VISION, GOVERNANCE STRUCTURE AND CERT ROADMAP (DELIVERABLE 1b)

v1.0 OCTOBER 2018

PREPARED BY
ANDY HUMPHRYS MSc, CISSP, CISM, CEH
SENIOR INFORMATION SECURITY CONSULTANT

Version Control

Version	Date	Comments
v0.1	*14/08/18*	*Initial Draft*
v0.5	*03/09/18*	*Draft updated and issued for initial review*
v0.7	*13/09/18*	*Draft updated and issued for secondary review*
v0.8	*28/09/18*	*Draft updated and issued for final review*
v0.9	*08/10/18*	*Final version issued for approval/sign-off*
v1.0	09/10/18	Approved at workshop 09/10/18

Document Approval

Name	Organisation/Position	Date
Peter Salloum	Crown Agents	09/10/18
Lt. Col. Khaled Youssef	ISF (ID)	09/10/18
Lt. Col. Nader Abdallah	ISF (IT)	09/10/18
Beindy Dagher	EU Delegation	

1. CONTENTS

This page has been left blank.

1. INTRODUCTION

1.1. Objective

1.1.1. The objective of this document is to provide a recommended vision, structure for information security governance and a proposed roadmap which will lead to full implementation of the CERT/CSIRT for the Lebanese Internal Security Forces (ISF).

1.2. Background

1.2.1. The Lebanese Internal Security Forces (ISF) currently has a limited co-ordinated capability to provide both proactive cyber threat intelligence and a reactive response to cyber security incidents/attacks against its infrastructure.

1.2.2. Following a request received from the Lebanese ISF in late 2017 to establish a Computer Emergency Response Team (CERT) for the ISF, Crown Agents was engaged to provide a number a deliverables relating to this requirement.

1.2.3. The second of these deliverables relates to provision of a proposed vision, governance structure and high-level roadmap for the ISF CERT Implementation.

1.2.4. This deliverable was written by the Senior Expert in Information Security, Andy Humphrys, with both co-operation and significant input from the ISF cybersecurity committee. While all members of the committee provided input, it should be noted that the ISF's point of contact for the mission (Capt. El Weter) provided significant assistance in facilitating the document review process and any requested meetings with ISF personnel.

1.2.5. When organisations/institutions are planning to implement a CERT, elements in many different areas need to be considered. Given that many CERTS have been implemented to date, both Carnegie Mellon University[1] and the First[2] organisation have provided comprehensive documents outlining frameworks and suggested best-practice to be followed. These documents will be used as a reference to provide the appropriate framework for both this and the subsequent deliverable (strategic plan for CERT implementation).

1.3. Definition

1.3.1. A computer emergency response team (CERT), also known as a computer/cyber security incident response team (CSIRT) is defined as a capability that provides information/cyber security incident response management and alert information for a defined constituency, which might be a single organisation, multiple organisations, or national populace.

1.3.2. The key responsibilities of a CERT/CSIRT are as follows:

- Initial creation and ongoing maintenance of an incident response plan
- Investigation and analysis of cyber security incidents
- Remediation of incidents
- Management of both internal and external communications both during and post-incident
- Providing post-incident technology, governance and training recommendations

[1] *https://resources.sei.cmu.edu/asset_files/WhitePaper/2004_019_001_53064.pdf*
[2] *https://www.first.org*

1.3.3. It should be noted that a CERT/CSIRT's operation is very different from that of a security operations centre (SOC), the purpose of which is to provide real-time monitoring and defence for security elements of an organisation's infrastructure.

1.3.4. However, there are some elements of crossover between these types of organisations, as shown in figure 1.

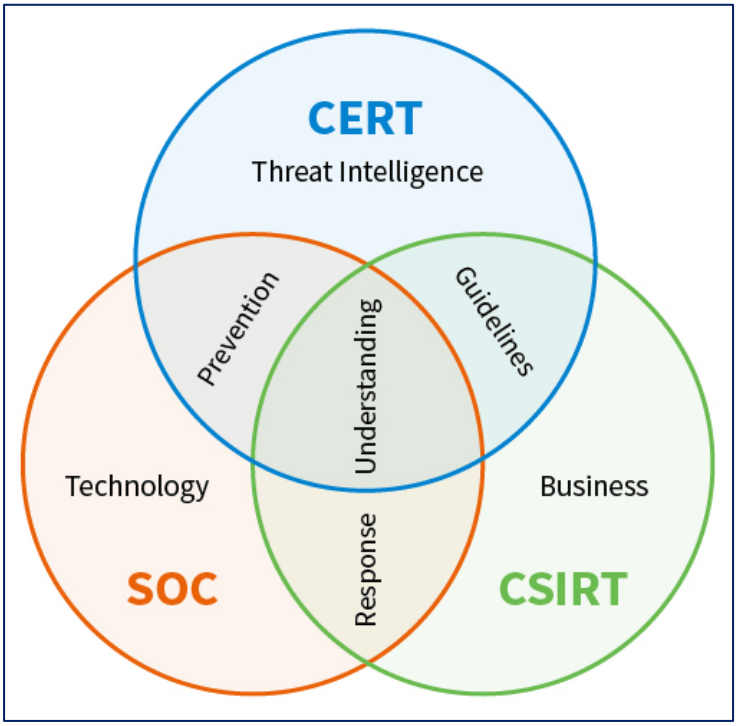


Figure 1 – The crossover functionality of SOCs, CSIRTs and CERTs. Source: Exabeam[3]

1.3.5. Given the role carried out by a SOC, it is imperative that some capability for provision of active monitoring/defensive measures can be provided in addition to the capability to respond to and manage incidents provided by a CERT/CSIRT.

1.3.6. A CERT/CSIRT is therefore a unit dedicated to guaranteeing that suitable technology and best systems management practices are utilized to counter attacks on networked environment, in addition to restricting harm and guaranteeing coherence and ongoing availability of critical services.

[3] https://www.exabeam.com

2. VISION

2.1. Overview

2.1.1. A vision statement can be described as an aspirational description of what an organisation would like to achieve. In terms of a suitable vision, it is suggested that the following statement be used:

"The ISF will provide a world-class incident response capability that will deliver valued incident prevention and detection services, and will become the trusted cybersecurity response team for the Lebanese information society".

2.1.2. When considering establishment of a CERT/CSIRT for the ISF, Carnegie Mellon University suggests that it should have four core principles, shown in figure 2:

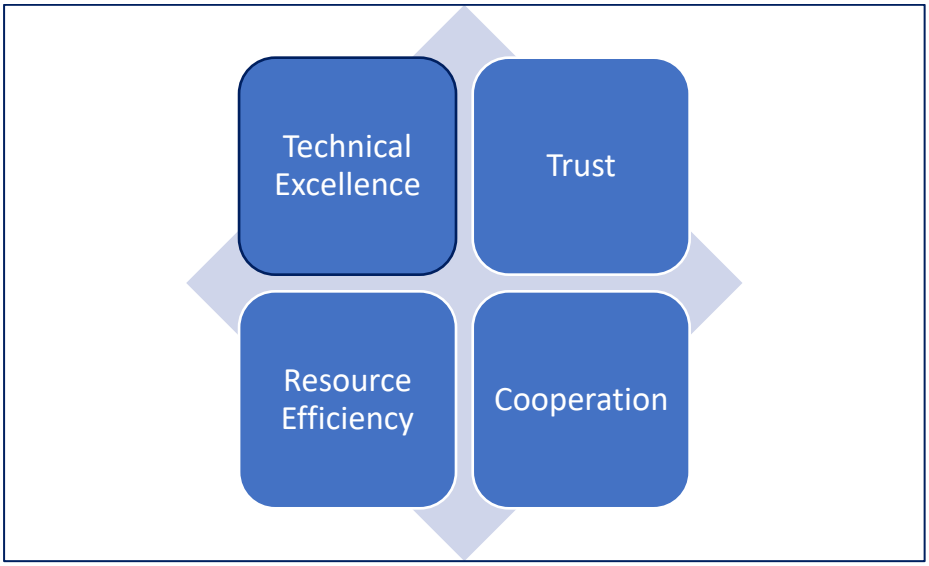


Figure 2 - The 'core principles' of a CERT. Source: Carnegie Mellon University

2.1.3. *Technical Excellence* – the planned ISF CERT/CSIRT should have up to date technical resources and must be able to provide advice supported by its own high levels of technical excellence. Given the planned phases of ISF CERT/CSIRT operation, it is likely that any initial advice provided will be in a limited number of areas, although as the CERT/CSIRT matures the scope of advice would be expected to increase.

2.1.4. *Trust* – the constituency served by the ISF's CERT/CSIRT should be able to explicitly trust it, in order to be able to both share data with it and make use of the services provided by it. As the CERT/CSIRT matures it is expected that information will be shared between it and other organisations, in both public and private sectors, so explicit trust between all parties is essential given the potentially sensitive nature of some of this information.

2.1.5. *Resource efficiency* – the ISF's CERT/CSIRT should ensure that it is constantly reviewing and analysing potential new threats to its constituency, so as to ensure that its resources are allocated accordingly to focus on areas which may potentially provide the greatest impact.

2.1.6. *Co-operation* - given the information sharing functionality discussed above, the ISF's CERT/CSIRT should maintain relationships with both its constituents,

external stakeholders (e.g. government departments) and other CERTS/CSIRT as appropriate.

2.1.7. When establishing a CERT/CSIRT vision, it is important to consider all component elements. As suggested by Carnegie Mellon University, these are shown below in figure 3:

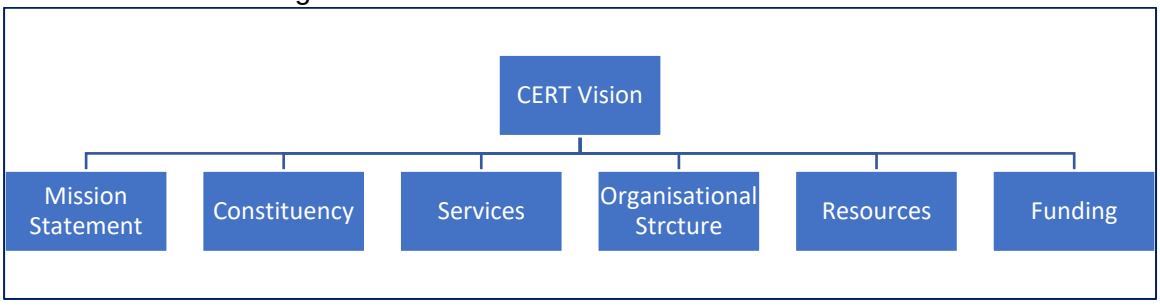


Figure 3 - Elements of a CERT vision. Source: Carnegie Mellon University

2.1.8. These elements will now be reviewed in further detail.

2.2. Mission Statement

2.2.1. A mission statement provides information relating to the overall purpose and function, together with a high-level overview of the CERT/CSIRT's objectives.

2.2.2. In terms of the proposed ISF CERT/CSIRT, a mission statement has been provided by the ISF for use, shown in figure 4:

> *The ISF CERT/CSIRT will provide a capability to detect and respond to cybersecurity incidents against ISF infrastructure, provide accurate and timely information regarding current and emerging cybersecurity threats, and promote security awareness and adoption of cybersecurity standards, together with the implementation of best-practice policies, procedures and technical tools to mitigate cybersecurity risk.*

Figure 4 - Proposed mission statement for ISF CERT/CSIRT

2.3. Constituency

2.3.1. Within the scope of CERT/CSIRT operation, a constituency is defined as those who will receive the services provided by it, which may be a single organisation, region or country.

2.3.2. In the initial phase of the ISF CERT/CSIRT operation, the defined constituency will consist of the ISF organisation i.e. all those who make internal use of the ISF's IT services.

2.3.3. As the CERT/CSIRT matures from a capability and knowledge/experience perspective, it is expected that the constituency will expand to include members of the public, and a cybersecurity-specific web portal will be created to provide a portal for both reporting of cybersecurity related incidents and for publishing alerts and cyber security advice/tips.

2.3.4. Eventually, this constituency might expand to include other Lebanese governmental and critical national infrastructure (CNI) entities within Lebanon. However, ISF's CERT/CSIRT is only planning to provide alerting and information sharing services with these other entities.

2.4. Services

2.4.1. As shown in figure 5 below, the fundamental activities of a CERT/CSIRT (as proposed by ENISA[4]) comprise of three main high-level areas, these being proactive services, reactive services and security management.

2.4.2. Within these identified areas, a number of other services exist, with the ability to provide these being limited by the CERT's technical and resource capabilities, together with the requirements of the identified constituency.

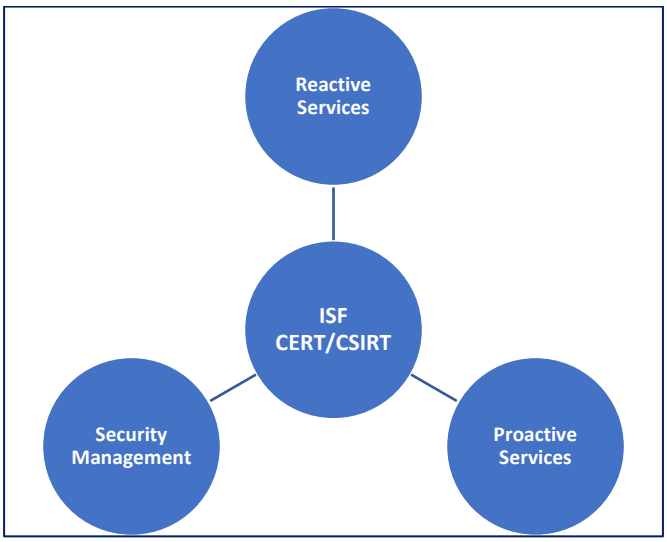


Figure 5 - Key areas of CERT/CSIRT operation. Source: ENISA

2.4.3. To provide further investigation into the detailed services that the ISF will provide to its constituents, version 1.1 of the FIRST framework[5] has been used as the main reference.

2.4.4. Unlike the ENISA model which has clear differentiation between proactive and reactive services, the FIRST framework provides a hierarchical model of top-level services areas, multiple supporting services, and subsidiary functions for each service, some of which have *both* proactive and reactive elements within them. Alongside the service areas/services/functions, the framework includes 'internal functions' referencing supporting activities within the organisation, but not necessarily part of the CERT/CSIRT organigram.

2.4.5. Figure 6 provides a graphical representation of the FIRST framework with its full-service capability suite comprising 7 main service areas.

2.4.6. It should be noted that while services in all service-areas are recommended, the level of ISF's current capabilities (technical/resource skill levels etc.) should be considered when defining which of these services can be provided to its constituency in the initial phases of CERT/CSIRT operation.

2.4.7. A summary of each service areas together with its high-level service offerings will then be provided. Further detailed information can be provided by review of the FIRST framework document[4].

[4] *European Union Agency for Network and Information Security - https://www.enisa.europa.eu/*
[5] *Forum of Incident Response and Security Teams - https://www.first.org/education/FIRST_CSIRT_Services_Framework_v1.1.pdf*

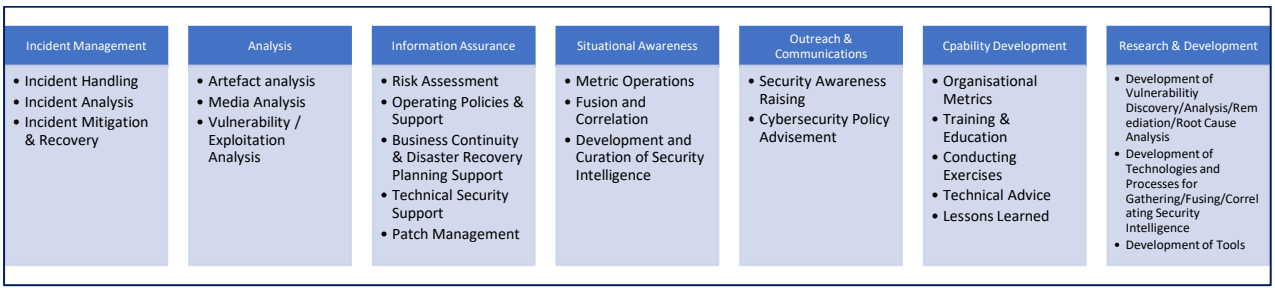


Figure 6 - The FIRST framework showing the seven main service areas. Source: FIRST

2.4.8. The first service area, 'Incident Management', is shown in figure 7. Given the commonly accepted stages of incident response, shown in figure 8, the specific activities and approach taken by the FIRST framework differ slightly from this list, albeit with the same end-result:

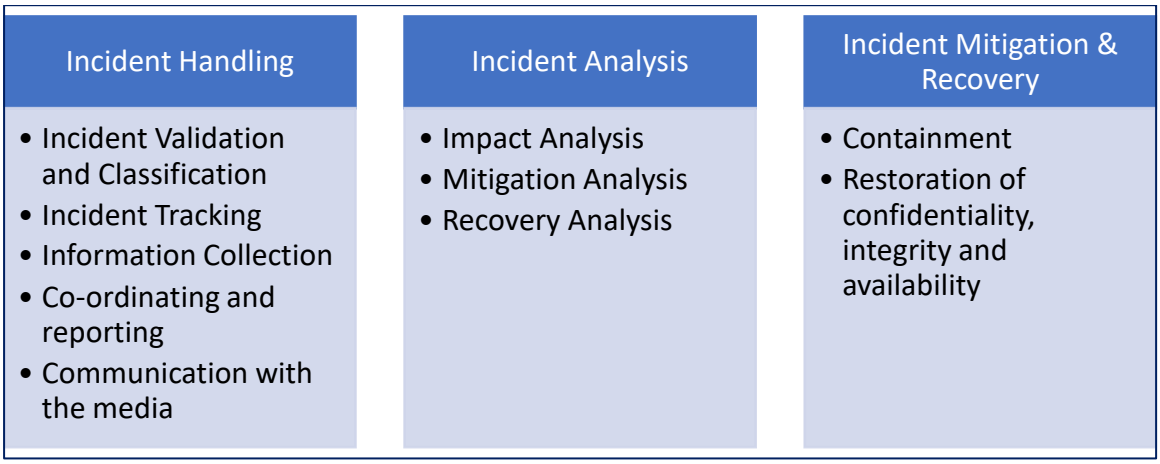


Figure 7 –The 'Incident Management' service area. Source: FIRST

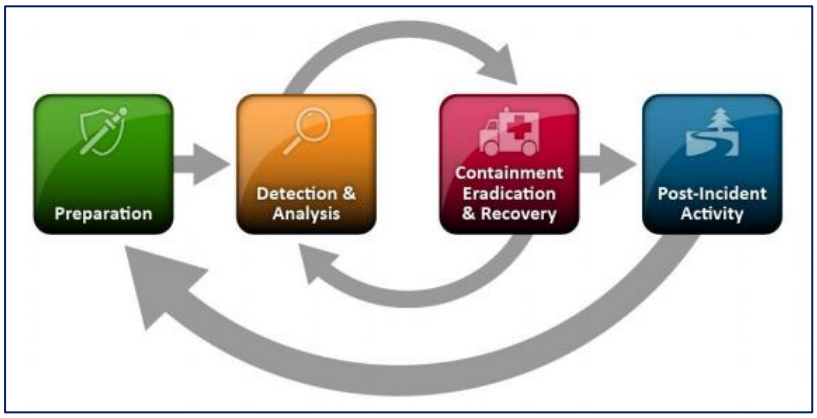


Figure 8 - The incident response life cycle. Source NIST

2.4.9. In addition to the 'technical' tasks relating to the incident management process, other 'non-technical' services such as co-ordination & reporting, together with external communication are included in the FIRST framework.

2.4.10. Depending on the nature of the incident, it may be necessary for initial incident responders to co-ordinate activities with other teams and for information/updates to be communicated to outside parties, potentially including the public. Clearly, any communications need to be managed by a team with specialist skills/experience in this area, as opposed to a purely technical team. From a

resourcing perspective, this would require those with public relations and communications skills/knowledge, with input from legal specialists as necessary.

2.4.11. From a process flow perspective, ITIL[6] provides a recommended Incident Management flowchart that can be used to illustrate the relevant stages. This flowchart is shown in Appendix A.

2.4.12. The second FIRST service area relates to subsequent analysis of relevant artefacts relating to the incident, if these are available. These artefacts will be found on that target/victim device/s, with the analysis process being akin to that of incident forensics.

2.4.13. The suggested FIRST 'Analysis' services are shown in figure 9.

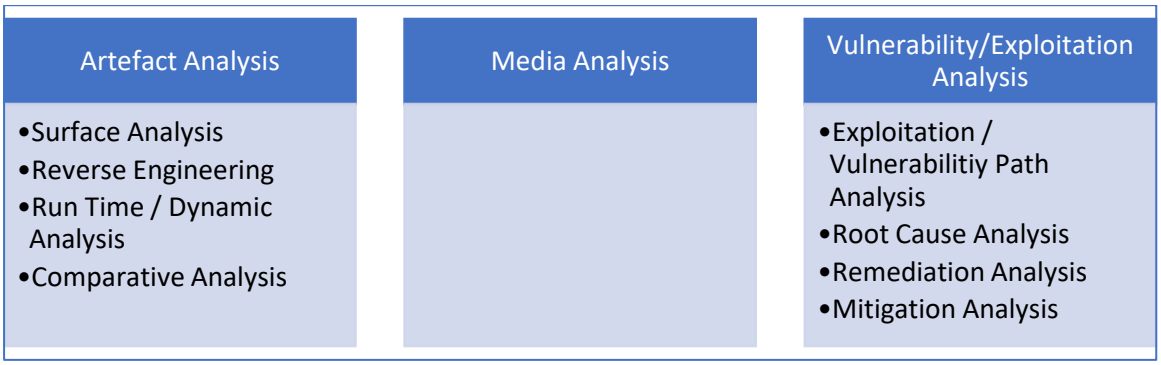
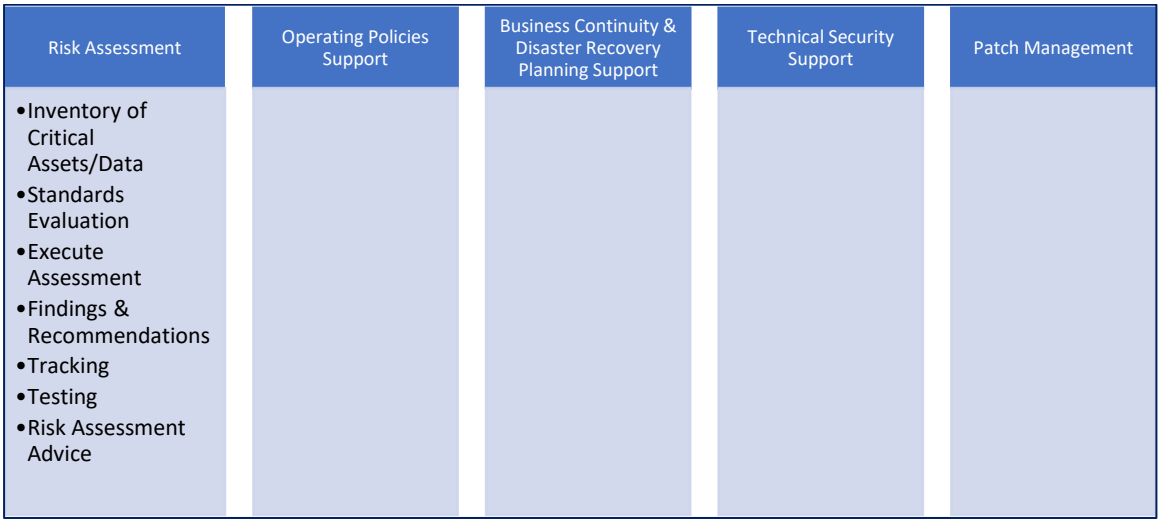


Figure 7 - The 'Analysis' service area. Source: FIRST

2.4.14. Given the nature of these tasks, it is clear that specialist forensic analysis knowledge, skills and experience are required for the composition of this team. At present the ISF (ID)'s Forensic team and many years' experience in this area, and while additional training would be recommended in order to provide an all - round knowledge/skillset within this team.

2.4.15. The third service area is that of 'Information Assurance'. Illustrated in figure 10, this service area is in many respects part of the 'security management' element identified in figure 5, as opposed to the 'reactive' nature of the first two service areas.



[6] *IT Infrastructure Library - https://www.axelos.com/best-practice-solutions/itil*

Figure 8 - The 'Information Assurance' service area. Source: FIRST

2.4.16. An overview of the relevant services is shown below:

a) *Risk Assessment* - A critical element within information/cyber security is that of risk assessment, as discussed in deliverable 1a. Based on current levels of activities, while some risk management activities are currently taking place, it is important to assess the *entire* technical estate and all *relevant* information assets.
b) *Operating Policies Support* – given the current all-purpose ISF information security policy in circulation, the ISF should ensure that its relevant policies are reviewed/maintained on a regular basis and most importantly enforced.
c) *Business Continuity (BC) and Disaster Recovery (DR) Planning Support* – a critical element for the ISF given their activities and operations, it is very important to both plan for and test various BC/DR scenarios. Based on the capability assessment there is scope for additional BC/DR plans to be created and tested to ensure that in the event of a major incident the ISFs infrastructure/resources can continue to operate and provide the required services.
d) *Technical Security Support* – this team would provide general security advise/consultancy services to the CERT/CSIRT's constituency.
e) *Patch Management* – Based on the assessment of the ISF's current capabilities, it appears that while some patch management activities are currently taking place (currently being implemented by the ID IT Security team), it is not centralised between all elements identified in the scope from deliverable 1a and does not consider all recommended patches (only high/critical patches are installed at present), given the lack of either a logically or physically separated development/testing network infrastructure. This team would be responsible for identifying, testing and subsequent deployment of all required patches to the production infrastructure.

2.4.17. The fourth service area is that of 'Situational Assessment', illustrated in figure 11. To be in a position to focus its operational activities and provide input into the risk management process, the ISF's CERT/CSIRT will need to implement a number of tasks to provide an awareness of the environment in which it is operating.

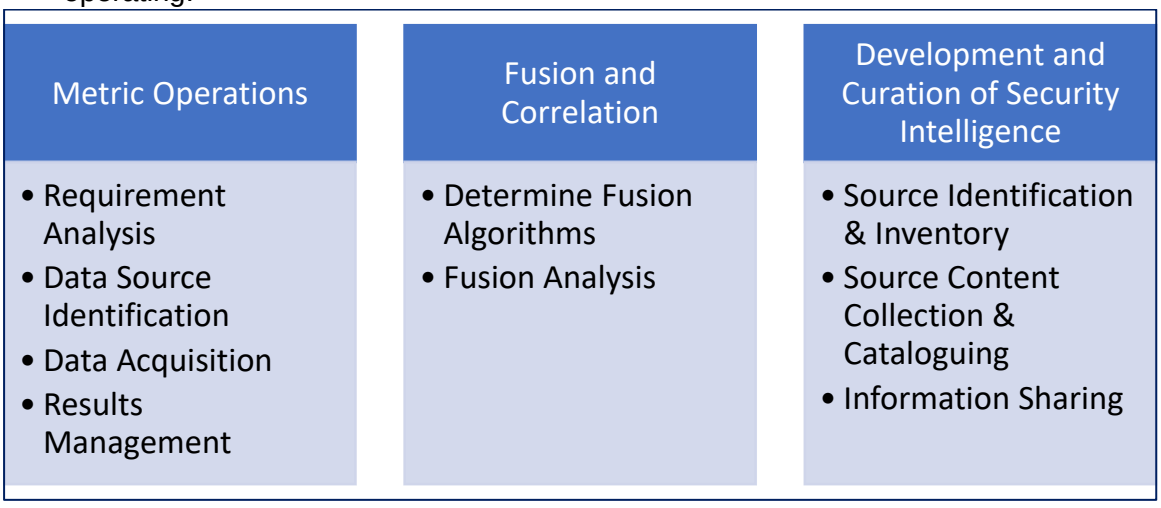


Figure 9 - The 'Situational Awareness' service area. Source: FIRST

2.4.18. These services are discussed below:

a) *Metric Operations* – in order to be able to provide accurate reporting metrics, the requirements for these metrics needs to be identified, the data acquired, and results provided, often in the form of a dashboard or weekly management report showing information such as identified threats, their source, and type.

b) *Fusion and Correlation* – this service focusses on the correlation and analysis of data from multiple sources, and would provide the ISF CERT/CSIRT with the ability to integrate the information gained into a more complete situational awareness assessment.

c) *Development and Creation of Security Intelligence* – this is necessary requirement for the ISF CERT/CSIRT to provide a high level of situational awareness for the supported constituency. External sources would be used by the ISF to provide ongoing threat intelligence relating to both current active threats and potential future threats to the ISFs infrastructure and information assets. While some information sources are free of charge, some require a paid subscription. At present the ISF (ID)'s Security team maintain a daily review of US-CERT and other security-related websites/blogs and it is recommended that the scope of the activities be expanded to include formal threat intelligence and information sharing feeds (both free and subscription based), some examples of which are shown below:

- *FireEye* - https://www.fireeye.com/
- *Looking Glass* - https://www.lookingglasscyber.com/
- *Symantec* - https://www.symantec.com/security-center
- *Recorded Future* - http://recordedfuture.com/
- *ThreatConnect* - https://www.threatconnect.com/
- *SecureWorks* - http://secureworks.com/
- *SANS Internet Storm Center* - https://isc.sans.edu/xml.html
- *Zone-H*- http://www.zone-h.org/
- *Shadowserver* - https://www.shadowserver.org/wiki/
- *Team Cymru* - http://www.team-cymru.com/
- Digital Shadows - https://www.digitalshadows.com/products/digital-shadows-searchlight

2.4.19. The 'Outreach/Communications' service area shown in figure 12 deals with the following:

a) *Security Awareness Raising* - is concerned with the dissemination of information from the ISF's CERT/CSIRT relating to awareness of current/potential threats to all its constituents. Given the lack of both formal awareness training and no significant measure of existing security culture (both discussed in deliverable 1a), a team would be responsible for design, delivery and maintenance of cybersecurity-related training/awareness materials. Given the initially identified constituency of the ISF, all material would need to be relevant to ISF personnel, with any awareness materials being adapted for use with future constituencies as required. This service

would be provided alongside that of Training and Education, discussed in 2.4.18.b.

b) *Cybersecurity Policy Advisement* – as a collection of advisory services, there is involvement required from specialist 'non-technical' areas such as legal counsel, communications, and public relations.

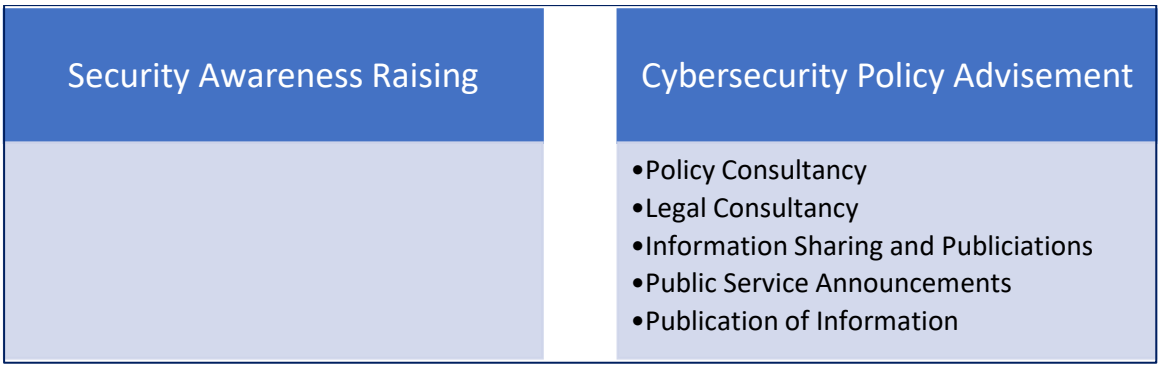


Figure 10 – The 'Outreach / Communications' service area. Source: FIRST

2.4.20. The sixth service area is that of 'Capability Development', illustrated in Figure 13. This looks at the following services:

a) *Organisational Metrics* – as part of any service operation, it is necessary to provide management information (MI) relating to evaluation of the performance of its services. This service is concerned with defining, collecting and analysing service metrics.

b) *Training and Education* – given the requirement for ongoing training/education for all stakeholder of the ISF'S CERT/CSIRT, whether they are a member of the served constituency of or the team delivering the CERT/CSIRT's services.

c) *Conducting Exercises* – as part of the provision of any security service, there is a requirement for testing policies and procedures in a practical environment, such as ensuring that a documented Business Continuity/Disaster Recovery Plan *actually* works when implemented in practice. As part of this process, personnel can be trained in new/revised procedures and assessed as to whether they can carry them out in a practical setting.

d) *Technical Advice* – As the levels of the CERT/CSIRT service mature, its members will be able to provide levels of technical advice to its stakeholders and constituents. While this is not a service that the ISF CERT/CSIRT would look to provide initially, as it's levels of technical expertise advance it would be appropriate for the CERT/CSIRT to act in a 'trusted advisor capacity.

e) *Lessons Learned* – as part of any incident response process, there is a requirement for a review of the steps followed when dealing with an incident to document them and to ultimately learn from any lessons identified, in order to improve any processes/procedures in place.

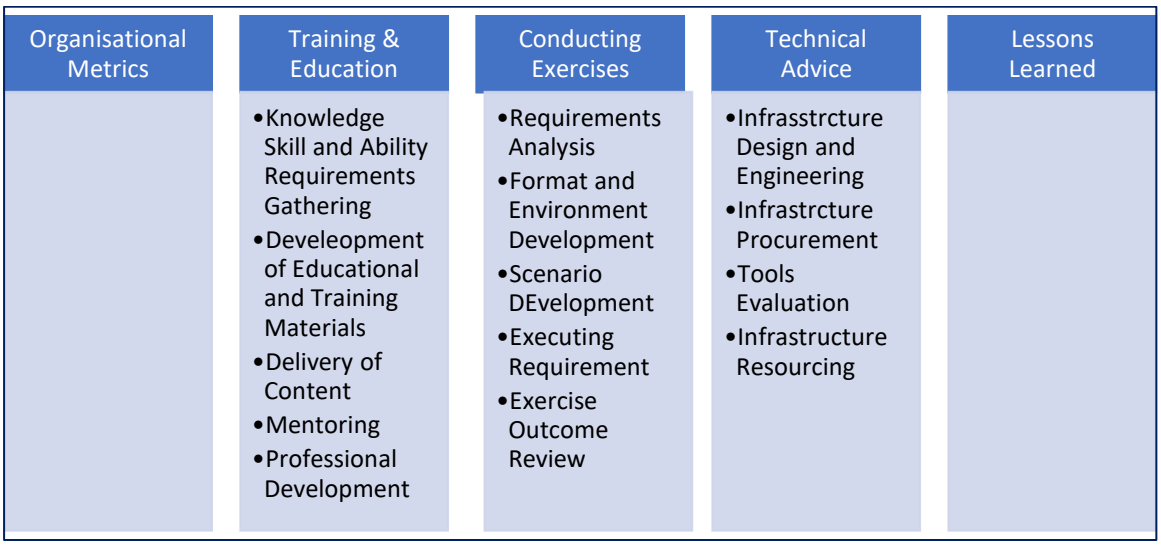


Figure 11 – The 'Capability Management' service area. Source: FIRST

2.4.21. The final service area is that of 'Research and Development', shown in figure 14. The majority of services within this area are more than likely only provided by CERTS with a high level of maturity in knowledge/skills/experience and are able to provide dedicated resources. This service area is comprised of three service areas, as described below:

a) *Development of Vulnerability Discovery/Analysis/Remediation/Root Cause Analysis* – this relates to the ability of a CERT to develop its own capability to discover and analyse vulnerabilities, as opposed to using external third parties, as mentioned in 2.4.16.c

b) *Development of Technologies and Processes for Gathering/Fusing/Correlating Security Intelligence* – this is concerned with the ability of a CERT to develop its own processes to collect, analyse and assess externally-sourced information relating to potential threats to its information assets. Given that the ISF currently has a team working in the area of Open-Source Intelligence (OSINT), this service is in essence further development of that capability, albeit with additionally trained/experienced resources in place to provide this service.

c) *Development of Tools* – given the requirement to maximise the efficiency of all personnel resources dedicated to it, there will be a requirement for a team to work on automating/streamlining the processes, so as to make best use of all CERT personnel.

Figure 12 – The 'Research and Development' service area. Source: FIRST

2.5. Organisational Structure

2.5.1. As discussed in Deliverable 1a, the ISF's IT management, support and administration functions are currently not centralised and there is distinct

demarcation between the Information Department's IT (managed by Lt Col. Youssef) and the remainder of the ISF's IT (managed by Lt. Col. Abdallah).

2.5.2. Given the objective of providing a centralised CERT/CSIRT (also known as an *embedded CERT*[7]) to support the identified constituency, the ISF should consider merging the IT support/administration function of both separate departments.

2.5.3. This merger will provide significant improvement of the knowledge/skills and experience pool within the ISF's overall IT technical pool, and will enable the forming of specialist groups within it who can provide the proposed range of CERT/CSIRT and SOC services.

2.5.4. Based on the framework provided by FIRST, it is proposed that limited services are to be provided by the ISF CERT/CSIRT given the current experience/skillset and the timeline for acquisition of additional specialist skills in incident response through formal training. This proposed initial service offering is shown in figure 15.

2.5.5. It should be noted that a number of activities including development and documentation of processes/procedures, implementation of network infrastructure, hardware and software solutions and completion of technical training will be required in advance of the CERT/CSIRT being able to provide this initial service offering.

2.5.6. These services should be provided alongside those of a newly-created ISF SOC (providing real-time infrastructure/server/endpoint monitoring services). As the CERT/CSIRT matures in terms of knowledge, skills and experience, additional services will be provided to the supported constituency.

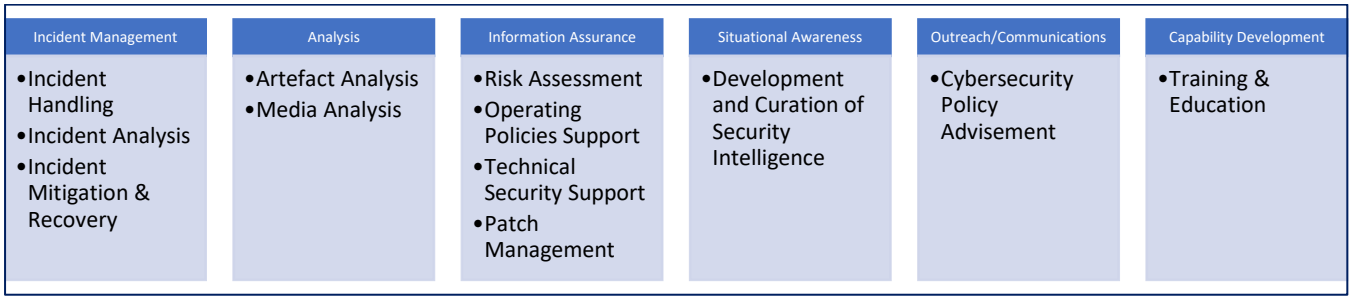


Figure 13 - Proposed initial service offering from the ISF CERT/CSIRT

2.5.7. The proposed initial services to be provided by the ISF CERT correlate with the provision of pro-active, reactive and security management tasks as proposed by ENISA and discussed previously in section 4.1.

2.5.8. Referencing the ENISA model, the it is proposed that the ISF CERT/CSIRT will provide the following initial core services:

a) *Reactive* - Incident response co-ordination/support & post-incident forensics.
b) *Proactive* – security intelligence, patch management.
c) *Security management* – risk management, training/awareness, policy management, business continuity management.

2.5.9. As discussed in Section 3.2.1 and shown in Appendix B, a number of dedicated CERT/CSIRT (and SOC) teams will need to be created in order to provide the operational services. Some of these teams will require specialist training in order to carry out their roles, examples being incident management and risk

[7] https://www.enisa.europa.eu/publications/csirt-setting-up-guide/at_download/fullReport

management. In terms of suggested numbers for these teams these are discussed further in deliverable 2.

2.6. Resources/Skillsets

2.6.1. All ISF CERT/CISRT and SOC resources shall be provided from within the ISF itself. As part of the discovery process for deliverable 1a, the following resource numbers were identified:

a) ISF IT

- Registry – 12 people
- System administration (server) – 3 people
- System administration (endpoint) 15 people
- Networking - 4 people
- Development Team – 15 people
- Deployment – 14 people

b) ISF (ID)

- IT
  - System administration (server/endpoint) – 5 people
  - Networking – 5 people
  - IT security – 5 people
- Forensics Group
  - Digital Forensics – 5 people
  - Open Source Intelligence/Cyber Investigations – 6 people
  - Research & Development – 3 people

c) Cybercrime Bureau

- Investigations (lead & assistant) – 20 people
- Technical analysts – 8 people
- Admin/logistical support – 24 people

2.6.2. In terms of the specific number of ISF resources required to provide the proposed initial service offering, this will be discussed as part of the implementation strategy.

2.6.3. From a skillset perspective, a detailed paper written by Carnegie Mellon University[8] identifies the key core skills that CERT/CSIRT members should have, as shown in figure 16.

[8] *https://resources.sei.cmu.edu/asset_files/WhitePaper/2017_019_001_485684.pdf*

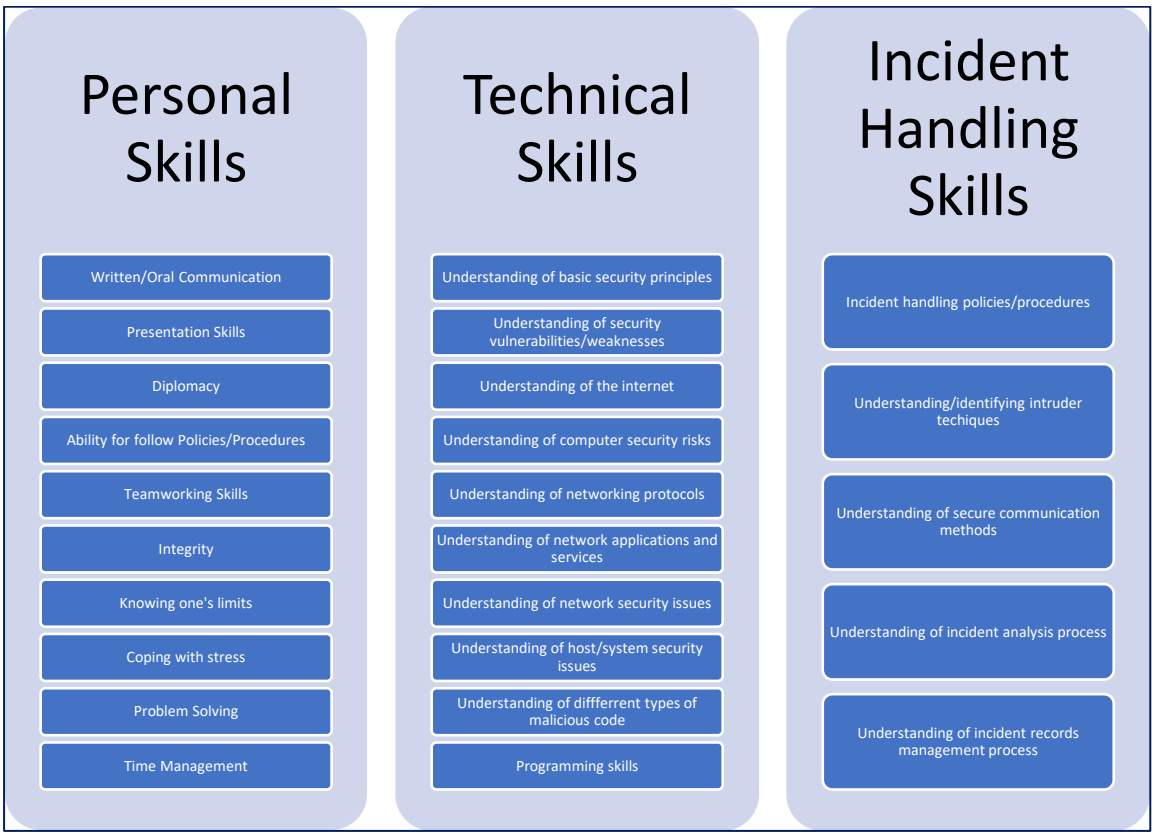


Figure 14 - Suggested skillset for CERT resources. Source: Carnegie Mellon

2.6.4. While all members of the ISF CERT will be expected to have the personal and technical skills as a baseline capability, those involved in the specific tasks surrounding the incident management process should be expected to have the specialist skills as suggested, although it is accepted that training will be required to acquire these skills.

2.6.5. In addition to the skillset identified in figure 16, additional specialist skills will be required for those who will be working in areas such as forensics, investigations and information assurance, with some training being required in these areas.

2.7. Funding

2.7.1. To fund the work to establish and manage the ISF's CERT/CSIRT & SOC, it is expected that the ISF will try to seek support from the donors from the international community.

3. GOVERNANCE

3.1. Governance/Organisation Structure

3.1.1. As discussed in deliverable 1a, a CERT committee has been formed to oversee the implementation and overall co-ordination of all activities relating to the implementation of the ISF CERT.

3.1.2. Figure 17 below shows the proposed initial governance/organisation structure for the ISF's CERT. It is proposed that a CERT 'working group' be formed to include those departments outside the IT management/security areas (i.e. legal, public relations/communications and human resources/personnel)

3.1.3. Given that the number of initially proposed activities will require input from outside of the technical field, hence the representation requirement from outside the organisation 'scope' defined in deliverable 1a.

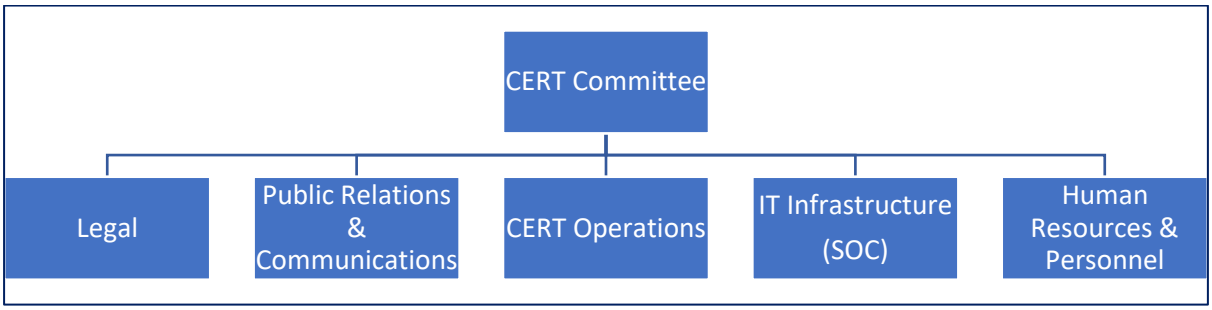


Figure 15 – Proposed initial CERT governance structure

3.1.4. From a perspective of the overall ISF organisation, the CERT/CSIRT should be formed as a dedicated entity (conjoined with the SOC) within the ISF, with a direct reporting/communication chain via the Intelligence Department up to the General Directorate. The CERT/CSIRT should be managed by a CERT/CSIRT Manager (the SOC by a team lead) who manage all operational areas of the CERT/CSIRT and will have under his/her command the dedicated members of the CERT/CSIRT team.

3.2. Roles

3.2.1. Within the CERT/CSIRT governance structure, secondary levels will be carrying out the day-to-day tasks of managing, administering and supporting the CERT/CSIRT. Further information will now be provided relating to the expected role and activities of each area identified in figure 17, with a second-level CERT/CSIRT organisation structure for operations team shown in in Appendix B.

3.2.2. Based on the expected number of resources for initial operation, these have also been provided in the organisation structure shown in Appendix B. Based on the advice provided by the Romanian CERT[9] at a conference held in August 2018 at the ISF Academy, suggested numbers for key service areas are included.

3.2.3. While the operations team is focussed on the 'core' activity of incident response and supporting incident forensics, other activity areas such as information assurance, security intelligence and training should not be neglected, even in the early stages of the CERT/CSIRT's operation.

3.2.4. It should be noted that while the key CERT/CSIRT services and support of its infrastructure should be fulfilled by *dedicated* resources, other roles such as HR,

[9] https://cert.ro/

Communications/Public Relations, Legal can be filled by resources that are not necessarily dedicated to the CERT at its inception and would be part-time/on-call resources.

3.2.5. Given the 24x7x365 nature of ISF operations, the CERT/CSIRT and SOC will need to provide services to support its constituency accordingly, given that incidents can occur at any time, and will therefore have to organise its manpower resources accordingly.

3.2.6. As the CERT/CSIRT matures in terms of capability/services, it is expected that these part-time/on-call resources would be allocated full-time to the CERT/CSIRT.

3.2.7. CERT/CSIRT Committee

3.2.7.1. *Role* - Oversight/governance of all CERT/CSIRT-related activities

3.2.7.2. *Expected scope of activities:*

- Liaison with ISF senior officers
- Liaison with other CERTS/CSIRTS
- Provide leadership of CERT/CSIRT working group

3.2.8. Legal

3.2.8.1. *Role* – Specialist legal adviser to the CERT/CSIRT working group.

3.2.8.2. *Expected scope of activities*:

- Works with communications team to provide legal advice relating to media statements, given the need to protect confidential information and the best interests of the ISF.
- Drafts information sharing agreements with external organisations.
- Provides specialist review of incident response plans.
- Liaison with communications team to complete relevant breach/incident notification documentation.
- Active member of the CERT/CSIRT working group.

3.2.9. Public Relations/Communications

3.2.9.1. *Role* - Single point of contact (SPoC) for anyone outside ISF regarding CERT/CSIRT activities.

3.2.9.2. *Expected scope of activities*:

- Management of all internal/external communications relating to the CERT/CSIRT.
- Establishment of communications policy with legal team.
- Communication of data breach/incident notifications as required following consultation with legal team.
- Active member of the CERT/CSIRT working group.

3.2.10. Operations

3.2.10.1. *Role* – Operational management of the CERT/CSIRT services provided to the constituency

3.2.10.2. *Expected scope of activities*:

- Management for day-to-day CERT/CSIRT operations.
- Co-ordination of technical teams' activities.
- Communications with CERT/CSIRT committee.
- Management of CERT/CSIRT-assigned personnel.
- Provision of management information (MI) reporting to CERT/CSIRT committee.
- Active member of the CERT/CSIRT working group.

3.2.11. IT Infrastructure (SOC)

3.2.11.1. *Role* – Operational management of CERT/CSIRT-related infrastructure

3.2.11.2. *Expected scope of activities*:

- Management of all IT infrastructure supporting CERT/CSIRT operations.
- Co-ordination of technical teams' activities
- Active member of the CERT/CSIRT working group.

3.2.12. Human Resources (HR) / Personnel

3.2.12.1. *Role* – Specialist HR adviser to the CERT/CSIRT committee.

3.2.12.2. Expected scope of activities:

- Provision of HR advice relating to incidents involving ISF personnel.
- Active member of the CERT/CSIRT working group.

4. ROADMAP

4.1. Background

4.1.1. Given the assessment of current capacities and working practices relating to security management previously initiated, several areas were identified in which the ISF needs to either improve existing capabilities (in areas such as patch management, security monitoring, risk management for example), or to implement additional elements (whether they be in technical, procedural, or areas of governance) in order to provide a secure working environment and the platform from which to implement a CERT/CSIRT.

4.1.2. In advance of any specific activities relating to the development of the ISF's CERT/CSIRT, it is advised that a significant number of activities take place which will provide a solid foundation on which to build the CERT/CSIRT and implement an initial service offering to its constituency.

4.1.3. These activities relate to both technical and non-technical areas, and have been placed into a 'Phase 0' of the proposed CERT/CSIRT implementation roadmap. For the implementation of the CERT to be successful, it is important that the pre-CERT/CSIRT activities be completed.

4.1.4. A graphical representation of this roadmap is shown in Appendix C and provided as a separate PowerPoint file.

4.1.5. In terms of subsequent phases, this document has outlined a number of phases (1-3) based on an initial service offering and subsequent implementation of additional services. Dependent on the results of the end-phase review process, there may be a requirement for additional (or fewer) subsequent implementation phases.

4.1.6. At present, no formal timeline has been included with this roadmap. Based on information provided by the Romanian CERT team, it was *estimated* that an initial phase of operation (i.e. initial operating capability (IOC) or 'Phase 1' within this document) would last between 6-12 months, before additional services were added to the CERT/CSIRT portfolio and final operating capability (FOC) would be attained. This suggested timeline does not take into the account Phase 0 outlined in Section 4.2 below, which will increase the length of the overall timeline to IOC and eventual FOC.

4.1.7. It should be noted that some of the Phase 0 activities identified in this document are already ongoing, so it should be noted that from an overall timeline perspective Phase 0 has *already* commenced.

4.1.8. While this document outlines a number of operational phases (these being 1-3) which take the CERT/CSIRT from initial operating capability (IOC) to final operating capability (FOC), there is a possibility that additional (or fewer) phases will be needed to get to a high level of service capability. The end-phase review will provide an opportunity to review the plan for the next phase.

4.1.9. Once the ISF CERT/CSIRT reaches a high level of service provision and maturity, it would be of benefit to make an application to Carnegie Mellon University for use of the CERT® trademark.

4.1.10. To measure maturity of the CERT/CSIRT and determine whether it is meeting its service objectives, ENISA developed a tool[10] which can be used to gauge the CERT/CSIRT's capabilities in multiple areas.

[10] *https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/*

4.1.11. Based on the SIM3[11] model for security incident management, the tool will allow the ISF to determine the maturity level of its CERT/CSIRT.

4.1.12. An example of the results of this assessment are shown in Appendix D. It should be noted that the results shown are for example purposes only and have not been based on a formal assessment.

4.1.13. It is recommended that the maturity assessment process is carried out at the end of each 'implementation phase', as it will assist in determining objectives for the next phase.

4.1.14. An alternative maturity assessment model has been created by the CREST[12] organisation. This model has been based on the assessment on the 3-main phases of incident management (prepare, respond, follow-up) and was developed with input from a broad range of commercial organisations, suppliers of security services and the UK government. An example of this assessment is shown in Appendix E.

4.1.15. A high-level maturity assessment tool has been provided by the Netherlands National Centre for Cybersecurity (NCSC.NL). The 'GCCS Maturity Scan'[13] provides an assessment of those areas requiring improvement. An example of the results of this assessment ca be found in Appendix F.

4.2. Phase 0 – Pre-IOC

4.2.1. *Governance*

a) A CERT/CSIRT operational organisation structure should be agreed (as suggested in Appendix B), to ensure that that all teams providing input into the CERT can allocate the required resources to it.

b) Given that the high-level CERT/CSIRT committee is already in existence to oversee its implementation, a second-level structure ''working group (as shown in in figure 17) should be formed to oversee operational aspects of the CERT/CSIRT.

c) To provide management and co-ordination for all elements relating to the creation of the CERT/CSIRT, the ISF should form a project team and create a formal project plan to ensure that all activities related to its creation are organised, planned, documented and structured.

d) A review of the current information security policy should be carried out with new versions of the documents created and issued, that will be applicable to both regular users and technical teams.

e) A comprehensive risk assessment should be carried out to identify all relevant ISF information assets potential risks and vulnerabilities. A Senior Risk Officer (SRO) role should be established to oversee all risk management activities.

f) Once the initial services/functionality to be provided by the ISF CERT/CSIRT has been confirmed, standardised operating procedures/processes should be developed and documented, to ensure that all personnel are aware of how to carry out their relevant role. This task should be carried out by the nominated incident response team leader, although it is expected that some external consultancy assistance may be needed in order to complete this task. The NIST publication SP800- 61r2[14] can be used to assist in this area.

[11] *https://www.terena.org/activities/tf-csirt/publications/SIM3-v15.pdf*
[12] *https://www.crest-approved.org/index.html*
[13] *https://check.ncsc.nl/*
[14] *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf*

g) As per the Deming cycle[15] outlining the process for continual review and improvement, both d) and e) should be reviewed on a regular basis to confirm that they continue to meet the operational requirements of the ISF.
h) Working relationships should be established with recognised CERTS/CSIRTS to create an information/best practice information exchange process and also establish the proposed ISF CERT as a formal entity.
i) In addition, an application should be submitted for 'Liaison Member' level membership of the FIRST organisation. This will provide access to information sharing forums with other incident response teams.
j) While the approval of relevant legislation is out of control of the ISF, the committee should familiarise themselves with the draft versions of the legislation relating to cyber security/cybercrime, to provide a level of understanding as to their legal bounds in this area.

4.2.2. Training

a) Following identification of any specific requirements, based on the service offering to be provided by the CERT/CSIRT, training courses should be undertaken to ensure that that all resources have the appropriate level of knowledge and skills for the role they will be carrying out once the CERT/CSIRT becomes operational.
b) An internal ISF cyber security awareness programme should to be developed, to be used to educate all ISF personnel and provide a foundation level of understanding in all areas of cyber security.

4.2.3. *Technical*

a) A number of security elements (SIEM & IDS/IPS) are currently in the proof-of-concept phase on the Intelligence Department (ID) IT network. A separate project is currently ongoing to create a data centre (DC) for the ISF IT network, which will also include SIEM and IDS/IPS elements (the expected timeline for completion of this DC build is expected to be early in 2019). It should be noted that in advance of full operation, these security appliances will require 'tuning' in the live production environment to eliminate excessive false positives, so that alerts from these appliances will relate to unusual or anomalous activities. This task can potentially last for several months until the excess false positives are eliminated, impacting the overall CERT implementation timeline.
b) Given the requirement for ongoing real-time monitoring of the devices discussed in a) above, a security operating centre (SOC) team should be created to provide this dedicated service for security appliances and other devices on ISF infrastructure, such as servers, network devices.
c) A review should be carried out to determine the exact number of endpoints running non-supported operating systems/software on the ISF estate. A project should be initiated to ensure that all non-supported endpoints are upgraded to a supported operating system, which will minimise the existing vulnerabilities and mitigate potential endpoint risk.
d) Given the potential risk of un-tested patch deployment onto production devices, a separated (preferably physically) network infrastructure should be created so that all patches/updates can be *fully* tested in terms of system, end-to-end, integration testing perspectives. This will ensure that full testing can

[15] *https://deming.org/explore/p-d-s-a*

be carried out for all recommended and critical/high patches prior to deployment.

e) The current network infrastructure for both ISF and ID LANS should be reviewed to ensure that it continues to meet operational requirements. Given that one of the identified threats to the ISF relates to denial of service (DoS) attacks, the ISF should ensure that its infrastructure has the availability to cope with this type of attack. As such, the technical infrastructure may need to be redesigned accordingly.

f) A separate network infrastructure be created for use by the CERT/CSIRT team, with a dedicated subnet/VLAN created for the purposes of forensics and malware analysis. A simplified LAN design is shown in figure 18.

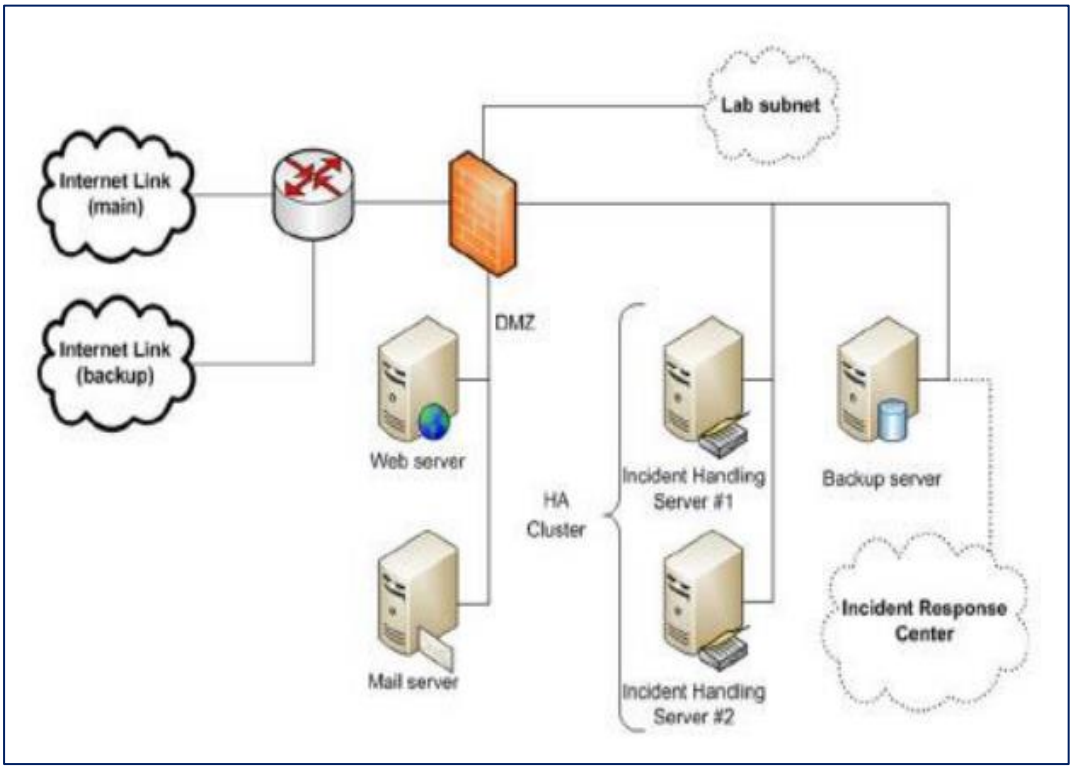


Figure 16 - Suggested CERT/CSIRT LAN design. Source: ENISA

g) In addition to CERT/CSIRT LAN, consideration should be given to the hardware/software requirements for the CERT/CSIRT team. This should include dedicated server/s, workstations for the incident response (IR) team, laptops for forensics/analysis teams and network devices that can support port mirroring (providing network traffic capture).

h) To assist with infrastructure development, ENISA have provided a guide[16] to support a related online training module in this area.

i) Further to points d) to f) above, a physical location needs to be determined from where the ISF can provide SOC-related and CERT/CSIRT services. This location should provide appropriate physical security and provide space for future expansion when additional personnel are assigned to the CERT/CSIRT.

j) Based on the requirements identified above for specific network infrastructure and hardware/software to be provided to the ISF CERT/CSIRT, a dedicated

[16] *https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/2016-resources/developing_csirt_infrastructure-handbook*

physical location should be determined from where the CERT/CSIRT and SOC will operate. This location should be able to provide future expansion in terms of people and equipment, and should be physically secured as per ISF's standard operating procedures (SoPs). While a 'virtual' location may be suitable for a short initial period, a specific location should be agreed from where an eventual 'physical' CERT/CSIRT and SOC can operate.

k) A full technical vulnerability assessment should be carried out on the entire ISF estate. This will enable existing vulnerabilities to be remediated/patched in advance of CERT/CSIRT's initial operation.

l) Given the importance of being able to track cyber security incident tickets and build a base of information for reporting/knowledge-sharing, a requirements analysis process should be carried out to determine the best CERT/CSIRT ticketing system, information sharing and other supporting applications to be implemented. Once the best solution has been identified (whether it be open-source or commercial-off-the-shelf (COTS)), it should then be implemented and appropriate training provided to the personnel who will be using it. As part of the conference held in August 2018 at the ISF Academy, personnel from the Romanian-CERT suggested several applications which could be used for ticketing and information sharing:

- RTIR - https://bestpractical.com/rtir
- OTRS - https://otrs.com/
- MiSP - http://www.misp-project.org/

m) As part of the implementation process for the incident management ticketing application, the CERT/CSIRT committee should agree on the incident classifications to be used – proposed classifications[17] are provided by Trusted-Introducer scheme. An alternative classification scheme[18] is suggested by FIRST.

4.3. Phase 1 - IOC

4.3.1. *Governance*

a) Previously defined CERT/CSIRT operating processes/procedures should be monitored during this phase and reviewed to ensure they meet requirements. The CERT/CSIRT working group/committee will meet regularly to review activities.

b) As the CERT/CSIRT commences operations, it should register itself as an 'operational team' with the TF-CSIRT scheme[19] and also make an application to Carnegie Mellon for use of the CERT trademark[20].

4.3.2. *Operations*

a) The CERT/CSIRT will commence operations, providing a limited number of services as suggested by the FIRST framework (see figure 15).

b) Incident trends will be identified and management reports provided to the CERT/CSIRT working group/committee.

[17] *https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf*
[18] *https://www.first.org/resources/guides/csirt_case_classification.html*
[19] *https://www.trusted-introducer.org/processes/registration.html*
[20] *https://www.sei.cmu.edu/education-outreach/license-sei-materials/authorization-to-use-cert-mark/*

c) Towards the end of phase 1, a review of the current level of CERT/CSIRT service offering should be carried out to determine effectiveness of operation and also determine the next phase of service offering.

4.3.3. Training

a) The training/awareness programme for ISF personnel shall be established. This training will be scheduled on a regular basis and be supported by interim updates/refresher training.

4.4. Phase 2

4.4.1. Governance

a) The ISF CERT/CSIRT should apply for full membership of the FIRST organisation. This will provide it with formal recognition of its status as a CERT/CSIRT.

b) The CERT/CSIRT working group will continue to meet regularly to review activities/incident metrics.

c) As part of the continual-review process, the CERT/CSIRT operating processes/procedures should be reviewed to ensure they meet requirements.

4.4.2. *Operations*

a) Additional CERT/CSIRT services will be implemented, dependent on resource availability and skills/experience.

b) Towards the end of phase 2, a review of the current level of CERT/CSIRT service offering should be carried out to determine effectiveness of operation and also determine the next phase of service offering.

4.4.3. *Training/Awareness*

a) A review of the training carried out to date (user awareness and technical team) to determine effectiveness and provide recommendations for future training.

b) Cybersecurity awareness material should be designed/created for use with general public.

4.4.4. *Technical*

a) Development of the ISF website to provide improved cybercrime reporting capability and alerting functionality.

4.5. Phase 3 - FOC

4.5.1. Governance

a) The CERT/CSIRT working group will continue to meet regularly to review activities/incident metrics.

a) As part of the continual-review process, the CERT/CSIRT operating processes/procedures should be reviewed to ensure they meet requirements.

b) An information sharing capability should be developed with other Lebanese entities such as government departments and critical national infrastructure (CNI) entities.

c) The ISF CERT/CSIRT should look to apply for full membership of the FIRST organisation. In addition, it should look to apply for formal accreditation with the TF-CSIRT scheme.

4.5.2. *Operations*

a) Additional CERT/CSIRT services will be implemented, dependent on resource availability and skills/experience.

b) Towards the end of phase 2, a review of the current level of CERT/CSIRT service offering should be carried out to determine effectiveness of operation and also determine the next phase of service offering.

4.5.3. *Training/Awareness*

a) A review of the training carried out to date (user awareness and technical team) to determine effectiveness and provide recommendations for future training.

b) Cybersecurity awareness material released to the general public.

4.6. Additional Phases

4.6.1. Dependent on the maturity of the ISF CERT/CSIRT's capability, the requirement for additional phases may exist as new services are provided. This may be based on the timeline for personnel to receive training in specialist areas.

4.6.2. Given the ISF's long-term plan is to evolve into providing alerts for an enlarged constituency, additional phases in the maturity of the ISF CERT/CSIRT will provide the opportunity for gradual growth. As part of this process, there is a requirement to apply to Carnegie Mellon University to use the CERT® trademark[21], given that they have control over the use of this term. An application to use the trademark and therefore be able to call itself a CERT will therefore need to be submitted.

[21] *https://www.sei.cmu.edu/education-outreach/license-sei-materials/authorization-to-use-cert-mark/index.cfm*

5. CONCLUSIONS

5.1. Summary

5.1.1. Following previous identification of the current capacities within ISF in respect to management of information/cyber security, this document has outlined a proposed vision for the planned implementation of a CERT/CISRT providing an incident response capability and supporting services to the ISF.

5.1.2. Based on the FIRST (Forum of Incident Response and Security Teams) framework, a number of service areas together with supporting services has been suggested as the initial service offering to be provided to the ISF's constituency, (identified as the ISF and its infrastructure).

5.1.3. Given the ISF's current capabilities from a technical perspective, it is proposed that the number of services is initially limited, and expanded as the CERT/CSIRT's level of maturity increases and personnel have received training in the specialised areas in which they can provide services.

5.1.4. In addition to the CERT/CSIRT activities, it is recommended that the ISF implements a dedicated security operations centre (SOC) which will provide ongoing infrastructure monitoring and direct liaison with the incident management team in the CERT/CSIRT.

5.1.5. Given the role of the ISF in investigation of cyber-related crimes, the CERT/CSIRT will have direct liaison with other departments outside of its 'organisation structure' (such as the cybercrime bureau and forensics group) who will provide specialist investigatory teams dependent on whether the suspected perpetrator is a nation-state/terrorist group or an alternative threat actor group).

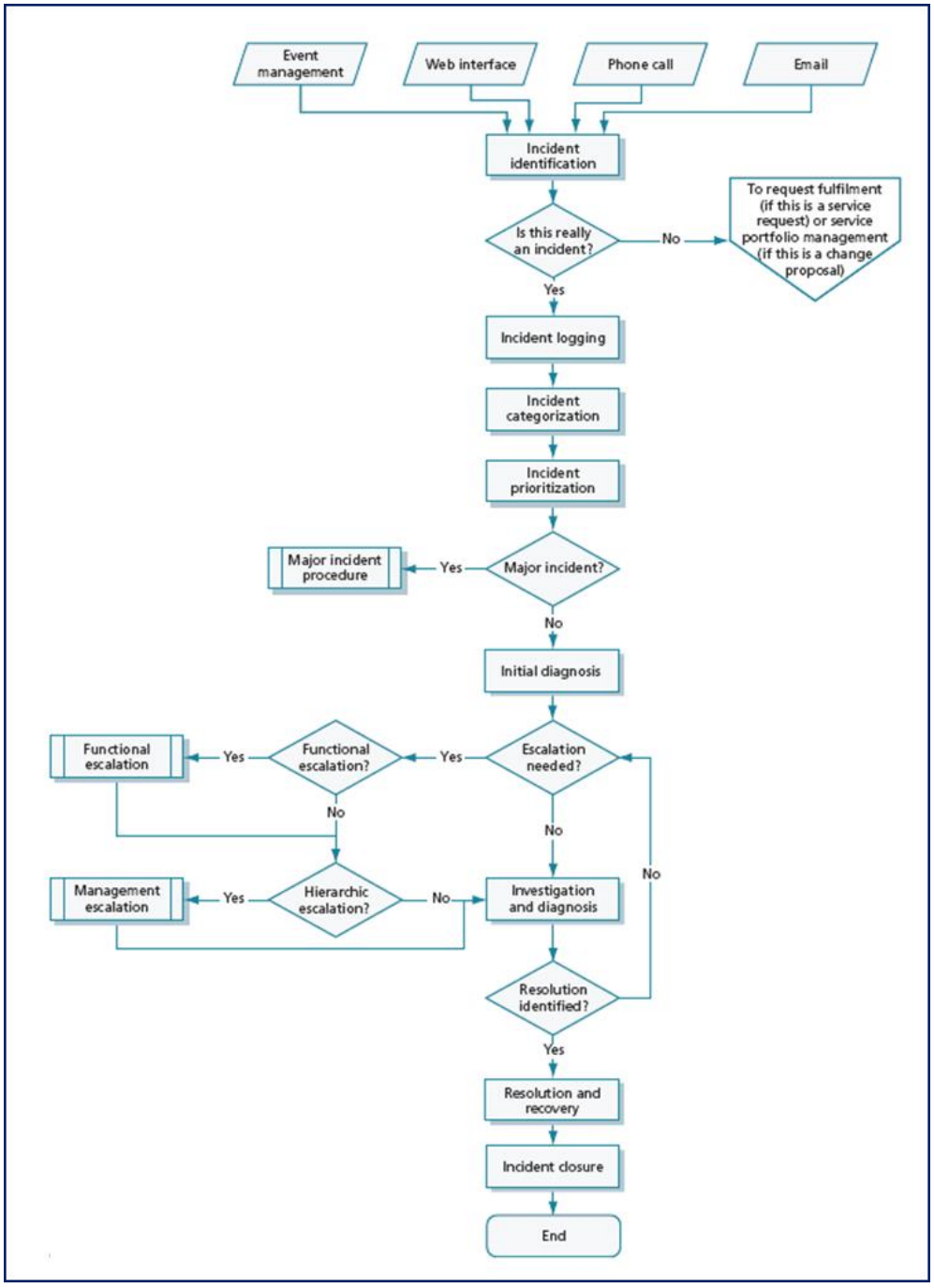
5.1.6. In advance of the ISF CERT/CSIRT's initial phase of operation (i.e. IOC), the number of recommended pre-IOC activities (discussed in Section 4.2) is considerable. These activities relate to both technical and non-technical tasks, and should ensure that once implemented, the CERT/CSIRT can successfully initiate operations with a dedicated infrastructure, personnel resources, supporting applications, formal governance/organisation structure, and relevant policies and supporting document processes/procedures that will standardise operational tasks, irrespective of the personnel implementing them.

5.1.7. Given the number of activities identified in 'Phase 0', the timeline for initial operation of the CERT/CSIRT (Phase 1) is very much dependent on the implementation of all the recommended elements. Some will clearly take longer than others (such as the tuning/configuration of SIEM/IDS appliances) and implementation of the dedicated CERT/CSIRT infrastructure, applications. This will in turn impact subsequent phases/activities and the activation (IOC) of the CERT/CSIRT.

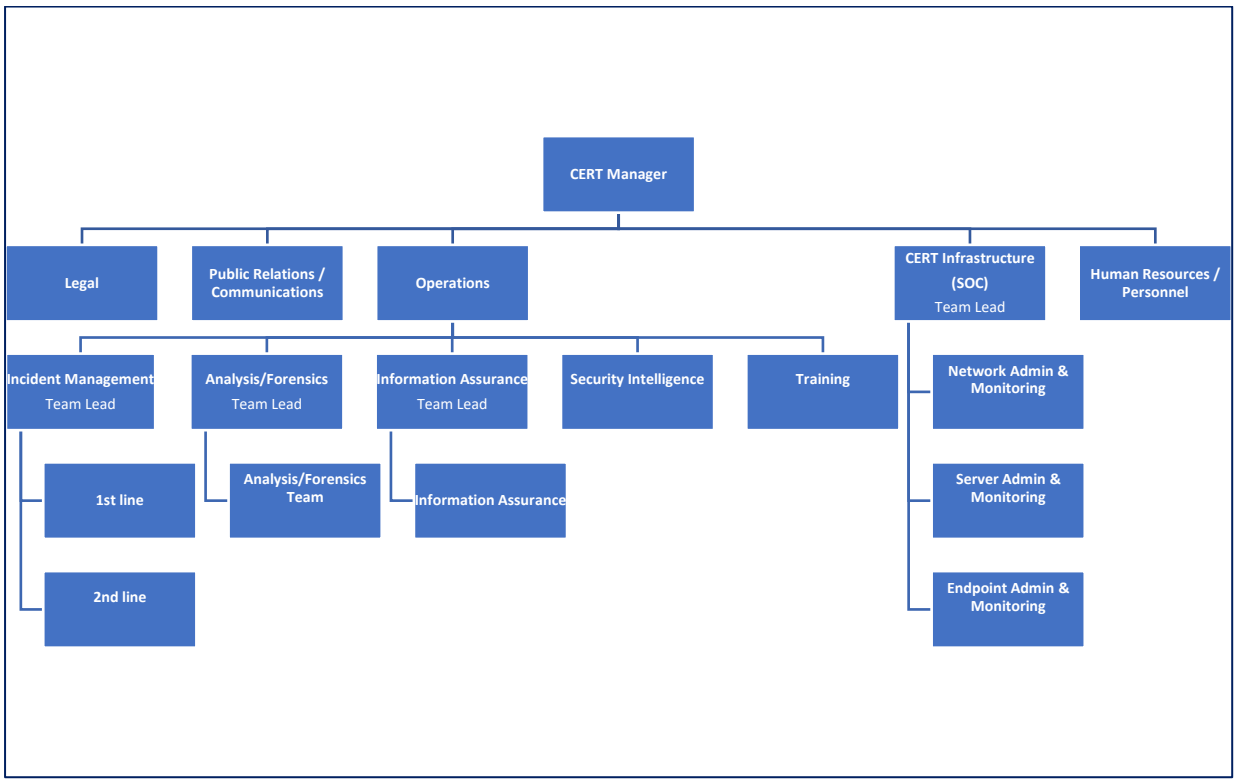
5.1.8. In terms of follow on from this document, a strategic implementation plan will be created, the contents of which will include a detailed CERT/CSIRT action plan, proposed timetable, budget estimation, key recommended standards and training plan.

6. APPENDICES

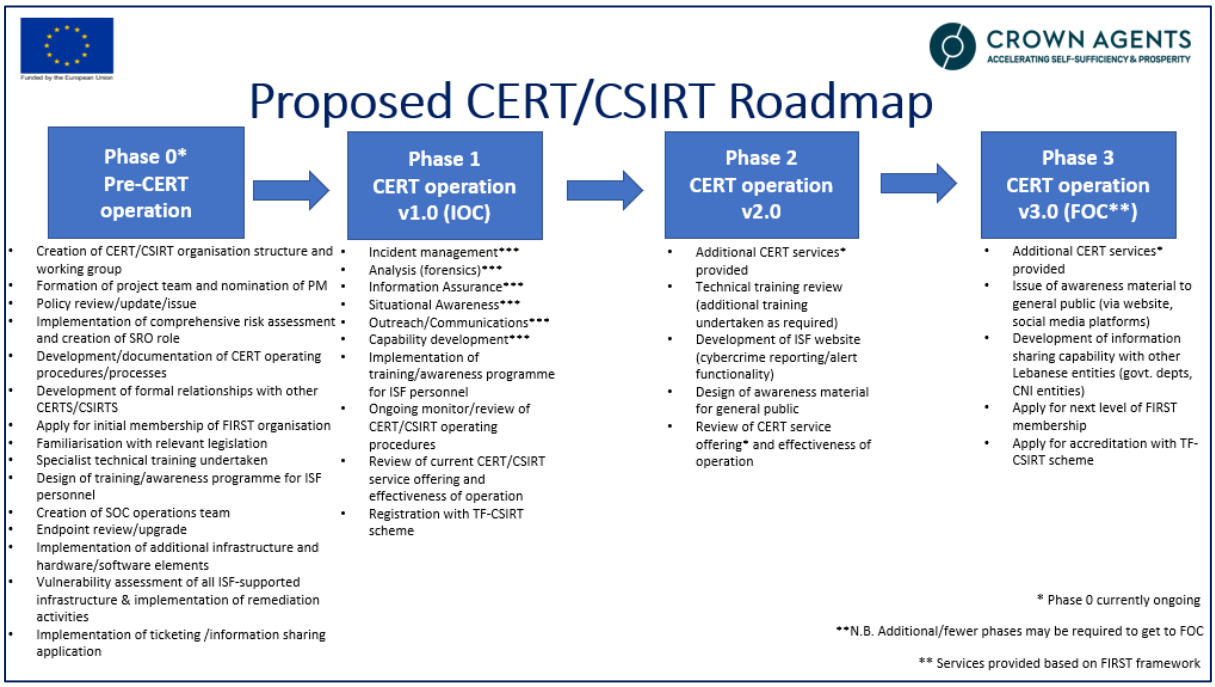
6.1. Appendix A – ITIL Incident Management process flowchart



6.2. Appendix B – Proposed ISF CERT/CSIRT organisation structure



6.3. Appendix C – Graphical Representation of Roadmap

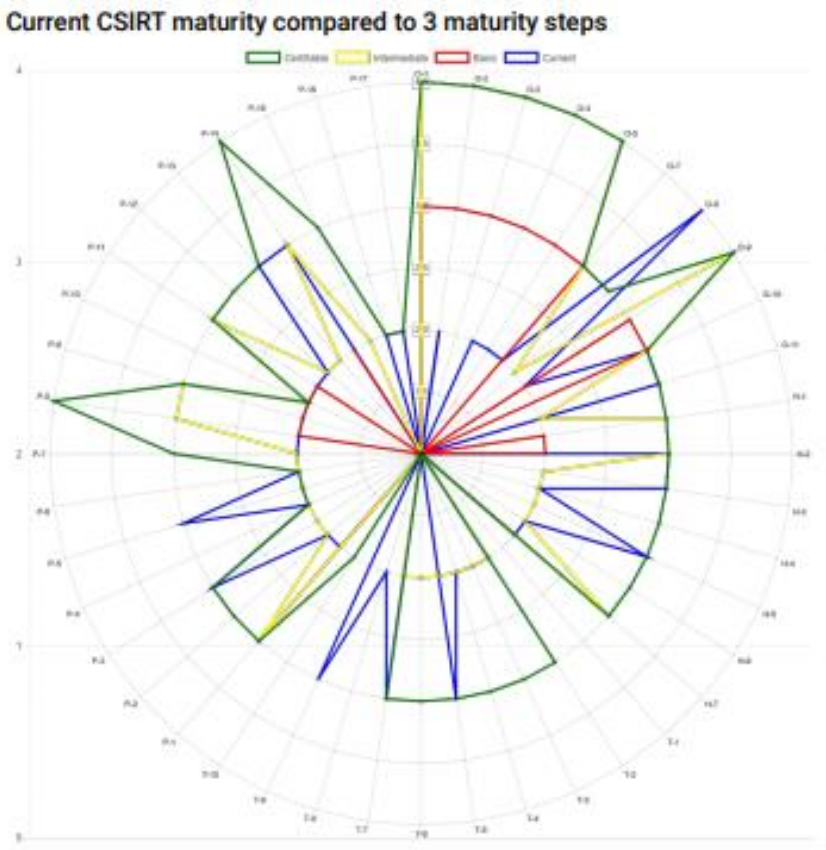


6.4. Appendix D – Example of ENISA CSIRT Maturity Assessment

CSIRT Maturity - Self-assessment Survey

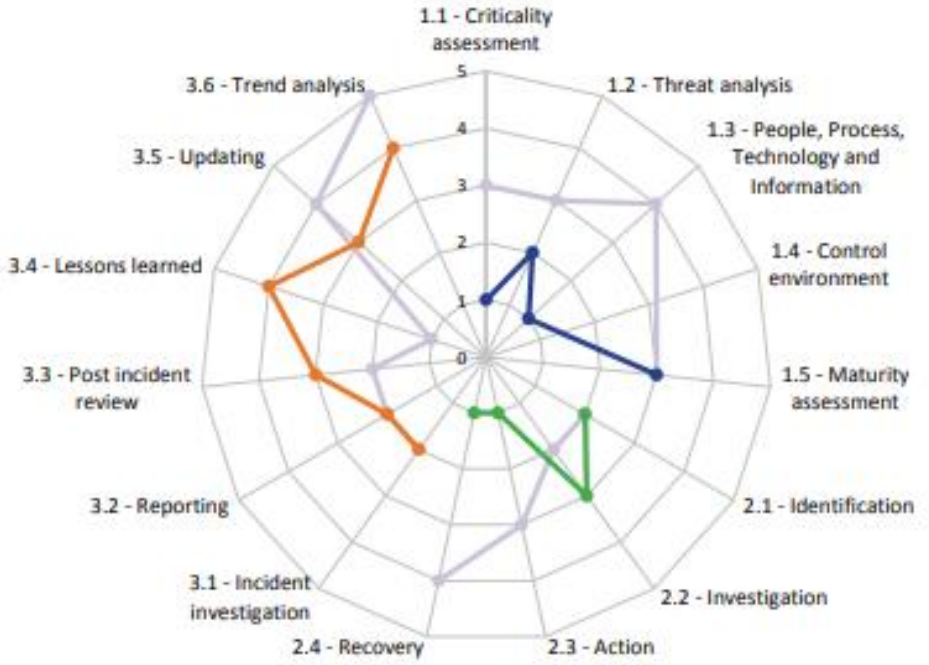
SIM3 Parameter	Parameter description	Assessed maturity:	Minimum demand for the 3 maturity steps:		
		Current	Basic	Intermediate	Certifiable
O-1	Mandate	1	3	4	4
O-2	Constituency	2	3	4	4
O-3	Authority	1	3	4	4
O-4	Responsibility	2	3	4	4
O-5	Service Description	2	3	4	4
O-7	Service Level Description	2	3	3	3
O-8	Incident Classification	4	1	2	3
O-9	Participation in Existing CSIRT Frameworks	2	3	4	4
O-10	Organisational Framework	3	3	3	3
O-11	Security Policy	3	1	2	3
H-1	Code of Conduct/ Practice/Ethics	1	2	3	3
H-2	Personal Resilience	3	2	3	3
H-3	Skillset Description	3	1	2	3
H-4	Internal Training	2	1	2	3
H-5	(External) Technical Training	3	1	2	3
H-6	(External) Communication Training	2	1	2	3
H-7	External Networking	2	2	3	3
T-1	IT Resources List	1	1	1	1
T-2	Information Sources List	2	1	2	3
T-3	Consolidated E-mail System	2	1	2	3
T-4	Incident Tracking System	2	1	2	3
T-5	Resilient Phone	3	1	2	3
T-6	Resilient E-mail	1	1	2	3
T-7	Resilient Internet Access	3	1	2	3
T-8	Incident Prevention	2	1	1	1

SIM3 Parameter	Parameter description	Assessed maturity:	Minimum demand for the 3 maturity steps:		
		Current	Basic	Intermediate	Certifiable
	Toolset				
T-9	Incident Detection Toolset	3	1	1	1
T-10	Incident Resolution Toolset	1	1	1	2
P-1	Escalation to Governance Level	2	3	3	3
P-2	Escalation to Press Function	2	1	2	3
P-3	Escalation to Legal Function	3	1	2	3
P-4	Incident Prevention Process	2	1	2	2
P-5	Incident Detection Process	3	1	2	2
P-6	Incident Resolution Process	2	1	2	2
P-7	Specific Incident Processes	2	1	2	3
P-8	Audit/Feedback Process	2	2	3	4
P-9	Emergency Reachability Process	2	2	3	3
P-10	Best Practice Internet Presence	2	2	2	2
P-11	Secure Information Handling Process Question	2	2	3	3
P-12	Information Sources Process	2	1	2	3
P-13	Outreach Process	3	1	2	3
P-14	Reporting Process	3	2	3	4
P-15	Statistics Process	1	1	2	3
P-16	Meeting Process	2	1	1	2
P-17	Peer-to-Peer Process	2	1	1	2

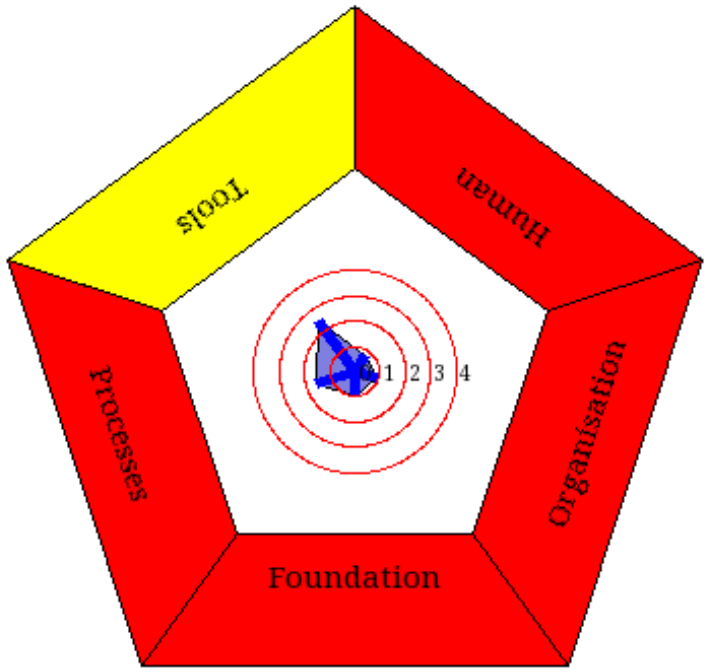


6.5. Appendix E – Example of the CREST Incident Response Maturity Assessment

Cyber Security Incident Response	Maturity level (1 to 5)	Target maturity (1 to 5)
CSIR - Overall	1.2	1.6
Phase 1 - Prepare	0.8	1.3
Step 1 - Criticality assessment	1	3
Step 2 - Threat analysis	2	3
Step 3 - People, Process, Technology and Information	1	4
Step 4 - Control environment		
Step 5 - Maturity assessment	3	3
Phase 2 - Respond	0.8	1.4
Step 1 - Identification	2	2
Step 2 - Investigation	3	2
Step 3 - Action	1	3
Step 4 - Recovery	1	4
Phase 3 - Follow up	2.2	2.0
Step 1 - Incident investigation	2	2
Step 2 - Reporting	2	2
Step 3 - Post incident review	3	2
Step 4 - Lessons learned	4	1
Step 5 - Updating	3	4
Step 6 - Trend analysis	4	5



6.6. Appendix F – Example of the NCSC.NL GCCS Maturity Scan



Legend:

Red:	Low overall maturity, demands attention on most if not all areas.
Amber:	Mixed overall maturity, requires closer auditing and attention on lacking areas.
Green:	Good overall maturity, deserves closer auditing and attention on focus areas.