Capacity building Republic of Moldova

Eugeniu CROITOROV
06.10.2022, Telč, Czech Republic

STISC – INFORMATION TECHNOLOGY AND CYBERSECURITY SERVICE

ITSEC - Public institution

Website: www.stisc.gov.md

Created: 2018

Mission: Ensuring administration, maintenance and development of the information technology infrastructure, government's Public key infrastructure, implementing state policy in the field of cyber security

Main fields of activity

Telecommunication system of public administration authorities

MCloud

Government PKI infrastructure

Administration of state Information Systems

National registrar of the ".md" superior level domain

Cyber Security

STISC – INFORMATION TECHNOLOGY AND CYBERSECURITY SERVICE

ISO 27001

FIRST
Improving Security Together

CERTIFICATE OF MEMBERSHIP

FIRST.Org, Inc. certifies that

Cyber Security Center CERT-GOV-MD

Is a FIRST Member in good standing for **2022**.

Alexander Jaeger
Chair, FIRST.Org, Inc.

ACCREDITED BY TRUSTED INTRODUCER

2020:

➤ **STISC – appointed as** Government response center to cyber security incidents **(CERT-GOV)**
➤ Single point of contact and reporting of cybersecurity incidents
➤ Implementor of State Register for cyber security incidents

Main responsibilities:

☐ Policy implementation for prevention and counteraction of cyber incidents;
☐ Organizational and technical framework for information sharing among CERT teams, entities and users;
☐ Identification, registration, classification and analysis of cyber incidents;
☐ Consultancy and support in prevention and response
☐ Awareness events raising understanding of threats, vulnerabilities and reported or identified incidents;
☐ Capacity building via trainings, exercises and workshops for enhancing reaction capabilities to cyber incidents;
☐ Interagency cooperation

Framework

2017 - Law nr. 299 – Information Security Concept of Republic of Moldova

2018 - Government Decision nr. 257 – Information Security Strategy 2019-2024

2018 – Action plan for Strategy implementation

Information security Strategy 2019-2024

Pillar I:

Security of cyber informational space

Pillar II:

Security of media information space

Pillar III:

Enhancing of operational capabilities

Pillar IV:

Process optimization, coordination and international cooperation
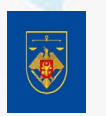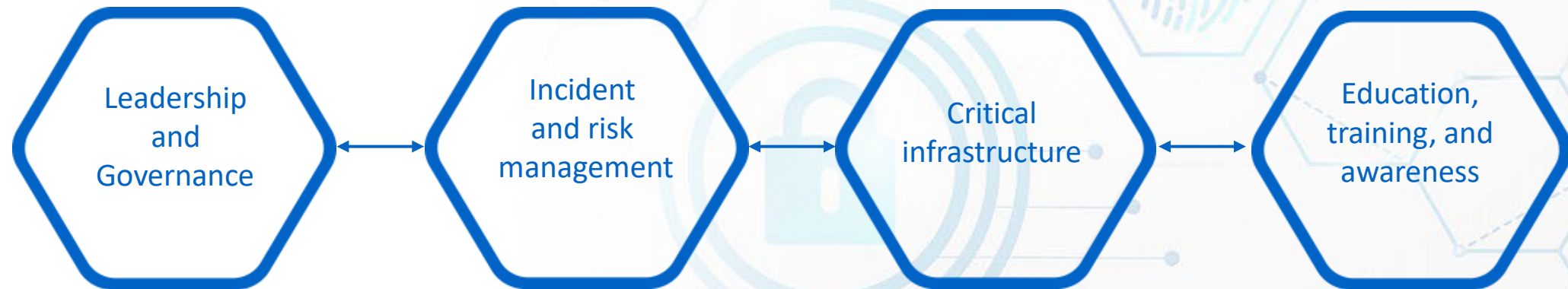
SIS   STISC   AGE   MIDR / ME   MA   MAI   PG   CNPDCP

Current initiatives

- Increasing cyber resilience of public sector organizations and key critical infrastructure sectors
- Develop and implement a new Cybersecurity Framework based on best practices and international experience
- Align to EU cybersecurity framework and NIS Directive

Areas to cover

Leadership and Governance ↔ Incident and risk management ↔ Critical infrastructure ↔ Education, training, and awareness

Capacity building – Education, training and awareness raising

Perform awareness raising events

Perform cybersecurity professionals training both for public and private sectors

Develop self learning tools

Thank you

www.stisc.gov.md