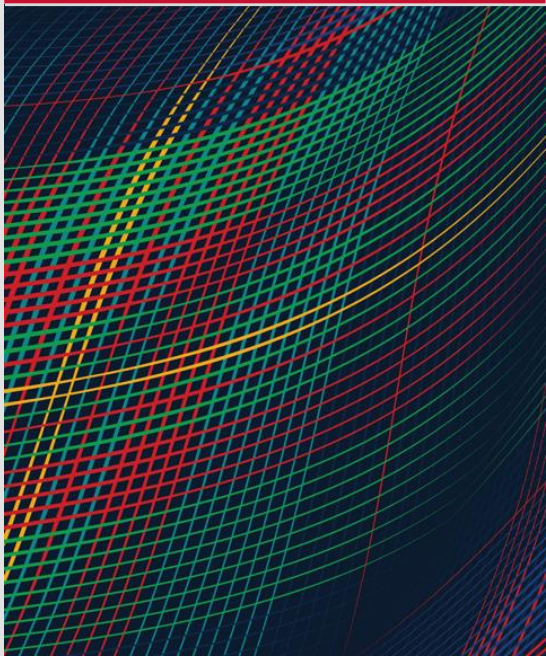
Carnegie Mellon University
Software Engineering Institute



Module 1: Introduction to Planning and Implementing a National/Government CSIRT

Planning and Implementing a National/Government CSIRT

Introduction

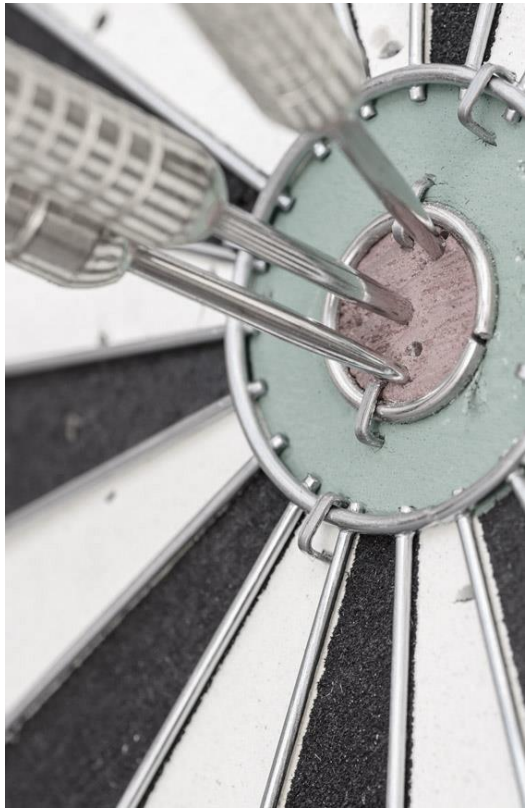
Carnegie Mellon University
Software Engineering Institute

Purpose

To help you

- understand the functions of National or Government Computer Security Incident Response Teams (CSIRTs) and the philosophy behind them
- appreciate the possible roles played by such CSIRTs
- identify some of the challenges faced by these types of CSIRTs
- appreciate the key issues and decisions that must be addressed when creating or operating a National or Government CSIRT

Course Goals



Discuss the unique role of a National or Government CSIRT.

Review the components of a CSIRT in general.

Identify enablers and supporting resources for establishing a National or Government CSIRT.

Characterize Stakeholders for National and Government CSIRTs.

Identify needed collaboration, coordination, and information sharing initiatives and activities.

Discuss planning decisions and strategies.

Identify implementation strategies.

Review methods for evaluating National and Government CSIRTs and implementing resulting process improvements.

Intended Audience

Individuals tasked with creating a National or Government CSIRT or incident management capability

Other individuals who need or would like an understanding of general CSIRT and specifically National CSIRT issues and processes

Individuals interested in learning more about CSIRTs, National CSIRTs, and incident management activities in general

Agenda -1

Module 1:	Introduction to Planning and Implementing a National/Government CSIRT
Module 2:	National Incident Management Ecosystem
Module 3:	Defining Incident Management (IM)
Module 4:	The Evolving Nature of Incident Management Capabilities
Module 5:	Defining CSIRTs
Module 6:	Uniqueness of a National or Government CSIRT
Module 7:	National CSIRT Principles
Module 8:	Connection with Critical Infrastructures
Module 9:	Planning a National or Government CSIRT: Building Your Strategy
Module 10:	Planning a National or Government CSIRT: Best Practices
Module 11:	Planning a National or Government CSIRT: Key Decisions
Module 12:	Implementing Your National or Government CSIRT

Agenda -2

Module 13:	Implementing Your National or Government CSIRT: Roles and Responsibilities
Module 14:	Implementing Your National or Government CSIRT: Incident Criteria and Incidents of National Importance
Module 15:	Implementing Your National or Government CSIRT: Incident Reporting Requirements
Module 16:	Implementing Your National or Government CSIRT: Policies and Procedures
Module 17:	Implementing Your National or Government CSIRT: Challenges
Module 18:	Implementing Your National or Government CSIRT: Politics and Policies
Module 19:	Implementing Your National or Government CSIRT: Branding
Module 20:	Implementing Your National or Government CSIRT: Information Sharing
Module 21:	Process Improvement and Sustainment
Module 22:	Summary
Module 23:	Resources

Applying Course Materials

Each organization is different.

Refer to your own country, economy, or government rules, regulations, laws, and policies.

Refer and align with your parent organization incident management policies, procedures, and processes for

- established roles and responsibilities
- approved workflows
- appropriate responses and response times
- prioritization and escalation criteria

No Single Recipe

There is no single recipe for creating a CSIRT.

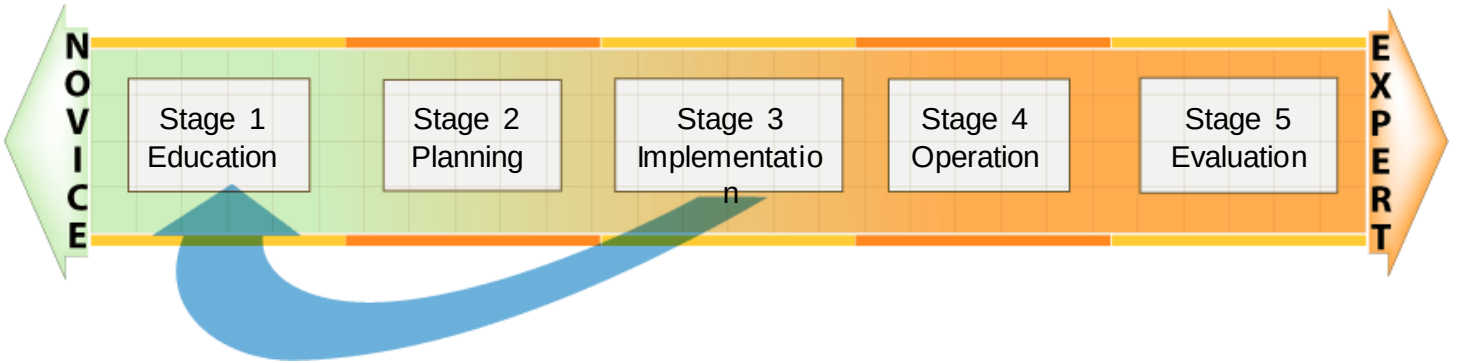
It depends on your

- needs and requirements
- mission and goals
- available resources and support

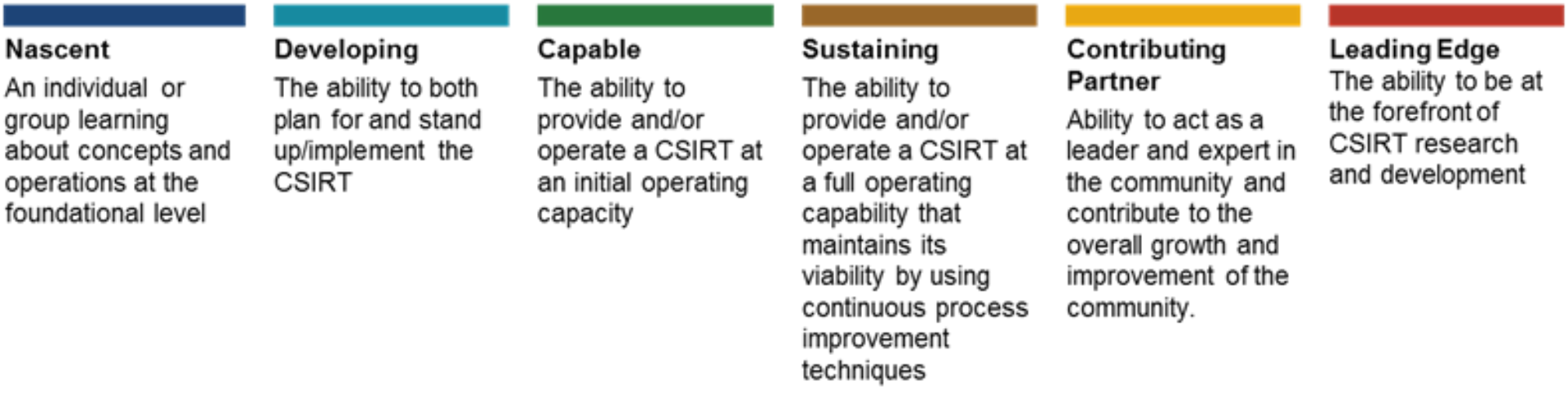
Stages of CSIRT Development

Carnegie Mellon University Software Engineering Institute

Stage 1 Educating the organization
Stage 2 Planning effort
Stage 3 Initial implementation
Stage 4 Operational phase
Stage 5 Evaluation and improvement



CSIRT Development Continuum



Some Definitions

Carnegie Mellon University Software Engineering Institute

Term	Definition
CSIRT	• Computer Security Incident Response Team or capability • an organization or capability that provides services and support, to a defined constituency, for preventing, handling, and responding to computer security incidents
National CSIRT	• CSIRT with National responsibility • designated to have specific responsibilities in cybersecurity protection for a country or economy
Government CSIRT	• can be a CSIRT responsible for cybersecurity strategies and protection for government ministries or departments or a national CSIRT or perform the role of both
Constituency	• organization or individuals being served by the CSIRT
Stakeholder	• internal or external organizations or individuals who are interested in, support, or partner with the CSIRT

Questions and Discussion