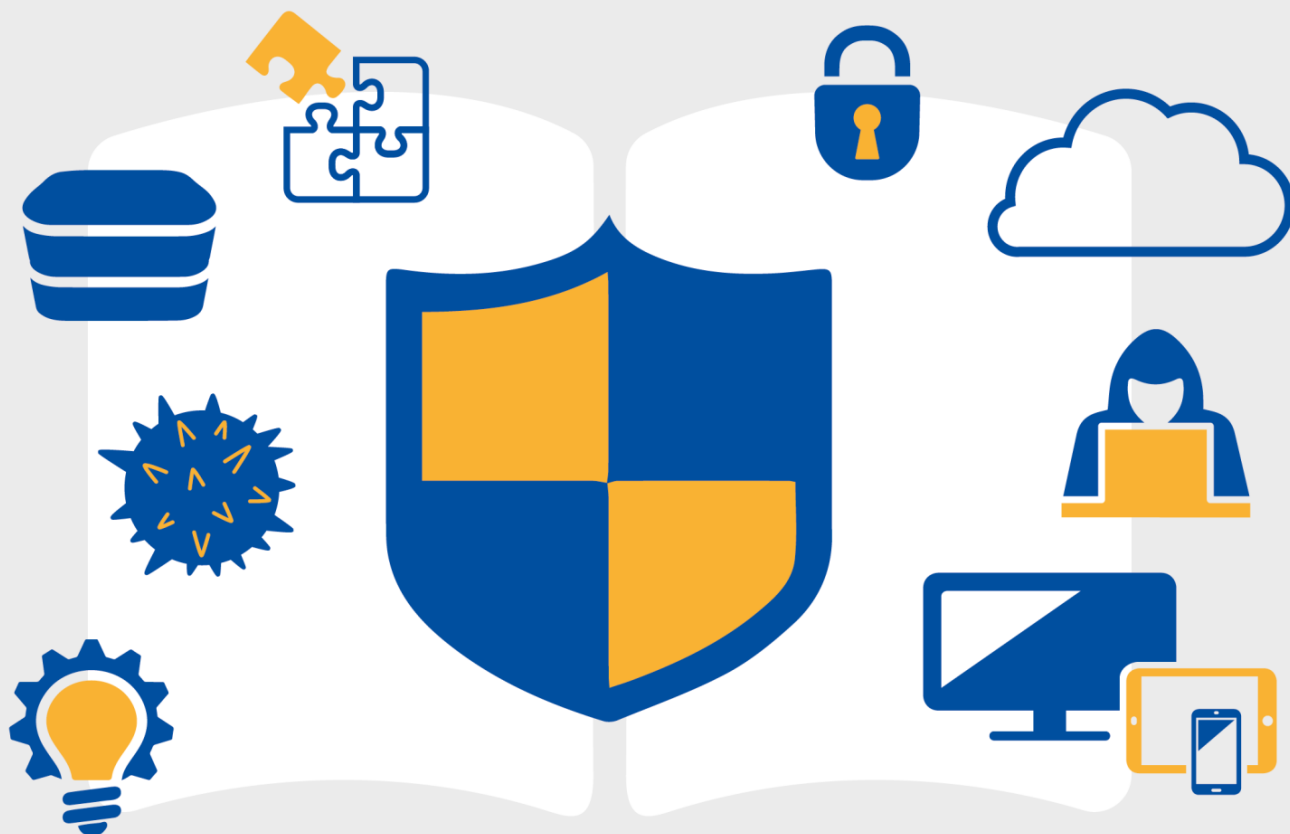




HOW TO SETUP UP CSIRT AND SOC

GOOD PRACTICE GUIDE

DECEMBER 2020

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

CONTACT

For queries in relation to this study, please use: csirt-relations@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

Edgars Taurins, ENISA.
Activities supporting this study were conducted under contract with NRD Cyber Security.

ACKNOWLEDGEMENTS

Study was performed with the input from Informal Expert Group on EU Member States Incident Response Development.

LEGAL NOTICE

Notice must be taken that this publication represents the views and interpretations of ENISA unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 2019/881.
This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright notice

© European Union Agency for Cybersecurity (ENISA), 2020
Reproduction is authorised provided the source is acknowledged.

For any use or reproduction of photos or other material that is not under the ENISA copyright, permission must be sought directly from the copyright holders.

ISBN 978-92-9204-410-7 - DOI 10.2824/056764



TABLE OF CONTENTS

1. INTRODUCTION	5
1.1 CONTEXT OF THE WORK	5
1.2 OBJECTIVES OF THE WORK	5
1.3 OVERVIEW OF THE METHODOLOGY	6
1.4 DEFINITIONS OF CSIRT AND SOC	6
1.4.1 Computer security incident response teams	6
1.4.2 Security operations centres	7
1.5 PREVIOUS ENISA WORK ON THE TOPIC OF CSIRTS	9
2. GUIDELINES FOR ESTABLISHING CSIRTS	10
2.1 ORGANIZATION OF THE GUIDELINES	10
2.2 ASSESSMENT FOR READINESS	13
2.2.1 Preliminary mandate	14
2.2.2 Governance structure	16
2.2.3 Identification of the CSIRT hosting organisation	16
2.2.4 High-level roadmap and budget	16
2.2.5 Detailed requirements for the design stage	18
2.3 DESIGN	19
2.3.1 Approved detailed mandate	19
2.3.2 CSIRT services plan	20
2.3.3 CSIRT processes and workflows plan	21
2.3.4 CSIRT organisation, skills and training structure plan	26
2.3.5 CSIRT facilities plan	31
2.3.6 CSIRT technologies and processes automation plan	32
2.3.7 CSIRT cooperation plan	33
2.3.8 CSIRT IT and information security management plan	34
2.3.9 Detailed requirements for the implementation stage	34
2.4 IMPLEMENTATION	34
2.4.1 Approval and implementation of the organisational structure	34
2.4.2 Hiring and appointing of staff	35
2.4.3 Execution of a training plan for different staff roles	35
2.4.4 Preparation of facilities	35
2.4.5 Development and implementation of detailed processes and procedures	35
2.4.6 Implementation of technology for the automation of processes	35
2.4.7 Implementation of IT and information security management procedures	35
2.4.8 Training of staff for CSIRT operations	36



2.4.9	Signing of relevant agreements with the constituency, stakeholders and partners	36
2.4.10	Test run of CSIRT services and tuning of results	36
2.4.11	Launch of CSIRT communications and celebrations	36
2.5	OPERATIONS	37
2.5.1	Measurement of key performance indicators	37
2.5.2	Annual operations performance review	38
2.5.3	Annual stakeholder needs review	38
2.5.4	Approval of the annual budget	38
2.5.5	Collection of improvement initiatives	38
2.6	IMPROVEMENT	38
2.6.1	List of improvement initiatives	38
2.6.2	Detailed plans for improvement initiatives for the design stage	40
2.6.3	Preliminary budget for improvement initiatives	40
3.	CONCLUSIONS	41
4.	GLOSSARY AND ACRONYMS	42
5.	BIBLIOGRAPHY	43
A	ANNEX: QUESTIONNAIRE	44
6. B	ANNEX: METHODOLOGY MAPPING	48

EXECUTIVE SUMMARY

This publication provides results-driven guidance for those who are interested in establishing a computer security incident response team (CSIRT) or security operations centre (SOC), and guidance on possible improvements for different types of CSIRTs and SOCs that exist currently.

The content of this report is based on an analysis of current publications on the establishment of CSIRTs (the analysis is summarised in Annex B); a field questionnaire (Annex A), which was completed by 40 CSIRTs and SOCs; and the authors' experiences in establishing and improving CSIRTs as part of numerous projects carried out in Europe, Asia, Africa and South America.

A results-driven approach is taken throughout the publication to provide guidance on the different stages involved in the establishment of a CSIRT or SOC organisation:

- Assessment for readiness
- Design
- Implementation
- Operations
- Improvement.

The reader will receive practical guidance on what to focus on during the individual phases of establishment and improvement.

Up to July 2020, ENISA had published 61 reports and 21 translated versions of reports supporting CSIRTs on its website ⁽¹⁾. ENISA's training package ⁽²⁾ provides online training materials, training courses and exercise materials for cybersecurity specialists, based on the 'Train the Trainer' philosophy. This document aims to enhance ENISA's existing body of knowledge on the establishment of CSIRTs.

¹ <https://www.enisa.europa.eu/publications#c8=CSIRTs>

² <https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/>