

CERT: to do list

- 1. Identify Stakeholders and participants**
- 2. Obtain management support and sponsorship**
- 3. Develop a CERT project plan**
- 4. Gather Information**
- 5. Identify the CERT Constituency**
- 6. Defined the CERT mission**
- 7. Secure funding for CERT operations**
- 8. Decide on the range and level of services the CERT will offer**
- 9. Determine the CERT reporting structure, authority and organizational model**

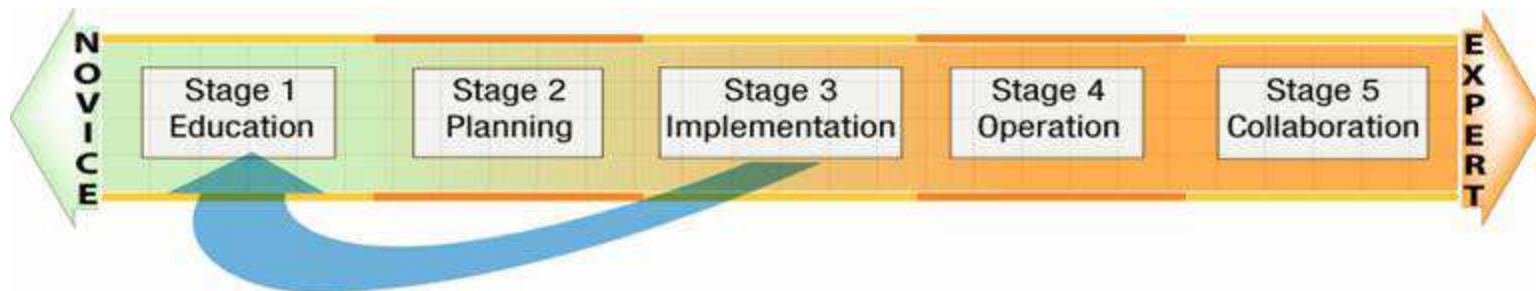
- 10. Identify required resources such as staff equipment and infrastructure**
- 11. Define interaction and interfaces**
- 12. Define roles responsibilities and the corresponding authority**
- 13. Document the workflow**
- 14. Develop policies and corresponding procedures**
- 15. Create and implementation plan and solicit feedback**
- 16. Announce the CERT when it becomes operational**
- 17. Define methods for evaluating the performance of the CERT**

18. Have a backup plan for every element of the CERT

19. BE FLEXIBLE

Stages for Creating a National CSIRT

- Stage 1 – Educating stakeholders about the development of a national team
- Stage 2 – Planning the CSIRT
- Stage 3 – Implementing the CSIRT
- Stage 4 – Operating the CSIRT
- Stage 5 – Collaboration



Timeline

Depending on the resources that are provided and “buy-in” from its key stakeholders and constituency, a CSIRT can take anywhere from 18-24 months to become fully operational (see the projected timeline below). This timeline can be extended or compressed, depending on a number of factors and decision points that are made. These are indicated at the bottom of the picture.

Awareness/Education

Planning

0-5 months

Implementation

9 months

6 months

Operations

+3



Course of Action - Decision points to be considered:

1. mission/vision
2. constituency
3. scope
4. authority
5. services (interaction/levels/structure)
6. external interactions
7. terminology (incidents, types, categories)