Implemetation
- CIRT Gap Analysis
- Cyber Drill

CIRT Assessment

Introduction

The primary aim of this service are to assist the identified countries in the assessment of its readiness to implement a national CIRT (Computer Incident Response Team). The national CIRT will provide a capability to identify, respond and manage cyber threats and at the same time will enhance the cybersecurity posture of the sovereign country.

Objectives

The main objectives of the CIRT Assessment are to:

- Study and analyze the countries' current cybersecurity status and needs.

- Provide high-level recommendations to improve the cybersecurity posture of the countries.

- Study and suggest institutional and organizational requirements, and arrangements for setting-up National CIRTs.

- Conduct trainings for human capacity building to impart knowledge and skills for operation, maintenance and coordination of CIRTs with relevant agencies, both local and international.

Deliverables

CIRT readiness assessment report contain the current country risk exposure and recommendations.

CIRT Implementation

Introduction

CIRT Implementation service is to assist governments in establishing and further developing Cybersecurity capabilities including the establishment of a Computer Incident Response Team (CIRT) with national responsibility in 3 phases. The overall vision is to facilitate the process towards a global Cybersecurity strategy for the country. The national CIRT will serve as a trusted and central coordination point of contact for cybersecurity aimed at identifying, defending, responding to, and managing cyber threats

Objectives

The main objectives are to:
• Create a functioning national CIRT, able to provide its constituents with a basic set of services.

• Build human capacity in the field of cybersecurity and train government on CIRT operation and incident response.
• Improve the national preparedness on the identification, prevention, response and resolution of cybersecurity incidents at identified constituents of the CIRT.
• Ensure the utilization and operation of the CIRT by building an effective and efficient capable CIRT that is ready to respond to cyber threats
• Implement, review and test day-to-day operations on processes, workflow developed, and CIRTs tools

Deliverables

CIRT design document and implementation plan, SOPs, Operating manuals, Training material, Tools

CIRT Gap Analysis

Introduction

The main aim of CIRT gap Analysis is to study and evaluate the readiness of the current CIRT Structure for government CIRT with its capabilities and ensure computer incidents, intrusion attempts, and emergencies are appropriately managed to levels consistent with industry standards and good business practices. This is based on a finite set of current conditions, a limited set of key drivers used to estimate the current CIRT health relative to a defined benchmark. Decision-makers can then determine if the current state of the CIRT is acceptable, or if actions are required to improve the situation.

Objectives

The main objectives for CIRT Gap Analysis are to :

- Study all current policies, procedures, and forms developed for computer incident, intrusion, or emergency response process.
- Review the risk assessment process employed to determine the computer incident, intrusion and/or emergency response processes.
- Evaluate the tools designed and used to prevent and detect computer incidents or intrusions.
- Provide a comprehensive recommendation report to tackle the current gaps if any based on the best practices.

Deliverables

CIRT Gap reports include all the shortcomings and recommendations to overcome these gaps.

Cyber Drills Exercises

Introduction

Cyber Drill is conducted to expose the participants from the national Computer Emergency Response Teams (CERTs) to various scenarios based on case studies and real-life situations, which provides them with an opportunity to test their skills and knowledge in responding to such attacks. The Cyber Drill will be preceded by a workshop covers a variety of notable topics in addressing computer emergency response matters.

Objectives

The main objective of this Cyber Drill is to enhance communication, teamwork, and participating teams' incident response capabilities to ensure continued collective efforts against cyber threats through the CIRT of the region.

Deliverables

Cyber drill simulation and participation report for the organizations.

Cybersecurity Capacity Building

Cybersecurity Capacity Building

The cybersecurity capacity building can help constituencies to build institutional cybersecurity capabilities and to develop programmatic and effective culture solutions. In addition, this service will raise awareness campaigns in the community, forums and at national level and providing cybersecurity training and development programs.

Cybersecurity Trainings and Workshops

Cybersecurity Conferences and Seminars

Cybersecurity Awareness

Cybersecurity Training and Workshops

Introduction

The cybersecurity capacity building can help countries to build institutional cybersecurity capabilities and to develop programmatic and effective culture solutions. ITU-ARCC provide a specific courses/workshops with customized content related to cybersecurity area according to the request of the partners or later after identifying the skills gap in the any field of information security.

Objectives

The main objective is to organize professional trainings or workshop to overcome current and future challenges in the field of cybersecurity through case studies and success stories that show how organizations successfully overcome cyber-attacks.

Deliverables

Specialized and customized courses, Workshops

Cybersecurity Conferences and Seminars

Introduction

ITU-ARCC is organizing national, regional, and international conferences or seminars that will focus on general topics of cybersecurity trends and measures.

As the country constituents, stakeholders and individual will be present; conferences or seminars will serve the country as an effective motivator to tackle the current tentative and create a clear and transparent channel of communication to initiate cooperation and integration in order to build a national cybersecurity structure.

Objectives

The main objectives of the Cybersecurity conference and seminars is to provide insight into setting up, maintaining and improving information security, protection against hybrid threats at the national/regional/international level, through information and education on ways to minimizing risks and alleviating the consequences of cyberattacks.

Deliverables

Summits, Conferences, Seminars, Forums.

Cybersecurity Awareness

Introduction

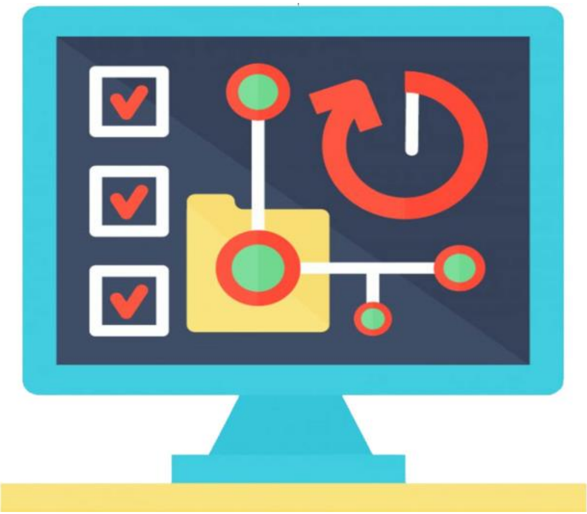
Any person working in a technology driven environment must be exposed to the threats faced by these environments from the perspective of regular intended use.
To make the most of technology, users must be empowered with knowledge of secure practices and methods to minimize the risks associated with their use.

Objectives

Help technology users to understand the fundamentals of information security, threats associated with use of information or communication technology and secure practices to minimize occurrence of incidents.

Deliverables

Awareness sessions, campaigns, challenges.



www.arcc.om

iturcc

ITU-ARCC

ITUARCC