Funded by the European Union

CROWN AGENTS
ACCELERATING SELF-SUFFICIENCY & PROSPERITY

STRATEGIC PLAN FOR ESTABLISHING A COMPUTER EMERGENCY RESPONSE TEAM (DELIVERABLE 2)

v1.0 OCTOBER 2018

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

Version Control

Version	Date	Comments
v0.1	03/09/18	Initial Draft
v0.5	*26/09/18*	*Draft updated and issued for initial review*
v0.7	*N/A*	*Draft updated and issued for secondary review*
v0.8	*N/A*	*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	

CONTENTS

1. INTRODUCTION

1.1. Background

1.1.1. 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.

1.1.2. 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.

1.1.3. The third of these deliverables relates to provision of a strategic implementation plan, which will include an action plan, timetable, budget estimation, related key-standards and training master plan.

1.1.4. 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. Objective

1.2.1. The objective of this document is to provide a strategic implementation plan which will lead to implementation of the CERT/CSIRT for the Lebanese Internal Security Forces (ISF).

1.3. Scope

1.3.1. The scope of this document encompasses the recommended steps that the ISF will need to take in order to prepare itself for initial operating capability (IOC) of its CERT/CSIRT and eventually final operating capability (FOC), the state in which the full suite of services to its constituency.

1.3.2. As discussed in deliverable 2, the ISF will need to carry out a number of activities in different areas, encompassing technical, procedural and educational tasks.

1.3.3. This document will outline a proposed action plan for each stage of the CERT/CSIRT implementation, together with an estimation of the effort required to complete the suggested tasks.

1.3.4. To assist formalisation of processes and procedures, information will be provided relating to supporting standards and frameworks within information security that will support the ISF in its efforts to create both a CERT/CSIRT and manage ongoing information security issues affecting its organisation.

1.3.5. Given the requirement previously identified for training in multiple areas, information will be provided relating to the expected knowledge and skills needed to both establish and manage a CERT/CSIRT. Following investigation as to appropriate training courses, this information will be provided together with both specific suggested training recommendations and training providers, both inside and outside of Lebanon.

2. ACTION PLAN AND TIMETABLE

2.1. Overview

2.1.1. As outlined in deliverable 1b, a number of phases have been identified which will take the CERT/CSIRT from pre-initiation through to initial operating capability (IOC) and onwards to full operating capability (FOC).

2.1.2. Given the multiple-phases identified, these are shown in figure 1 below together with an approximate overall timeline.

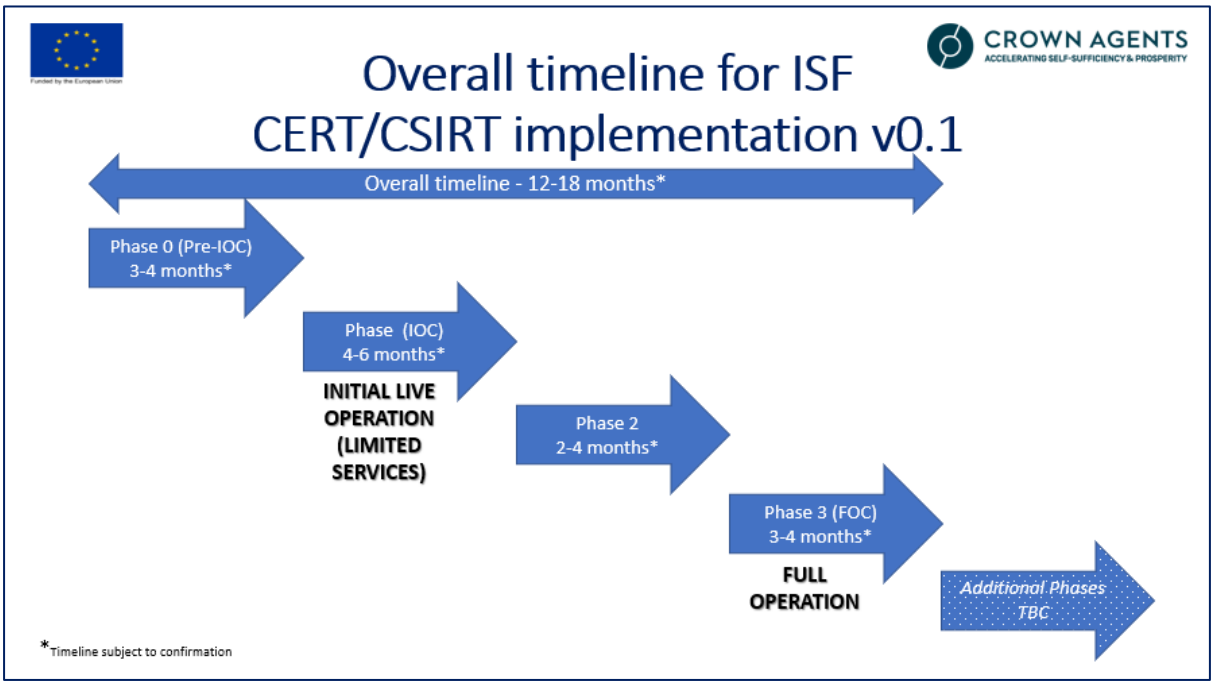

Figure 1 - Overall estimated timeline for ISF CERT/CSIRT implementation

2.1.3. The steps required for each of these stages will now be examined in further detail to provide an action plan for each one.

2.1.4. It should be noted that the list of activities discussed is not exhaustive and there may be additional tasks which arise as the CERT/CSIRT implementation project develops.

2.2. Phase 0 – Pre-IOC

2.2.1. Following initial assessment of current capabilities (documented in deliverable 1a) and as discussed in the separate deliverable 1b, this phase contains the suggested activities that will be need to be carried out in advance of activations and 'go-live' for the initial capability for the ISF CERT/CSIRT. In addition, a number of identified 'sub-projects' have been listed.

2.2.2. An overview of these activities, together with an estimated timeline is shown below in Figure 2.

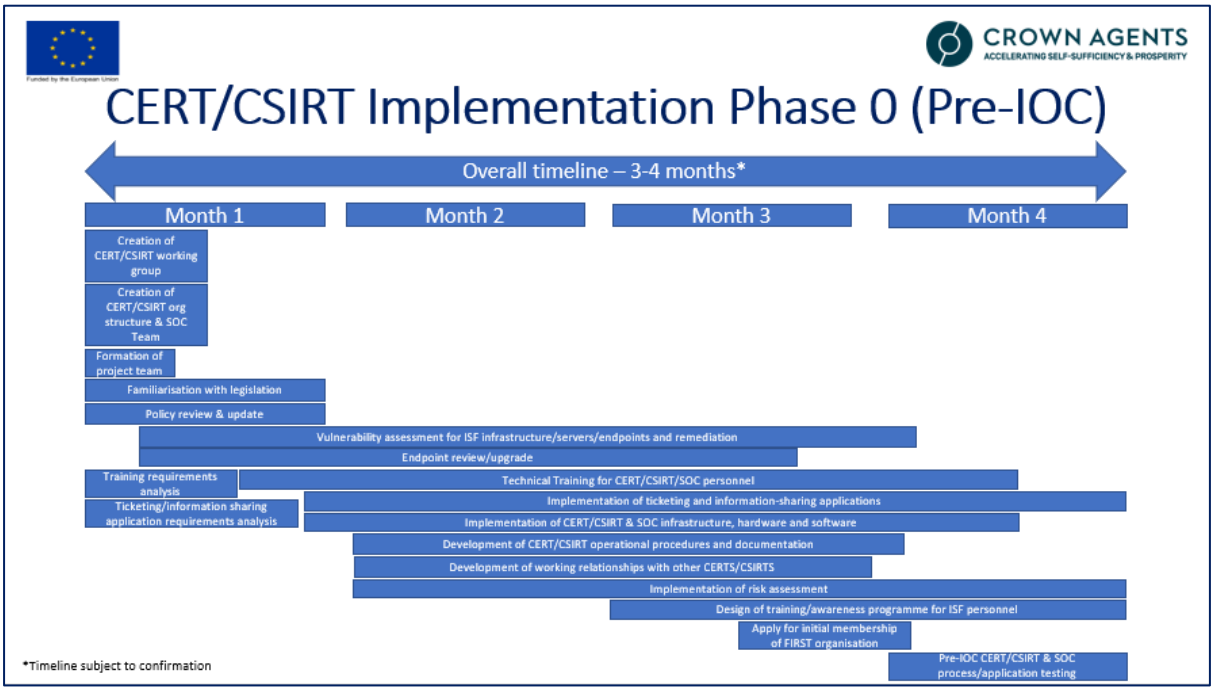

Figure 2 - Phase 0 tasks with estimated timeline

2.2.3. To ensure that all activities related to the implementation of the CERT/CSIRT are organised and co-ordinated, a programme/project team should be formed, under the control of an appointed programme/project manager (PM). The PM will act as the initial point of contact for all activities relating to the CERT/CSIRT's implementation and will work closely with the already-existing CERT committee.

2.2.4. In addition to the programme/project team, a CERT/CSIRT working group should be formed to include involvement from 'non-IT' teams given the activities required once the CERT/CSIRT is operational. Given the involvement from these other teams (PR/communications, legal and human resources/personnel) as part of the operational team and also the proposed working group, discussions with these departments should be initiated

2.2.5. Consideration should also be given to the technical resources who will form the CERT/CSIRT team, together with the security operations centre (SOC) team. This should be based on the proposed organisational structure discussed in deliverable 1b and also shown below in figure 3.

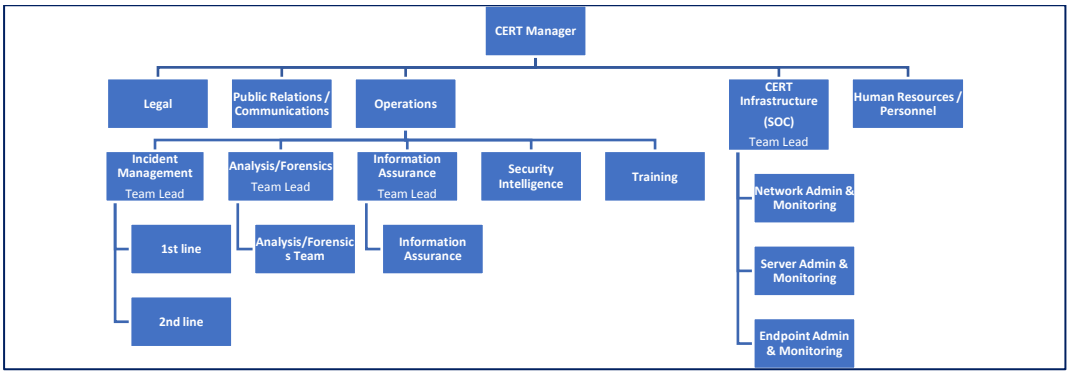

Figure 3 - Proposed CERT/CSIRT organisational structure

2.2.6. As at the time of writing this document, formal legislation relating to cybersecurity/cybercrime has not been passed by the Lebanese parliament. However, given that draft versions of the legislation should be available for review, all personnel required to operate within the bounds of it should use the time to become familiar with these documents.

2.2.7. As discussed in deliverable 1a, the current version of the information security policy document requires review and significant changes to be made in order to be fit for purpose for both technical and non-technical ISF personnel. Once updated, the document will need to undergo review and formal approval by the ISF Director General process prior to issue.

2.2.8. The technical scope of the initial constituency consists of three separate infrastructure networks, these are identified as the main ISF network, the Intelligence Department (ID) network (closed network with no internet access), and a separate ID network providing access to the internet.

2.2.9. The initial capacity assessment carried out in deliverable 1a identified that vulnerability assessments had previously been carried out against some, but not all of the ISF-managed infrastructure. Given the requirement for a stabilised/protected infrastructure from commencement of a CERT/CSIRT & SOC operation (to avoid the potential for constant incident 'fire-fighting') it is vital that all network infrastructure elements (endpoints, servers and network devices) are fully patched/updated. This process of assessment of identified vulnerabilities should therefore be initiated early in phase 0, given the time required for subsequent remediation.

2.2.10. In addition to the vulnerability assessment and post-testing remediation, a separate project should be initiated early in phase 0 to upgrade currently unsupported endpoints running Windows XP on the ISF network. As with section 2.29 above, it is vital to remove multiple known vulnerabilities and mitigate the risk to these devices as part of stabilisation of the constituency's infrastructure in advance of CERT/CSIRT operation.

2.2.11. From a training perspective, the proposed CERT/CSIRT and SOC roles outlined in figure 1 will result in training being required in certain areas. The training requirements and options for training providers and certifications will be discussed further in section 5. It should be noted that this initial training should be completed in advance of commencement of CERT/CSIRT and SOC operations.

2.2.12. With regards to the design of an awareness training programme for ISF personnel, it may be appropriate to engage with external organisations that specialise in provision of cyber security awareness programmes and supporting materials in multiple languages (see sections 5.5.4.5 & 5.5.4.6).

2.2.13. As part of a workshop held in August with the ISF, CyberSouth and CT MENA, a number of suggested options for CERT ticketing and information sharing applications were provided by a visiting team from the Romanian CERT[1]. Detailed analysis of these suggestions should be initiated during phase 0 so that any detailed ISF configuration requirements for these applications can be discussed and confirmed and formally documented. Following completion of a requirements analysis phase, the required applications then need to be installed and configured accordingly, and then tested in advance of

[1] *https://cert.ro*

CERT/CSIRT 'go-live'. It should be noted that the design and implementation of the required applications to support CERT/CSIRT operation will incur costs, which are at this stage unknown.

2.2.14. Alongside the implementation of the CERT/CSIRT-specific applications, any additional applications relating to implementation of the operational SOC should be installed and configured accordingly. As discussed in previous deliverables, both intrusion detection/prevention systems (IDS/IPS) and security incident and event management (SIEM) appliances are currently in the proof-of-concept stage to monitor the Intelligence Department's LANs, and a data centre is currently being built for the separate ISF LAN which will also have these appliances installed. Given the logs extracted from sensors installed on any monitored appliances, including IDS/IPS and SIEM appliances, these will need to be collated and analysed by suitably qualified analysts in the SOC.

2.2.15. Given the importance of standardised documented incident response processes and procedures, consideration should be given to the production of these documents. While a document[2] has been provided by NIST to assist with this task, it is accepted that the ISF may not have the required knowledge to be able to write their own documents, which will result in assistance from external third-party organisations.

2.2.16. With regards to the action plan and activities defined above, it is possible to identify a number of potential 'sub-projects' within the initial phase (phase 0) of the overall CERT/CSIRT implementation programme, given the length of expected activity, potential for technical complexity or the requirement of input from a number of different areas, both internal and external to the ISF. These suggested 'sub-projects are listed below:

a) Vulnerability assessment for ISF and post-assessment remediation
b) Endpoint review/upgrade
c) Co-ordination of technical Training for CERT/CSIRT/SOC personnel
d) Implementation of ticketing and information-sharing applications
e) Development of CERT/CSIRT operational procedures and documentation
f) Implementation of risk assessment
g) Design of training/awareness programme for ISF personnel

2.2.17. Given the importance of the tasks described in phase 0, it is not recommended that the ISF moves to phase 1 (IOC) until all suggested phase 0 tasks (and any additional ones identified during the detailed planning stage) have been completed. While it is accepted that some of the tasks (such as remediation of the results of the vulnerability assessment and upgrade/potential replacement of unsupported endpoints) may take longer than anticipated, moving forward into the next phase would potentially result in multiple alerts generated based on already-known vulnerable devices.

2.2.18. It should also be noted that a potential option for the ISF to is to temporarily exclude areas of known weakness (either whole LANs or specific VLANs/subnets) from the initial 'scope' of infrastructure monitored by the SOC and incident response teams while these areas are remediated. This would reduce the number of 'known' potential positives' and avoid continual 'incident firefighting' by those in the role of the SOC and initial incident response.

[2] *https://resources.sei.cmu.edu/asset_files/TechnicalReport/2004_005_001_14405.pdf*

2.3. Phase 1 – IOC

2.3.1. The timeline and high-level activities for this phase are shown below in figure 4.

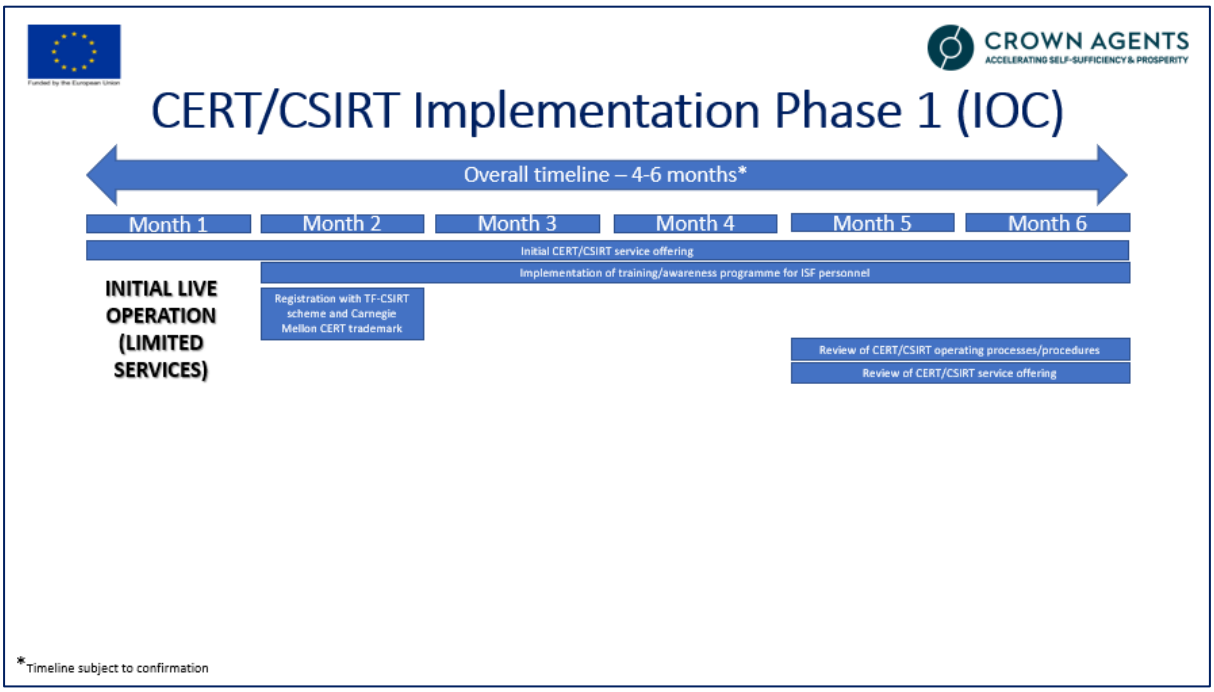

Figure 4 Phase 1 tasks with estimated timeline

2.3.2. Following completion of phase 0, the CERT/CSIRT should be ready to move into an Initial Operating Capability (IOC), providing a limited range of services to its constituency.

2.3.3. As proposed in deliverable 1b, these services are illustrated in figure 5 shown below:

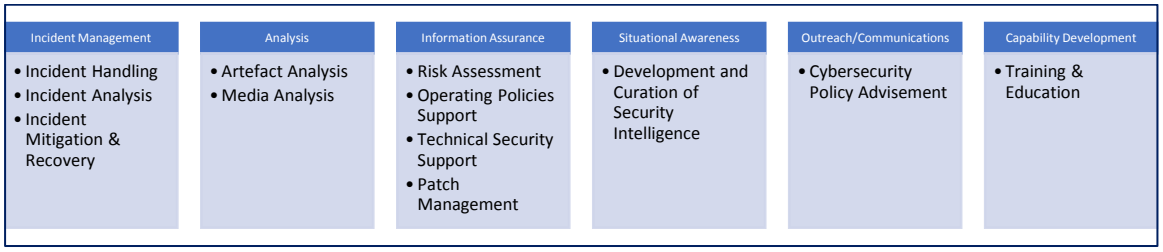

Figure 5 - Suggested initial service offering

2.3.4. Given the technical training undertaken in phase 0, completion of this training will determine the confirmed service offering provided by the ISF's CERT/CSIRT.

2.3.5. From a resource numbers perspective, detailed information is provided in section 3.3, with a summary being provided in appendix A.

2.3.6. In addition to the above services being provided, the training/awareness programme designed in phase 0 should be implemented. This will complement the incident reporting and subsequent investigation service.

2.3.7. Once the CERT/CSIRT has been in initial operation for 2-3 months, applications should be made to both the TF-CSIRT scheme and also for use of the CERT trademark from Carnegie Mellon. This will provide legitimacy to the ISF CERT/CSIRT and provide some measure of visibility of it to other Lebanese government agencies and private sector organisations.

2.3.8. Towards the end of this phase two reviews should be initiated, the first being analysis of the processes and procedures used to manage all reported incidents to date so that they could be amended/updated accordingly. The second review should be concerned with the CERT/CSIRT's service offering to its constituency, to determine whether additional services can be implemented in the next phase of CERT/CSIRT maturity or whether its personnel/resources need to gain additional experience with the current services before expanding the service offering.

2.4. Phase 2 – Continued Operations

2.4.1. The timeline and high-level activities for this phase are shown in figure 6.

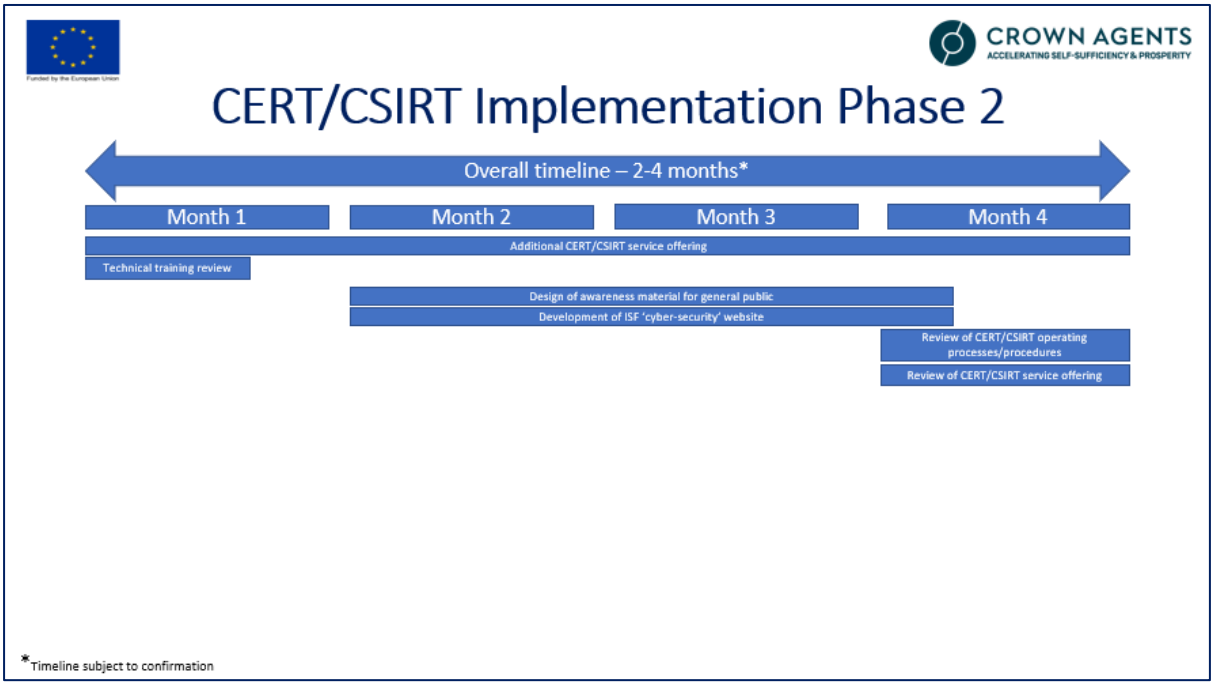

Figure 6 - Phase 2 tasks with estimated timeline

2.4.2. Based on the service review completed at the end of phase 1, additional CERT/CSIRT services may (or may not) be added to the service offering provided to the ISF constituency.

2.4.3. From a resource numbers perspective, detailed information is provided in section 3.4, with a summary being provided in appendix A.

2.4.4. Within the initial month of phase 2 operation, a review should be carried out relating to the CERT/CSIRT relevant technical training completed to date, to determine what (if any) additional training is required in order to develop the knowledge and skill-set of the CERT/CSIRT and SOC personnel. If there is a requirement for further training this should be scheduled considering both resource and course availability, given that the CERT/CSIRT will at this stage be operational.

2.4.5. A major task for this phase is the development of cybersecurity awareness materials for the general public in conjunction of development of a cybersecurity -specific website for the ISF, which will provide functionality in the areas of both awareness and cyber security incident reporting. As with the internal ISF awareness training materials, it may be beneficial to engage with external organisations that specialise in awareness training and production of supporting materials in multiple languages.

2.4.6. As discussed in phase 2.3.7, towards the end of this phase two reviews should be initiated, the first being analysis of the processes and procedures used to manage all reported incidents to date so that they could be amended/updated accordingly. The second review should be concerned with the CERT/CSIRT's service offering to its constituency, to determine whether additional services can be implemented in the next phase of CERT/CSIRT maturity or whether its personnel/resources need to gain additional experience with the current services before expanding the service offering.

2.5. Phase 3 – FOC

2.5.1. As per the proposed timeline for CERT/CSIRT implementation this is the final phase, during which final operating capability (FOC) is attained. The timeline and high-level activities for this phase are shown in figure 7.

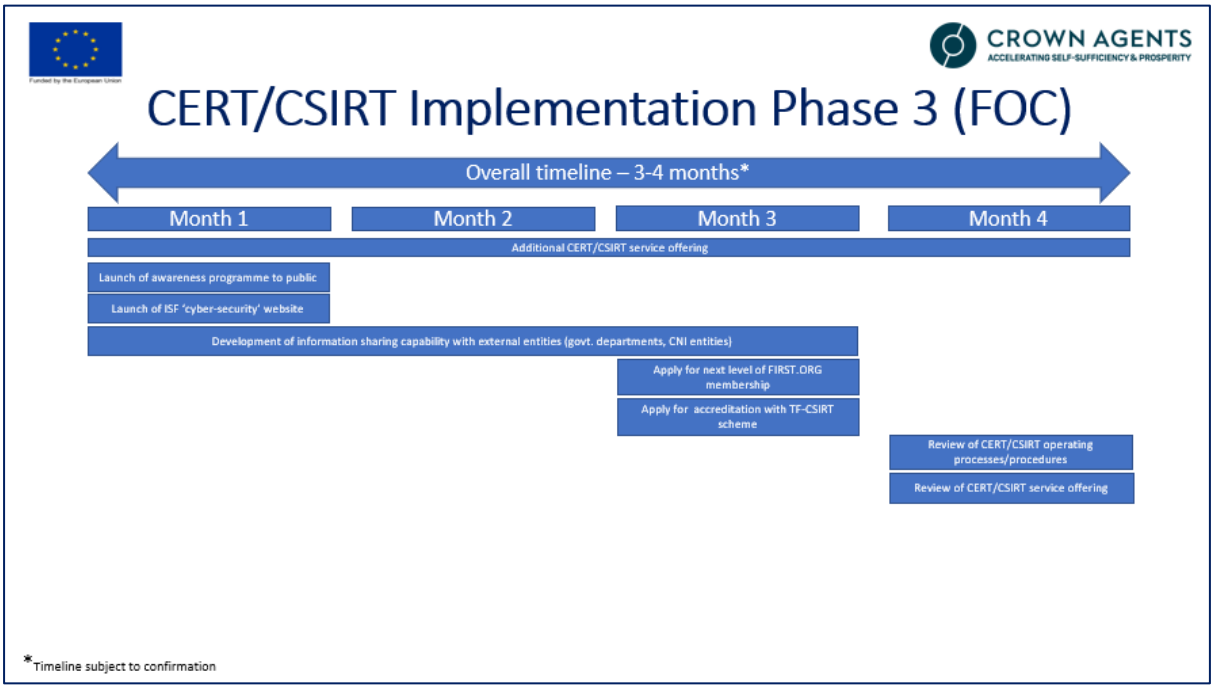

Figure 7 - Phase 3 tasks with estimated timeline

2.5.2. Given that the ISF's CERT/CSIRT should have been operating for between 9-14 months (depending on the duration of previous phases), any additional services that the CERT/CSIRT wishes to provide should be implemented during this phase.

2.5.3. From a resource numbers perspective, detailed information is provided in section 3.3, with a summary being provided in appendix A.

2.5.4. Following development of both awareness materials for the general public and development of the cybersecurity-specific website in the previous phase, both should be released, with co-ordination/involvement from other areas within ISF and also outside of the organisation, such as the media.

2.5.5. Given the level of maturity of the CERT/CSIRT from a capability perspective, it should look to develop a capability for sharing threat information with other Lebanese government organisations, in addition to those entities managing critical national infrastructure (CNI) elements such as transport, utilities, and finance. This will increase the ISF's own threat intelligence capability via a collaborative approach with other key government bodies. Regular workshops and intelligence sharing protocols should be drawn up and implemented to ensure the effective flow of key threat intelligence. As part of this, the ISF should promote its own best-practice to both public and private sector organisations.

2.5.6. Linked to the expected level of operational maturity, the ISF's CERT/CSIRT should apply for the 'full' level of FIRST membership[3]. In addition, and following initial listing with the TF-CSIRT[4] scheme, the ISF CERT/CSIRT should apply for formal accreditation.

[3] https://www.first.org/members/
[4] https://www.trusted-introducer.org/processes/accreditation.html

3. BUDGET ESTIMATION

3.1. Background

3.1.1. Given the majority of tasks identified in section 2 will be carried out by ISF personnel, it makes calculation of costs very difficult.

3.1.2. From a cost perspective, the only charges that are likely to be incurred will be related to those of external consultants engaged to provide support/consultancy to the ISF team as part of the implementation phases identified previously. Additional costs will be incurred relating to attendance at training courses and associated accommodation and travel costs.

3.1.3. In order to provide some additional detail relating to the manpower and effort requirements for the tasks identified in the action plan, each task has been broken down to show expected resource requirements and overall effort, described in terms of the industry standard term of man-days (MD). All information regarding resource numbers should therefore be regarded as an 'estimate'.

3.1.4. It should be noted that the information provided in section 3.2 may well vary once a detailed project plan is produced, a task which does not form part of the three deliverables defined within the overarching terms of reference.

3.2. Phase 0 – Pre IOC

3.2.1. Given the proposed phase 0 activities shown in figure 2, the task information is shown in figure 8 together with resource requirements, expected task duration and total estimated effort.

3.2.2. To calculate the overall man day (MD) effort for each task, the task duration is multiples by the number of expected resources, the sum of which is then multiplied for the FTE[5] figure to provide an overall MD effort.

3.2.3. It should be noted that the information provided is an estimate and is based on the tasks identified in the CERT/CSIRT implementation roadmap. Given the nature of reported incidents, there may be a requirement for increased effort from the forensics teams for example, given that they are 'part-time' resource.

3.2.4. In addition, it does not include specific costs for the following elements which would have to be costed seperately:

a) Vulnerability assessment carried out by external entity
b) External training courses (+ travel/accommodation)
c) Any CERT/CSIRT & SOC application licences and implementation support
d) External implementation consultancy

Task	No. of resources[6]	Expected task duration (working days)	Expected MD effort calculation	Total MD effort for task
Creation of CERT/CSIRT working	3	3	9 ((3 x 3) MD x 0.25 FTE[5])	2.25

[5] Full-time equivalent (FTE) is a unit that indicates the workload of an employed person in a way that makes workloads or class loads comparable across various contexts.
[6] Resources based on the CERT/CSIRT proposed organisational structure shown in figure 3.

group				
Creation of CERT/CSIRT org structure & SOC Team	3	3	9 ((3 x 3) MD x 0.5 FTE[5])	2.25
Familiarisation with legislation	All	ongoing	N/A	N/A
Policy review & update	3	20	10 ((1 x 15) MD x 1.0 FTE[5]) *(1 x author)* 10 (2 x 5) MD x 0.5 FTE[5]) *(2 x reviewer)*	20
Vulnerability assessment & remediation	7	40	30 ((3 x 10) MD x 1.0 FTE[5]) *(3 x testing resources)* 120 ((4 x 30) MD x 0.75 FTE[5]) *(4 x remediation resources)*	120
Endpoint review/upgrade	3	50	150 ((3 x 50) MD x 0.75 FTE[5])	112.5
Training requirements analysis	1	15	15 ((1 x 15) MD x 0.75 FTE[5])	11.25
Technical training	TBC	60	TBC x 1.0 FTE	(TBC)
Ticketing/information sharing application requirements analysis	2	20	40 ((2 x 20) MD x 0.75 FTE[5])	30
Implementation of ticketing and information-sharing applications	4	40	20 ((2 x 10) MD x 0.75 FTE[5]) *(2 x resources)* 20 ((2 x 10) MD x 0.5 FTE[5]) *(2 x resources)*	25
Implementation of CERT/CSIRT & SOC infrastructure, hardware and software	4	50	40 MD x 0.75 FTE[5]) *(2 x resources)* 20 MD x 0.5 FTE[5]) *(2 x resources)*	40
Development of CERT/CSIRT operational procedures and documentation	4	50	30 ((2 x 15) MD x 0.75 FTE[5]) *(2 x author)* 40 ((2 x 20) MD x 0.5 FTE[5]) *(2 x reviewer)*	32.5
Development of working relationships with other CERTS/CSIRTS	2	40	20 (2 x 10) MD x 0.25 FTE[5])	5
Implementation of risk assessment	3	60	30 ((1 x 30) MD x 0.75 FTE[5]) (*1 x resource*) 60 ((2 x 30) MD x 0.5 FTE[5]) (*2 x resources*)	52.5
Design of training/awareness programme for ISF personnel	3	60	40 ((1 x 40) MD x 0.75 FTE[5]) *(1 x author)* 20 ((2 x 20) MD x 0.5 FTE[5]) *(2 x reviewer)*	40

Apply for initial membership of FIRST organisation	1	10	10 ((1 x 10) MD x 0.5 FTE[5])	5
Pre-IOC CERT/CSIRT & SOC process/application testing	6	20	120 ((6 x 20) MD x 1.0 FTE[5])	120

Figure 8 - Expected effort for Phase 0

3.3. Phase 1 - IOC

3.3.1. Given the proposed phase 1 activities shown in figure 4, the task information is shown in figure 9 together with resource requirements, expected task duration and total estimated effort. It should be noted that exact numbers will be determined by the services to be provided by the CERT/CSIRT (which are not yet confirmed, and the table provides a general indication of resource numbers and effort.

3.3.2. The expected effort has been based on a phase 1 length of 6 months (120 working days approx.) *, although it is possible that this phase may only last for 4 months.

3.3.3. It should be noted that the effort calculations of the incident response (IR) team and security operations centre (SOC) team have been based on 24 x 7 operation, approximately 150** working days over 6 months.

3.3.4. The expected effort for supporting teams such as the Legal, PR/Communications and HR/Personnel teams has been based on a minimal level of involvement, although this may increase depending on a potential large -scale incident.

Task	**No. of resources**[6]	**Expected task duration (working days)**	**Expected MD effort calculation**	**Total MD effort for task**
Initial CERT service offering[7]	1) IR team - 6 2) Forensics - 2 3) IA – 2 4) Sec Int – 2 5) SOC – 6 6) Legal – 1 7) PR – 1 8) HR - 1	120*	1) 900 ((6 x 150**) MD x 1.0 FTE[8]) 2) 120 ((2 x 120) MD x 0.5 FTE[7]) 3) 180 ((2 x 120) MD x 0.75 FTE[7]) 4) 120 ((2 x 120**) MD x 0.5 FTE[7]) 5) 900 ((6 x 150) MD x 1.0 FTE[7]) 6) 30 ((1 x 120) MD x 0.25 FTE[7])) 7) 30 ((1 x 120) MD x 0.25 FTE[7]) 8) 30 ((1 x 120) MD x 0.25 FTE[7])	2,310
Implementation of training programme for ISF personnel	1	100	50 ((1 x 100) x 0.50 FTE[7])	

[7] Resources based on the CERT/CSIRT proposed organisational structure shown in figure 3.

[8] Full-time equivalent (FTE) is a unit that indicates the workload of an employed person in a way that makes workloads or class loads comparable across various contexts. 1.0 FTE equates to 100% effort on a task. 0.5 FTE equates to 50% effort.

Registration with TF-CSIRT scheme	1	20	5 ((1 x 10) x 0.50 FTE[7])	50
Review of CERT/CSIRT processes and procedures	3	40	90 ((3 x 30) x .050 FTE[7])	90
Review of CERT/CSIRT service offering	3	40	90 (3 x 30) x .050 FTE	90

Figure 9 - Expected effort for Phase 1

3.4. Phase 2 – Continued Operations

3.4.1. Given the proposed phase 2 activities shown in figure 6, the task information is shown in figure 10 together with resource requirements, expected task duration and total estimated effort. It should be noted that exact numbers will be determined by the services to be provided by the CERT/CSIRT (which are not yet confirmed, and the table provides a general indication of resource numbers and effort.

3.4.2. The expected effort has been based on a phase 1 length of 4 months (80 working days approx.) *, although it is possible that this phase may only last for 2 months.

3.4.3. It should be noted that the effort calculations of the incident response (IR) team and security operations centre (SOC) team have been based on 24 x 7 operation, approximately 120** working days over 4 months.

3.4.4. The expected effort for supporting teams such as the Legal, PR/Communications and HR/Personnel teams has been based on a minimal level of involvement, although this may increase depending on a potential large-scale incident.

Task	**No. of resources**	**Expected task duration (working days)**	**Expected MD effort calculation**	**Total MD effort for task**
Additional CERT service offering[9]	1) IR team - 8 2) Forensics - 4 3) IA – 3 4) Sec Int – 3 5) SOC – 8 6) Legal – 1 7) PR – 1 8) HR - 1	80*	1) 960 (8 x 120**) MD x 1.0 FTE[10] 2) 160 (4 x 80) MD x 0.5 FTE[8] 3) 120 (3 x 80) MD x 0.5 FTE[8] 4) 120 (3 x 80**) MD x 0.5 FTE[8]) 5) 960 (8 x 120**) MD x 1.0 FTE[8]) 6) 20 (1 x 80) MD x 0.25 FTE[8]) 7) 20 (1 x 80) MD x 0.25 FTE[8]) 8) 20 (1 x 80) MD x 0.25 FTE[8])	2,380
Technical training	2	15	30 ((2 x 15) x 0.5	30

[9] Resources based on the CERT/CSIRT proposed organisational structure shown in figure 3

[10] Full-time equivalent (FTE) is a unit that indicates the workload of an employed person in a way that makes workloads or class loads comparable across various contexts.

review			FTE[8])	
Design of awareness material for general public	2	50	50 ((2 x 50) x 0.50 FTE[8])	50
Development of ISF 'cyber-security' website	2	50	50 ((2 x 50) x 0.50 FTE[8])	50
Review of CERT/CSIRT processes and procedures	3	30	45 ((3 x 30) x .050 FTE[8])	90
Review of CERT/CSIRT service offering	3	30	45 ((3 x 30) x .050 FTE[8])	90

Figure 10 - Expected effort for Phase 2

3.5. Phase 3 – FOC

3.5.1. This is the final suggested phase of the CERT/CSIRT implementation. At this stage all required services are now being provided to the previously identified constituency of the ISF organisation.

3.5.2. Given the proposed phase 3 activities shown in figure 7, the task information is shown in figure 11 together with resource requirements, expected task duration and total estimated effort. It should be noted that exact numbers will be determined by the services to be provided by the CERT/CSIRT (which are not yet confirmed, and the table provides a general indication of resource numbers and effort.

3.5.3. The expected effort has been based on a phase 1 length of 4 months (80 working days approx.) *, although it is possible that this phase may only last for 3 months.

3.5.4. It should be noted that the effort calculations of the incident response (IR) team and security operations centre (SOC) team have been based on 24 x 7 operation, approximately 120** working days over 4 months.

3.5.5. The expected effort for supporting teams such as the Legal, PR/Communications and HR/Personnel teams has been based on a minimal level of involvement, although this may increase depending on a potential large-scale incident.

Task	No. of resources[11]	Expected task duration (working days)	Expected MD effort calculation	Total MD effort for task
Additional CERT service offering[11]	1) IR team - 9 2) Forensics - 5 3) IA – 4 4) Sec Int – 4 5) SOC – 9 6) Legal – 1 7) PR – 1 8) HR - 1	80*	1) 1080 ((9 x 120**) MD x 1.0 FTE[12]) 2) 300 ((5 x 120) MD x 0.5 FTE[12]) 3) 240 ((4 x 120) MD x 0.5 FTE[12]) 4) 300 ((4 x 150**) MD x 0.5 FTE[12])	3,060=

[11] Resources based on the CERT/CSIRT proposed organisational structure shown in figure 3

[12] Full-time equivalent (FTE) is a unit that indicates the workload of an employed person in a way that makes workloads or class loads comparable across various contexts.

			5) 1080 (9 x 120) MD x 1.0 FTE[12]) 6) 20 (1 x 80) MD x 0.25 FTE[10]) 7) 20 (1 x 80) MD x 0.25 FTE[10]) 8) 20 (1 x 80) MD x 0.25 FTE[10])	
Launch of awareness programme to public	2	20	30 (2 x 20) * 0.75 FTE[10]	30
Launch of ISF 'cyber security' website	2	20	30 (2 x 20) * 0.75 FTE[10]	30
Development of information sharing capability	2	60	120 (2 x 60) x 0.5 FTE[10]	120
Apply for next level of FIRST membership	1	20	5 (1 x 20) x 0.25 FTE[10]	5
Apply for accreditation with TF-CSIRT scheme	1	20	5 (1 x 20) x 0.25 FTE[10]	5
Review of CERT/CSIRT processes and procedures	3	30	45 (3 x 30) x .050 FTE[10]	45
Review of CERT/CSIRT service offering	3	30	45 (3 x 30) x .050 FTE[10]	45

Figure 11 - Expected effort for Phase 3

4. KEY STANDARDS AND FRAMEWORKS FOR INFORMATION SECURITY

4.1. Overview

4.1.1. To facilitate the establishment of a CERT/CSIRT and the implementation of a full-service offering to its constituency, a multitude of standards, frameworks and models exist which can be utilised to provide assistance to the ISF.

4.1.2. As discussed below, a number of standards, frameworks and codes of practice exist which can be used to assist the ISF in the design, implementation and operation of its incident management capability.

4.1.3. It should be noted that while the majority of the publications discussed below are free to use, the ISO documents require purchase.

4.2. Incident Management

4.2.1. ISO 27035-1: 2016 Principles of incident management[13] – the 27035 standard covers all aspects of incident management. The 27035-1 document covers the basic concepts and techniques of incident management and provides a structured approach to dealing with incidents.

4.2.2. *ISO 27035-2: 2016 Guidelines to plan and prepare for incident response*[14] – the 27035-2 document provides further information regarding the overall incident management process, and provides detailed steps to creation, testing and review of incident management plans.

4.2.3. *NIST SP800-61 Computer Security Incident Handling Guide*[15] – produced by the US National Institute of Science & Technology (NIST), this publication provides information relating to the organisation and operation of an incident response capability and process for handling an incident. The high-level stages are illustrated in figure 7.

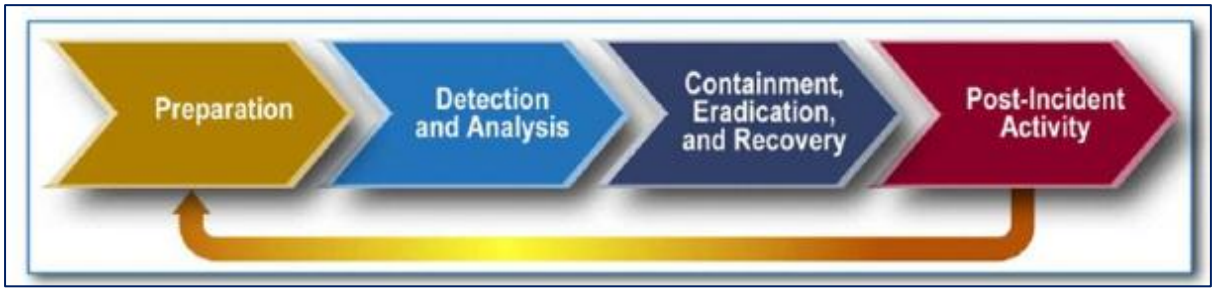

Figure 12 - Steps of Incident Handling. Source: NIST

4.2.4. *NIST SP800-83 Guide to Malware and Incident Prevention*[16] - this NIST publication discusses both malware incident prevention and subsequent response following emergence of an incident.

4.2.5. *TI CSIRT Code of Practice (CoP)*[17] – while not regarded as a standard, the CoP developed by the Trusted Introducer scheme should be adopted by the ISF CERT/CSIRT as part of developing 'best-practice' operations.

[13] https://www.iso.org/obp/ui/#iso:std:iso-iec:27035:-1:ed-1:v1:en
[14] https://www.iso.org/obp/ui/#iso:std:iso-iec:27035:-2:ed-1:v1:en
[15] https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf
[16] https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50875
[17] https://www.trusted-introducer.org/TI-CCoP.pdf

4.2.6. *Traffic Light Protocol (TLP)*[18] - the TLP system is used in conjunction with the information sharing process and provides standardised designations for potentially sensitive information. It utilises 4 different colours as shown in figure 9, going from the use of TLP: WHITE which permits unlimited disclosure up to TLP: RED signifying no disclosure beyond the initial distribution/recipient list.

Figure 13 - The levels of the Traffic Light Protocol

4.3. Forensics

4.3.1. *ISO 27037: 2012 Guidelines for identification, collection, acquisition and preservations for digital evidence*[19] - this document provides guidelines with respect to the entire digital evidence handling process and provides organisations with assistance to facilitate in situations where disciplinary procedures are required.

4.3.2. *NIST SP800-86 Guide to Integrating Forensic Techniques into Incident Response*[20] – this document provides a comparatively generic guide to incident forensics and generic processes and challenges related to the acquisition of forensic information from digital devices. It should be noted that this document was not written primarily for law enforcement, as opposed to those referenced in 6.3.2 and 6.3.3.

4.3.3. *US Department of Justice - Investigations involving the Internet and Computer Networks*[21] - although written primarily for US law enforcement agencies, this document outlines the procedures to be followed as part of any investigation involving the use of any computer network including the Internet.

4.3.4. *US Department of Justice – Electronic Crime Scene Investigation: A Guide for First Responders*[22] - as with the document discussed in section 4.3.2, this document was written primarily for US-based law enforcement agencies and particularly those who will need to secure and preserve and electronic crime scene and secure digital evidence.

4.4. Risk Management

4.4.1. *ISO 27005: 2018 Information Security Risk Management*[23] - this document provides guidelines and best-practice where risk management activities are concerned. It supports the concepts documented in ISO 27001 and can be

[18] https://www.trusted-introducer.org/ISTLP.pdf
[19] https://www.iso.org/standard/44381.html
[20] https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50875
[21] https://www.ncjrs.gov/pdffiles1/nij/210798.pdf
[22] https://www.ncjrs.gov/pdffiles1/nij/219941.pdf
[23] https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:en

used to assist the successful implemented of an information security management system (ISMS).

4.4.2. *NIST SP800-30 Guide to Conducting Risk Assessment* [24] - illustrated in figure 19, this document can be used to provide organisations with guidance in the area of risk management. As with other NIST documents in the SP-800 family, this document was originally designed for use with US-based government (federal) organisations, this publication can also be used with non-US organisations.

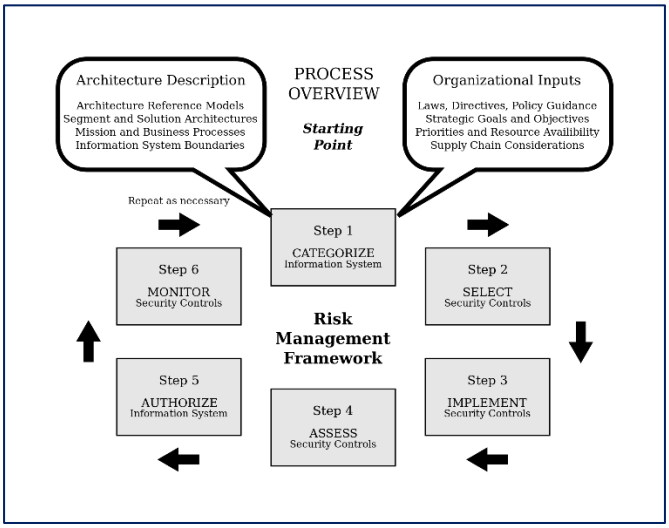

Figure 14 - The Risk Management process according to NIST SP800-30. Source: Cybrary.it

4.5. Security Management

4.5.1. *ISO 27001: 2013 Information Security Management Systems (ISMS) Requirements*[25] - together with the supporting code-of practice document ISO 27002: 2013[26], the 27001 standard covers the requirements for establishment, ongoing maintenance and continual improvement of an ISMS – the detail is shown in figure 8. Given the current levels of maturity concerning security management by the ISF, it is recommended that this document (together with ISO 27002) is used to provide direction for management of information/cyber security within the organisation, following initial review of the IASME standard (discussed in section 4.4.3). It should be noted that a member of the IFS's CERT committee holds a personal certification as an ISO 27001 Lead Auditor - the ISF should utilise organisational knowledge of this standard and provide training in this area to additional personnel to develop core knowledge in the area of ISMS implementation and management/audit.

[24] https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
[25] https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:en
[26] https://www.iso.org/standard/54533.html

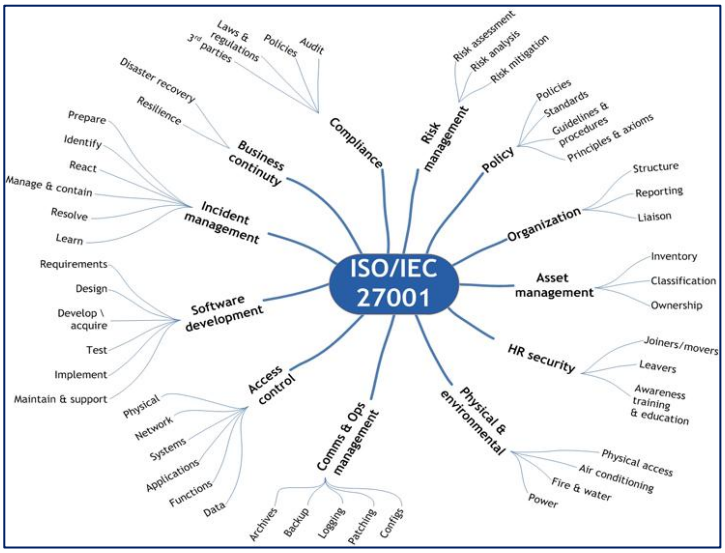

Figure 15 - ISO 27001 elements of an ISMS. Source IT Security.org

4.5.2. *ISO 27032 – Information Technology – Security Techniques – Guidelines for Cybersecurity*[27] - whilst not a 'standard' this document provides guidelines and best-practice security baseline activities for organisations looking to improve cybersecurity.

4.5.3. *NIST SP800-53 Security and Privacy Concerns for Federal Information Systems and Organisations*[28] - although primarily produced for US federal organisations, this standard can be used with all organisation types and with non-US organisations. Shown below in Figure 15, it is comparable to the combination of the ISO 2700/27002 documents. To differentiate between the 800-53 and 27001 standards, NIST produced a comparison document.[29]

IDENTIFIER	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

Figure 16 - The Family of SP800-53 controls. Source: NIST

[27] https://www.iso.org/standard/44375.html
[28] https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
[29] http://gocs.info/pages/fachberichte/archiv/178-sp800_53_r4_appendix-h_draft_ipd.pdf

4.5.4. *NIST SP 800-100 Information Security Handbook: A Guide for Mangers*[30] - this document provides information in many areas of both risk and security management, including governance, awareness/training, implementation of performance/metric measurements, security planning and incident response.

4.5.5. *NIST Cybersecurity Framework (CSF)* – the CSF, illustrated in figure 16, consists of a number of guidelines and practices which can be used to promote protection of critical infrastructure and cybersecurity. Consisting of three main components (core, tiers and profile) the CSF provides organisations with activities and context within which to implement security controls, and to align their security-related activities with organisational-wide objectives, risk appetite and resources.

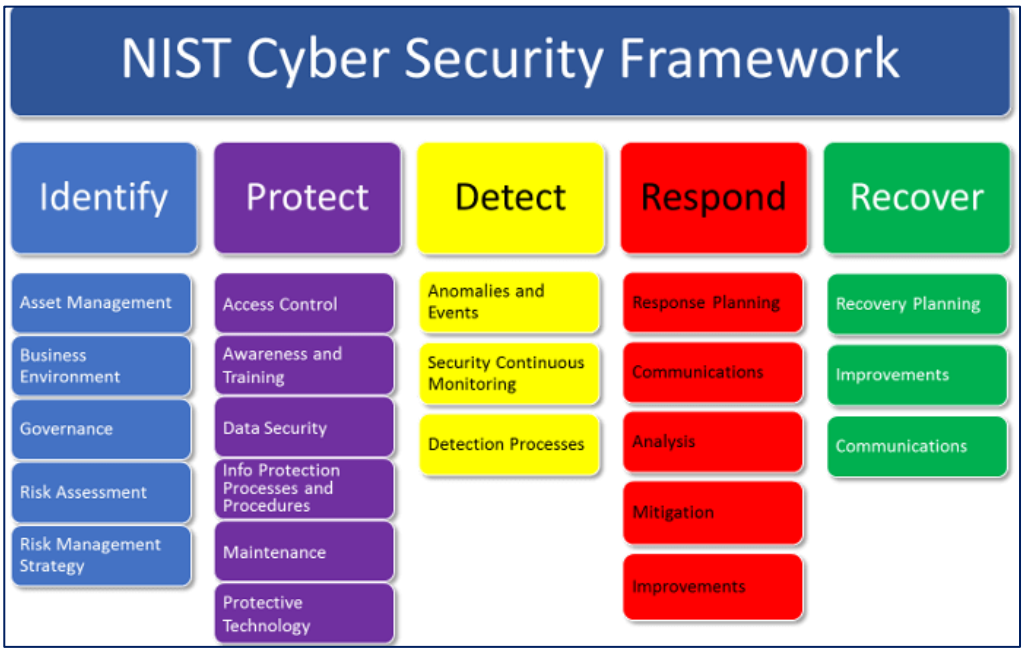

Figure 17 - the NIST Cybersecurity Framework elements. Source: NIST

4.5.6. *IASME Governance standard*[31] - produced by the UK's IASME organisation, this standard (shown in in figure 17) provides information for organisations looking to implementation a security governance process which will assist with ongoing management of security. It also provides a first step to eventual implementation and certification of an ISMS. While initially designed for small and medium size businesses, the standard can be used for business of all sizes and sectors and provide an excellent foundation

30 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf
31 https://iasme.co.uk/the-iasme-standard/free-download-of-iasme-standard/

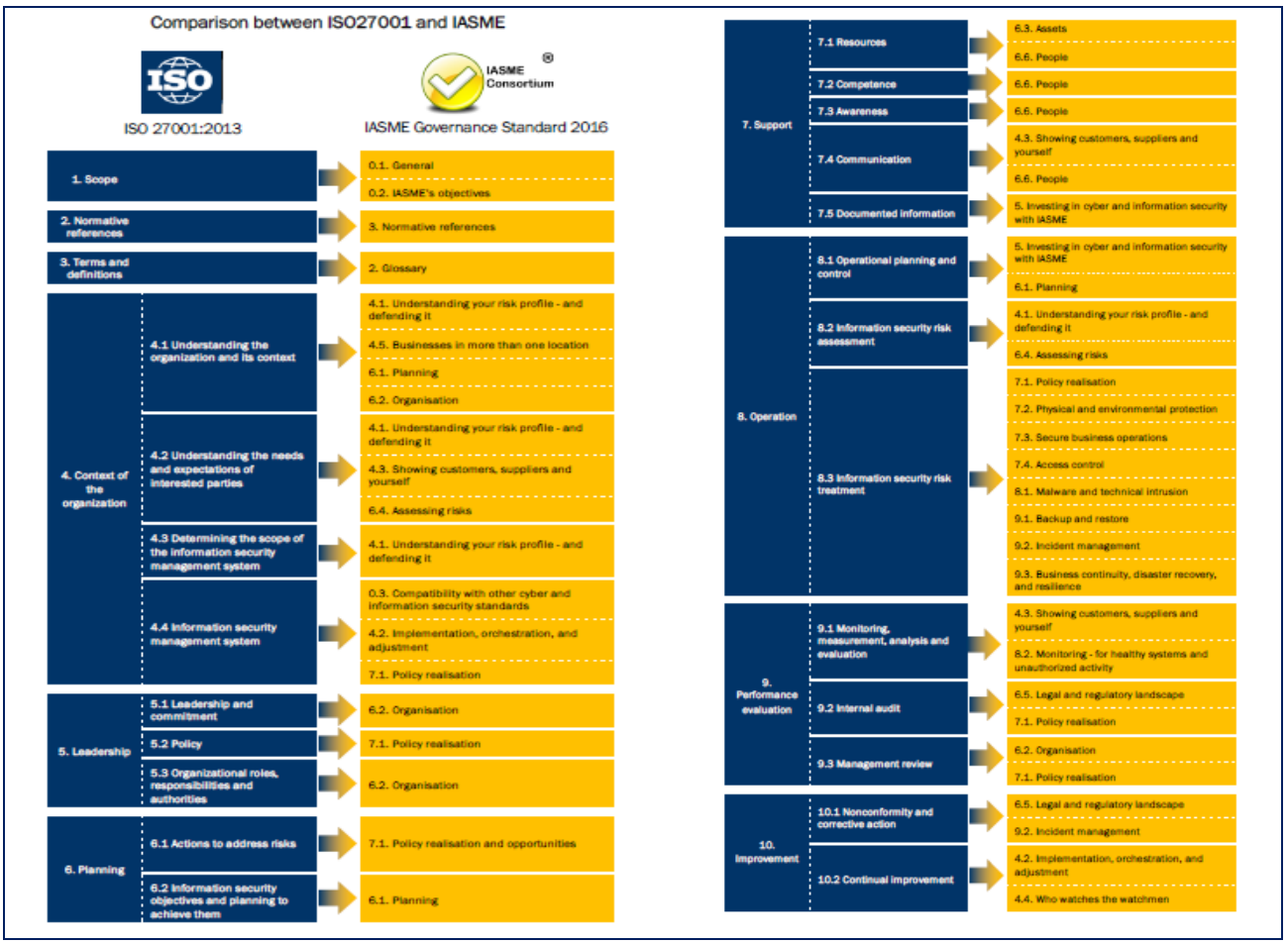

Figure 18 - Comparison between ISO27001 and the IASME Governance standard. Source: Stratia Consulting

4.6. Business Continuity

4.6.1. ISO 27031: 2011[32] *Guidelines for information and communication technology readiness for business continuity* – given the importance of continued readiness for information communication technology (ICT) elements within organisations of all sectors and sizes, this document uses the plan-do-check-act cycle to prevent, detect and manage major incidents resulting in disruption to business operations. In addition to business continuity-related activities, the document can be used as an extension to activities relating to incident response. The various activities within the scope of this document are illustrated in figure 18.

[32] https://www.iso.org/obp/ui/#iso:std:iso-iec:27031:en

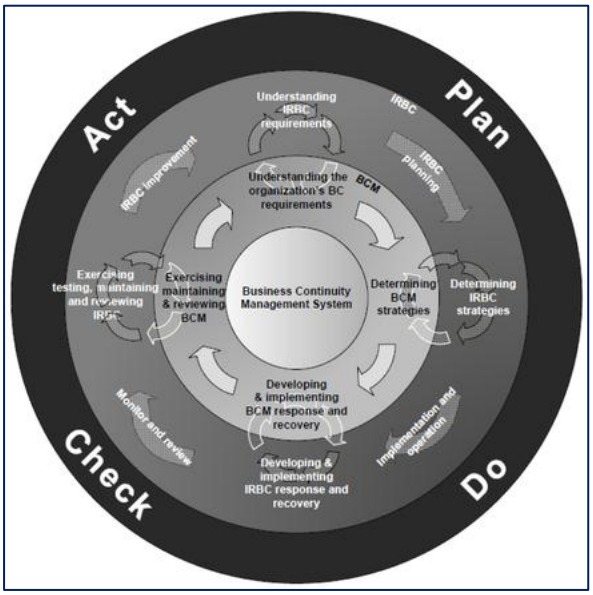

Figure 19 -The PDCA 'loop' showing activities relating to business continuity. Source: ISO

4.6.2. *NIST SP800-34 Contingency Planning Guide for Federal Information Systems*[33] - as with other NIST publications this was originally designed for use by US federal organisations. However, it is possible that this can also be used by non-US organisations by providing best-practice guidelines to assist planning for business and organisational contingency. To support this document, NIST also provides supporting documentation templates, including a Business Impact Analysis[34] template.

[33] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf
[34] https://csrc.nist.gov/CSRC/media/Publications/sp/800-34/rev-1/final/documents/sp800-34-rev1_bia_template.docx

5. TRAINING MASTER PLAN

5.1. Background

5.1.1. As part of deliverable 1a, an assessment was carried out related to the current levels of capability within the ISF in a number of areas relating to information security.

5.1.2. This assessment and subsequent gap analysis confirmed that while the ISF's IT and Security teams have high levels of knowledge and skills in many areas, the requirement exists for acquisition of knowledge and skills in both current areas and new ones, as will be discussed below.

5.1.3. The 'standard' skill and competency requirements of resources utilised in the operation of CERTs/CSIRTs are then reviewed, followed by an overview of relevant industry training and certifications relating to both the establishment and live operation of a CERT/CSIRT.

5.1.4. Based on the information provided, recommendations will then be provided regarding suggested training courses, attendance at which will ensure that the CERT/CSIRT and SOC technical and management resources will have the requisite knowledge and skills to be able to carry out their specialist roles.

5.1.5. It should be noted that in addition to the free/paid training courses discussed in this section, many different organisations run regular webinars in many different areas, which are invaluable for both technical and non-technical personnel to keep up to date with security issues and increase levels of knowledge.

5.2. CERT/CSIRT & SOC Knowledge and Skill Requirements

5.2.1. The CERT vision document (deliverable 1b) contained a proposed organisation structure (shown in figure 20) for the ISF CERT/CSIRT utilising the FIRST framework[35] of service areas and corresponding services.

5.2.2. In addition, the organisation structure also contained suggested numbers of personnel to be assigned to the relevant roles.

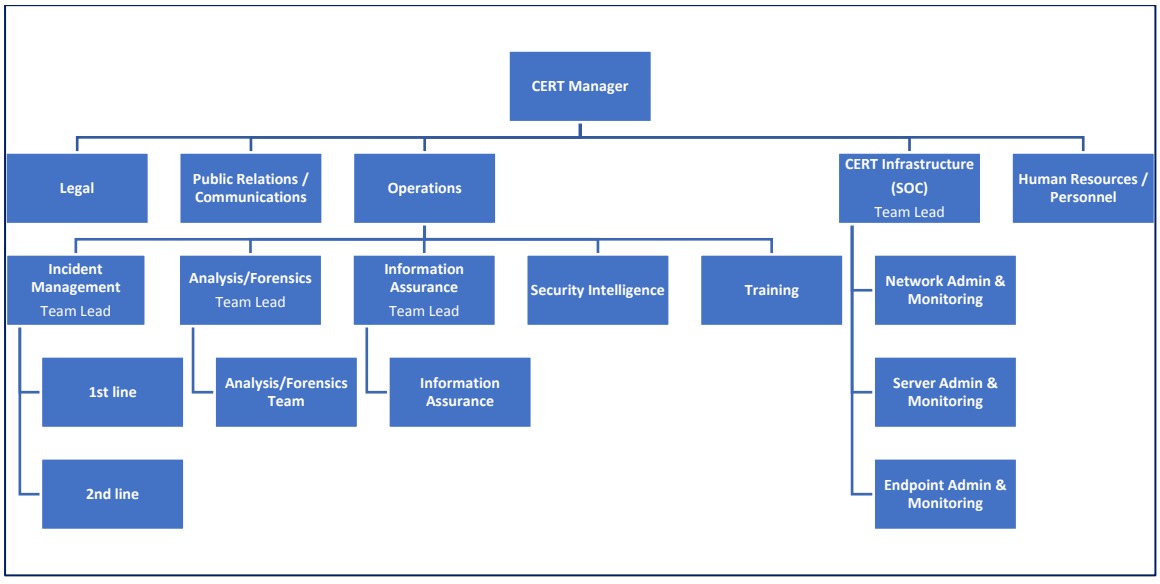

Figure 20 - Proposed CERT/CSIRT organisation structure

[35] https://www.first.org/education/csirt_service-framework_v1.1

5.2.3. Given the suggested services and resource numbers shown above, there is a clear requirement for personnel assigned to the CERT/CSIRT to have high levels of both skills and knowledge in the following areas:

- Incident management
- Analysis/forensics
- Information assurance/risk management
- Security intelligence/information analysis
- Training/awareness material design and delivery
- Network/server/endpoint administration and management

5.2.4. Following a conversation with a UK-based CSIRT, detailed information was provided in terms of the expected skills and competencies required for those working in a CERT/CSIRT and SOC, with a number of identified areas (reactive, compliance, tools/programming languages and proactive). This information is provided in Appendix B.

5.3. Relevant CERT/CSIRT Training Courses and Certifications

5.3.1. Overview

5.3.1.1. Given the many identified elements relating to CERT/CSIRT establishment, initial operation and ongoing management, there are many training courses (some with associated formal certifications) that can aid the ISF when increase the knowledge, skills and abilities of both its technical resources and those who will be managing the CERT/CSIRT and associated SOC.

5.3.1.2. These courses have been divided into the following areas:

a) CSIRT Establishment & Management
b) Incident Management
c) Digital Forensics
d) Threat Intelligence
e) Malware Analysis
f) Penetration Testing
g) Network Defence
h) Network Device Security
i) Operating System Security
j) Risk & Security Management
k) Business Continuity

5.3.1.3. Each area identified in section 5.3.1.2 will now be analysed in further detail, with further information provided related to leading industry training courses and certifications. A summary of all course is provided in Appendix C.

5.3.1.4. It should be noted that the cost information has been provided in some cases by the vendor or certification body and in other cases by a training provider. There is a possibility that the price of a course will differ depending on the training location and provider selected.

5.3.2. CSIRT Establishment & Management

5.3.2.1. *ENISA - Legal and Co-operation*[36]

- This free online training module provides information in the following areas:
  a) Establishing external contacts
  b) Co-operating with Law Enforcement Agencies – Advising in Cyber Crime Cases
  c) Assessment and Testing Communication Channels with CERTS and all their Stakeholders
  d) Identifying and handling cyber-crime traces
  e) Incident handling and co-operation during phishing campaign
  f) Cooperation in the Area of Cybercrime

5.3.2.2. ENISA - Setting up a CSIRT[37]

- This free online training module provides information in the following areas:
  a) Incident handling management
  b) Recruitment of CSIRT staff
  c) Developing CSIRT infrastructure

5.3.2.3. Carnegie Mellon - Creating a Computer Security Incident Response Team[38]

- This course is designed for managers and team leaders who are responsible for implementing a CSIRT and covers the following areas:
  a) Understand the requirements for establishing an effective CSIRT
  b) Strategically plan the development and implementation of a new CSIRT
  c) Highlight issues associated with assembling a responsive, effective team of computer security professionals
  d) Identify policies and procedures that should be established and implemented
  e) Understand various organizational models for a new CSIRT
  f) Understand the variety and level of services that can be provided by a CSIRT
- Course cost $1,100 (classroom-based only).

5.3.2.4. Carnegie Mellon - Managing Computer Security Incident Response Teams[39]

- This course is regarded as a companion to that discussed in section 5.3.2.3.

[36] https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/legal-cooperation
[37] https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/setting-up-a-csirt
[38] https://www.sei.cmu.edu/education-outreach/courses/course.cfm?courseCode=P25
[39] https://www.sei.cmu.edu/education-outreach/courses/course.cfm?courseCode=P28

- The course curriculum provides management insight into technical issues such hiring CSIRT staff, identifying critical information, publishing information, establishing effective working relationships, working with law enforcement, evaluating CSIRT operations, building CSIRT service capacity, and the importance of pre-established policies and procedures.
- Course cost $3500 (classroom-based only).

5.3.2.5. Carnegie Mellon - Overview of Creating and Managing CSIRTS[40]

- In addition to review of the relationship between organisational security management and incident management, this course provides a process-based model for structuring incident management activities and also provides an introductory view of CSIRTs to anyone new in the field.
- Topic discussed in this course include a high-level overview of the key issues and decisions that must be addressed in establishing and maintaining a CSIRT, including CSIRT services as well as key policies, procedures, methods, tools, and infrastructure components that are needed to run a CSIRT.
- Course and exam costs not provided by vendor at time of writing report.

5.3.3. Incident Management

5.3.3.1. ENISA - Operational[41]

- This free online training module provides information in the following areas:
  a) Incident handling during an attack on Critical Information Infrastructure
  b) Advanced Persistent Threat incident handling
  c) Social Networks used as an attack vector for targeted attacks
  d) Writing security advisories
  e) Cost of an ICT incident
  f) Incident handling in live role playing
  g) Incident handling in the cloud
  h) Large scale incident handling

5.3.3.2. TF-CSIRT - TRANSITS I[42]

- Run by the TF-CSIRT organisation, this course is aimed at those who are unfamiliar with the concept of a CSIRT and provides a foundation-level understanding of the main aspects and processes of an incident response team. It provides information in four key areas of a CSIRT operation:
  a) Organisational
  b) Technical
  c) Operational
  d) Legal.

[40] https://www.sei.cmu.edu/education-outreach/courses/course.cfm?courseCode=P68
[41] https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/operational
[42] https://tf-csirt.org/transits/transits-i/

- *Course cost – €1,200* (classroom-based only).

5.3.3.3. TF-CSIRT - TRANSITS II[43]

- Run as a follow-on course to the TRANSITS I course discussed in section 5.4.2.1, this course is aimed at those who have some experience working for/with CSIRTS and provides advanced knowledge in key areas of incident response through a number of separate modules:
  a) NetFlow analysis
  b) Forensics
  c) Communication
  d) CSIRT exercises
- Course cost €1,000 (classroom-based only).

5.3.3.4. Logical Operations – CyberSec First Responder[44]

- This training course has been designed to provide security professionals and incident response teams with the knowledge and skills to be able to analyse threats, design and implement secure environments, to be able to implement proactive defence measures and to deal with cybersecurity incidents.
- Course cost (from approx. $3495), exam cost $300.

5.3.3.5. EC Council - Certified Incident Handler[45]

- This certification course provides attendees with the fundamental skills and knowledge to be able to handle technical security incidents.
- The course curriculum covers many areas, including risk assessment processes, handling multiple incident types, and laws/policies governing incident management.
- Following successful completion of the course and subsequent assessment, candidates are then qualified as Certified Incident Handlers.
- Course cost from $670 (online) and exam costs $199.

5.3.3.6. Carnegie Mellon - Fundamentals of Incident Handling[46]

- This course is designed for those who have not previously been involved in the process of incident handling/response and will be part of a proposed incident response team.
- The main objectives of the course are as follows:

a) recognize the importance of following well-defined processes, policies, and procedures
b) understand the technical, communication, and coordination issues involved in providing a CSIRT service
c) critically analyse and assess the impact of computer security incidents

[43] https://tf-csirt.org/transits/transits-ii/
[44] http://logicaloperations.com/certifications/1/CyberSec-First-Responder/
[45] https://www.eccouncil.org/programs/ec-council-certified-incident-handler-ecih/
[46] https://www.sei.cmu.edu/education-outreach/courses/course.cfm?courseCode=P26

d) effectively build and coordinate response strategies for various types of computer security incidents

- Course cost $5800 (classroom-based training only).

5.3.3.7. Carnegie Mellon - Advanced Topics in Incident Handling[47]

- This course is designed for experienced incident handlers and SOC personnel and addresses advanced techniques for both detection and response to security threats and attacks.
- This course can be used as preparation for the CERT-Certified Computer Security Incident Handler certification as discussed in section 5.4.2.5.
- Course cost $6000 (classroom-based training only)

5.3.3.8. Carnegie Mellon - CERT-Certified Computer Security Incident Handler Qualification Examination[48]

- This examination covers the five major areas of incident handling and provides those who pass the assessment with a formal certification.
- The areas covered in the assessment are as follows:
  a) Protect Infrastructure
  b) Event/Incident Detection
  c) Triage & Analysis
  d) Respond
  e) Sustain

- Exam cost $499.

5.3.3.9. *ISACA – CSX Practitioner*[49]

- This examination tests candidates' abilities to identify and remediate vulnerabilities, implement and configure protective technologies and detect, respond to, and recover from cyber security incidents.
- The exam curriculum is based around the five stages of the NIST Cyber Security Framework as discussed in section 4.4.3.
- Exam cost $400-$500.

5.3.4. Digital Forensics

5.3.4.1. ENISA - Technical[50]

- This free online training module provides both information and tools in the following areas:
  a) Building artefact handling and analysis environment
  b) Processing and storing artefacts
  c) Artefact analysis fundamentals
  d) Advanced artefact handling
  e) Introduction to advanced artefact analysis
  f) Dynamic analysis of artefacts
  g) Static analysis of artefacts

[47] https://www.sei.cmu.edu/education-outreach/courses/course.cfm?courseCode=P23B
[48] https://www.sei.cmu.edu/education-outreach/courses/course.cfm?courseCode=V41
[49] https://cybersecurity.isaca.org/csx-certifications/csx-practitioner-certification#0-about-this-certification
[50] https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational

h) Forensic analysis: Local Incident Response
i) Forensic analysis: Network Incident Response
j) Forensics analysis: Webserver Analysis
k) Developing Countermeasures
l) Common framework for artefact analysis
m) Using indicators to enhance defence capabilities
n) Identification and handling of electronic evidence
o) Building artefact handling and analysis environment
p) Processing and storing artefacts
q) Digital forensics
r) Mobile threats incident handling
s) Mobile threats incident handling (Part II)
t) Proactive incident detection
u) Automation in incident handling
v) Network forensics
w) Honeypots
x) Vulnerability handling
y) Presenting, correlating and filtering various feeds

5.3.4.2. Microsoft - Windows Security and Forensics[51]

- Provided by the Microsoft Virtual Academy, this free online course provides attendees with a general overview of device hacking and the main principle of computer and network forensics.

5.3.4.3. SANS - Windows Forensic Analysis (FOR-500)[52]

- This course provides attendees with the skills and knowledge to be able to carry out the following tasks:
  a) Conduct in-depth forensic analysis of Windows operating systems and media exploitation focusing on Windows 7, Windows 8/8.1, Windows 10, and Windows Server 2008/2012/2016.
  b) Identify artefact and evidence locations to answer critical questions, including application execution, file access, data theft, external device usage, cloud services, geolocation, file download, anti-forensics, and detailed system usage.
  c) Focus your capabilities on analysis instead of on how to use a particular tool.
  d) Extract critical answers and build an in-house forensic capability via a variety of free, open-source, and commercial tools provided within the SANS Windows SIFT Workstation[53].
- Upon successful completion of both this course and associated formal assessment, the certification of GIAC Certified Forensic Examiner is awarded.
- Course cost $6210, exam cost $729.

5.3.4.4. SANS - Advanced Digital Forensics, Incident Response and Threat Hunting (FOR508)[54]

[51] *https://mva.microsoft.com/en-us/training-courses/windows-security-forensics-14383?l=YCKufUQsB_5105244527*
[52] *https://www.sans.org/course/windows-forensic-analysis*
[53] *https://digital-forensics.sans.org/community/downloads*
[54] *https://www.sans.org/course/advanced-incident-response-threat-hunting-training*

- This course provides attendees with the skills and knowledge to be able to carry out the following tasks:
  a) Detect how and when a breach occurred
  b) Identify compromised and affected systems
  c) Perform damage assessments and determine what was stolen or changed
  d) Contain and remediate incidents
  e) Develop key sources of threat intelligence
  f) Hunt down additional breaches using knowledge of the adversary

- Upon successful completion of both this course and associated formal assessment, the certification of GIAC Certified Forensic Analyst is awarded.
- Course cost $6210, exam cost $729.

5.3.4.5. SANS - MAC and iOS Forensic Analysis and Incident Response (FOR518)[55]

- This course provides attendees with the ability to carry out the following tasks:
  a) Mac and iOS Fundamentals: How to analyse and parse the Hierarchical File System (HFS+) and Apple File System (APFS) by hand and recognize the specific domains of the logical file system and Mac-specific file types.
  b) User Activity: How to understand and profile users through their data files and preference configurations.
  c) Advanced Intrusion Analysis and Correlation: How to determine how a system has been used or compromised by using the system and user data files in correlation with system log files.
  d) Apple Technologies: How to understand and analyse many Mac and iOS-specific technologies, including Time Machine, Spotlight, iCloud, Document Versions, FileVault, Continuity, and FaceTime.
- Course cost $6210, exam cost $729.

5.3.4.6. SANS - Memory Forensics in Depth (FOR526)[56]

- This course provides attendees with key skills that are required for digital forensics specialists to be able to carry out live system memory analysis and to be able to capture live memory images.
- Course cost $6210, exam cost $729

5.3.4.7. SANS - *Advanced Network Forensics: Threat Hunting, Analysis and Incident Response (FOR572)*[57]

- This course provides attendees with the tools, techniques and processes required to integrate network evidence sources into investigations.

[55] https://www.sans.org/course/mac-and-ios-forensic-analysis-and-incident-response
[56] https://www.sans.org/course/memory-forensics-in-depth
[57] https://www.sans.org/course/advanced-network-forensics-analysis

- Upon successful completion of both this course and the associated formal assessment, the certification of GIAC Network Forensic Analyst is awarded.
- Course cost $6210, exam cost $729.

5.3.4.8. SANS - Advanced Smartphone Forensics (FOR585)[58]

- This course provides attendees with the skills and knowledge to be able to carry out the following tasks relating to forensics of mobile devices:
  a) Where key evidence is located on a smartphone
  b) How the data got onto the smartphone
  c) How to recover deleted mobile device data that forensic tools miss
  d) How to decode evidence stored in third-party applications
  e) How to detect, decompile, and analyse mobile malware and spyware
  f) Advanced acquisition terminology and free techniques to gain access to data on smartphones
  g) How to handle locked or encrypted devices, applications, and containers

- Upon successful completion of both this course and the associated formal assessment, the certification of GIAC Advanced Smartphone Forensics is awarded.
- Course cost $6210, exam cost $729

5.3.4.9. Carnegie Mellon - Advanced Forensic Response and Analysis[59]

- This course is designed for those with some experience in the area of digital forensics and looks to build on a solid foundational knowledge in this specialist area. Its objectives are as follows:
  a) Prepare for an intrusion investigation, including performing reconnaissance and developing a known toolset
  b) Best practices for responding to an incident and methods to collect the most relevant data to their investigations.
  c) Methods for performing analysis of victim and perpetrator systems. Students will be able to identify malicious applications, correlate system events with file activity, perform runtime analysis of malicious applications and identify resident artefacts subsequent to the intrusion.

- Course cost $3800.

5.3.4.10. Carnegie Mellon - CERT Certificate in Digital Forensics[60] *(online)*

- This online course is designed for experienced system and network professionals and provides a foundation level education in the specialist area of digital forensics
- Course cost $850.

[58] *https://www.sans.org/course/advanced-smartphone-mobile-device-forensics*
[59] *https://www.sei.cmu.edu/education-outreach/courses/course.cfm?courseCode=P103*
[60] *https://www.sei.cmu.edu/education-outreach/courses/course.cfm?courseCode=V34*

5.3.5. Threat Intelligence

5.3.5.1. SANS - Cyber Threat Intelligence (FOR578)[61]

- This course provides attendees with the ability to carry out the following tasks:
  a) Develop analysis skills to better comprehend, synthesize, and leverage complex scenarios
  b) Identify and create intelligence requirements through practices such as threat modelling
  c) Understand and develop skills in tactical, operational, and strategic-level threat intelligence
  d) Generate threat intelligence to detect, respond to, and defeat focused and targeted threats
  e) Learn the different sources to collect adversary data and how to exploit and pivot off of it
  f) Validate information received externally to minimize the costs of bad intelligence
  g) Create Indicators of Compromise (IOCs) in formats such as YARA, OpenIOC, and STIX
  h) Move security maturity past IOCs into understanding and countering the behavioural tradecraft of threats
  i) Establish structured analytical techniques to be successful in any security role

- Upon successful completion of both this course and the associated formal assessment, the certification of GIAC Cyber Threat Intelligence is awarded.
- Course cost $5380, exam cost $729.

5.3.5.2. *Route9b – Cyber Threat Intelligence Analysis*[62]

- This US-based classroom course has been designed to provide knowledge in skills in the areas of collection, analysis and application of targeted cyber intelligence.
- This course teaches the core competencies in this area to provide a rounded education in this area.
- Course cost $4600.

5.3.6. Malware Analysis

5.3.6.1. SANS - Reverse-Engineering Malware: Malware Analysis Tools and Techniques (FOR610)[63]

- Designed for forensic teams, incident responders and IT engineers, this course develops the ability to reverse-engineer malicious software using a number of different tools and utilities.
- Course cost $6210, exam cost $729.

5.3.6.2. Black Hat (USA) – Mac OS Malware Analysis for Reverse Engineers[64]

- This course introduces attendees to the tools and techniques utilised to carry out analysis of malware that targets the Mac OS system.

[61] https://www.sans.org/course/cyber-threat-intelligence
[62] https://www.root9b.com/training/cyber-threat-intelligence-analysis/
[63] https://www.sans.org/course/reverse-engineering-malware-malware-analysis-tools-techniques
[64] https://www.blackhat.com/us-18/training/schedule/#macos-malware-analysis-for-reverse-engineers-9681

- It should be noted that this course was only scheduled to run during the Black Hat USA 2018 event, although it is expected that it will also be run during the 2019 event.
- Course cost from $3400.

5.3.6.3. Black Hat (USA) – Malware Analysis Crash Course[65]

- This course introduces attendees to the tools and techniques utilised to carry out detailed analysis of executable files containing potential malware.
- It should be noted that this course was only scheduled to run during the Black Hat USA 2018 event, although it is expected that it will also be run during the 2019 event.
- Course cost from $3600.

5.3.6.4. Black Hat (Europe) – A Practical Approach to Malware Analysis ad Memory Forensics[66]

- This course provides attendees with knowledge and skills in many areas relating to these two subject areas, including the tools and techniques to carry out malware analysis, how to analyse keylogger, software backdoors, how to acquire a memory image from a live system, an understanding of the methods used by malware to hide from forensic tools and how to determine host and network-based indicators of compromise (IOC).
- It should be noted that this course is currently only scheduled to run during the Black Hat Europe 2018 event, although it is expected that it will also be run during the 2019 event.
- Course cost from approx. $4739.

5.3.6.5. Black Hat (Europe) – Advanced Malware Traffic Analysis: Adversarial Thinking[67]

- This course provides the knowledge and skills to be able to understand the behaviour of malware on a network and to recognise anomalous malware patterns.
- It should be noted that this course is currently only scheduled to run during the Black Hat Europe 2018 event, although it is expected that it will also be run during the 2019 event.
- Course cost from $3424.

5.3.7. Penetration Testing

5.3.7.1. Offensive Security - Metasploit Unleashed[68]

- This online free course provides instruction in the use of the Metasploit application, in addition to providing a reference for penetration testing teams.

5.3.7.2. Offensive Security - Penetration Testing with Kali Linux[69]

[65] https://www.blackhat.com/us-18/training/schedule/index.html#malware-analysis-crash-course-9660
[66] https://www.blackhat.com/eu-18/training/schedule/index.html#a-practical-approach-to-malware-analysis-and-memory-forensics---2018-edition-4-day-10767
[67] https://www.blackhat.com/eu-18/training/schedule/index.html#advanced-malware-traffic-analysis-adversarial-thinking-11921
[68] https://www.offensive-security.com/metasploit-unleashed/
[69] https://www.offensive-security.com/information-security-training/penetration-testing-training-kali-linux/

- This online course introduces multiple ethical hacking tools and techniques and simulates all stages of a full penetration test.
- Upon successful completion of the course and subsequent 24-hour assessment, the certification of 'Offensive Security Certified Professional' is awarded.
- Online course – cost $800 (30-day access).

5.3.7.3. Offensive Security - Wireless Attacks[70]

- Designed for penetration testers and IT administrators, this online course aims to provide attendees with the skills to be able to secure and audit Wi-Fi devices.
- Upon successful completion of the course and subsequent 4-hour assessment, the certification of 'Offensive Security Wireless Professional' is awarded.
- Online course – cost $450 (120-day access).

5.3.7.4. Offensive Security - Cracking the Perimeter[71]

- This online course provides advanced levels of understanding in areas of device and infrastructure weakness and they ways in which vulnerabilities can be exploited.
- Upon successful completion of this course and the subsequent 48-hour exam the certification of Offensive Security Certified Expert is awarded.
- Online course - cost $1200 (including 30-day lab access and exam costs).

5.3.7.5. EC Council - Certified Ethical Hacker[72]

- Aimed at system/network administrators and security professionals, this course aims to provide an overview of the attack strategies, tactics, technology, tools and motivations of criminal hackers.
- Following successful completion of the course and subsequent 4-hour written assessment the certification Certified Ethical Hacker is awarded.
- To provide evidence of practical application of the skills learned on the course, a 6-hour practical assessment can be taken, the certification of 'Ethical Hacker-Practical', being awarded upon successful completion.
- Course cost $2900 (including access to online labs, materials and exam)
- Separate CEH Practical exam cost $550.

5.3.7.6. EC Council - Certified Security Analyst[73]

- The ECSA penetration testing course takes the skills learned in the CEH course discussed in section 5.3.7.5 and develops them further, based on the EC-Council's penetration testing methodology

[70] https://www.offensive-security.com/information-security-training/offensive-security-wireless-attacks/
[71] https://www.offensive-security.com/information-security-training/cracking-the-perimeter/
[72] https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/
[73] https://www.eccouncil.org/programs/certified-security-analyst-ecsa/

- To provide evidence of practical application of the skills learned on the course, a 12-hour practical assessment can be taken, the certification of 'ECSA-Practical', being awarded upon successful completion.
- Course cost $2899, exam cost $600.

5.3.7.7. EC Council - Licenced Penetration Tester[74]

- Following on from the CEH and ECSA courses and certifications, students on this hands-on course are provided with multiple lab-based scenarios and together with a statement of work (SoW) and minimal additional information, are required to carry out a number of testing tasks. The purpose of the course is to try and reflect a 'real' penetration test.
- Course cost $899 (access to online labs and courseware), exam cost $899 (45-day access window to assessment dashboard)

5.3.7.8. CompTIA - Pentest+[75]

- This 2.5-hour online assessment is designed to test candidates in many areas of penetration testing and vulnerability assessment and ensure that those passing the assessment have the knowledge and skills required to determine the resiliency of networks, infrastructure and devices against potential attack.
- A supporting 3-day course can be taken if required.
- Course cost $3250 (including exam). Standalone exam cost - $346

5.3.7.9. Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques (SEC642)[76]

- This advanced course is aimed at security testing professionals and teaching the skills and knowledge required to carry out testing against web applications. It provides information related to advanced attack techniques and how to defend against them.
- By passing the separate assessment, the certification of GIAC Web Application Penetration Tester is awarded.
- Course cost $6210, exam cost $729.

5.3.8. Network Defence

5.3.8.1. QA – Security Operations Centre Analyst[77]

- Designed to be a foundation level introduction for those new to the structure and activities of a SOC, and covers areas including security management, incident response, security education, security incident and event management (SIEM), vulnerability management and threat detection.
- Course cost $2564.

5.3.8.2. SANS – Managing Security Operations: Detection, Response and Intelligence (MGT517)[78]

- Designed for those responsible for managing SOCs, this course provides information related to the design, implementation, and

[74] https://www.eccouncil.org/programs/licensed-penetration-tester-lpt-master/
[75] https://certification.comptia.org/certifications/pentest
[76] https://www.sans.org/course/advanced-web-app-penetration-testing-ethical-hacking
[77] https://www.qa.com/hot-topics/cyber-security/cyber-security-operations/security-operations-centre-soc-analyst-foundation
[78] https://www.sans.org/course/managing-security-operations-detection-response-and-intelligence

operation of a SOC, including processes and procedures relating to incident management.

- Course cost $5820.

5.3.8.3. SANS – Continuous Monitoring and Security Operations (SEC511)[79]

- The subjects covered within this intermediate/advanced-level course include the design of defensible network architecture, network infrastructure security monitoring, continuous diagnostics and mitigation, and would benefit all ISF personnel assigned to provide SOC monitoring and defence for its network infrastructure.
- Successful completion of the separate assessment leads to the award of GIAC Continuous Monitoring.
- *Course cost $6610, exam cost $729.*

5.3.8.4. EC Council - Certified Network Defender[80]

- Designed for network/security administrators and security analysts, this course focusses on providing attendees with a detailed understanding and practical ability to deal with practical network infrastructure defence and attacks against it.
- It includes provision of the ability to design secure network infrastructure and an understanding of supporting software data transfer technologies and implementation of secure network perimeter devices.
- Course cost $2595, exam cost $350.

5.3.8.5. CompTIA - CySA+[81]

- Regarded as an intermediate course (and subsequent certification following completion of exam) within the CompTIA certification pathway, the Cybersecurity Analyst course focuses on four key areas comprising threat and vulnerability management, security architecture and incident response.
- Course cost $2475, exam cost $346.

5.3.9. Network Device Security

5.3.9.1. Cisco - Understanding Cisco Cybersecurity Fundamentals (SECFNDF)[82]

- This foundation-level course provides attendees with information regarding common security concepts, together with the fundamentals of the applications and supporting infrastructure used within a Security Operating Centre.
- Course cost (from approx. $3595), exam cost $300.

5.3.9.2. Cisco - CCNA Security (210-260 IINS)[83]

- The course curriculum focusses on essential security principles, and using a combination of discussions and lab-based exercises, provides an opportunity for students to learn best-practice

[79] https://www.sans.org/course/continuous-monitoring-security-operations
[80] https://www.eccouncil.org/programs/certified-network-defender-cnd/
[81] https://certification.comptia.org/certifications/cybersecurity-analyst
[82] https://www.cisco.com/c/en/us/training-events/resources/training-services/course-overviews/understanding-cisco-cybersecurity-fundamentals.html
[83] https://learninglocator.cloudapps.cisco.com/GlobalLearningLocator/courseDetails.do?actionType=executeCourseDetail&courseID=6136

concepts and deploy basic security techniques to secure network devices in their own organisations.
- Course cost - (from approx. $3500), exam cost $300

5.3.9.3. *Cisco* - Implementing Cisco Cybersecurity Operations (SECOPS)[84]
- This course focusses on providing the fundamental skills used by an analyst in a SOC, including threat analysis, event correlation, the identification of potentially malicious activity and how to carry out tasks related to incident response.
- Course cost (from approx. $3595), exam cost $300.

5.3.10. Operating System Security

5.3.10.1. *Microsoft – Windows 10 Security in Real Life*[85]
- This free training module (provided by the Microsoft Virtual Academy) covers areas such as device, identity, information and breach protection.

5.3.10.2. *Microsoft - Security Fundamentals MTA (98-367)*[86]
- This course provides attendees with an understanding of a number of security-related topics, including server and endpoint security, security policies, network security, and security layers.
- Course cost from $40 (online) - exam price $85.

5.3.10.3. Microsoft - Securing Windows Server 2016 (70-744)[87]*.*
- This course has been designed to give IT administrators the knowledge and skills to be able to improve the security of the devices that they are responsible for managing.
- Using advanced features/functionality contained within Server 2016, instruction is provided in threat identification and mitigation, how to secure virtualised environments and the use of deployment to provide secure updates, and how to utilise Microsoft encryption tools to secure data.
- Course cost – from (approx. $3000), exam cost $110.

5.3.10.4. Linux Foundation - Linux Security (LFS416)[88]
- Delivered as a live 'online' course, the course curriculum covers multiple areas that are relevant to the security of this open source operating system, and provides recommendations to mitigate any potential security risks.
- Course cost $2950

5.3.10.5. SANS – Securing Linux/Unix[89]
- This course provides guidance and best practice rating to both securing and mitigating potential vulnerabilities and issues that exist on these operating systems.
- Upon successful completion of the separate exam the certification of Certified Unix Security Administrator is awarded.
- Course cost $6610, exam cost $729.

84 *https://www.cisco.com/c/en/us/training-events/resources/training-services/course-overviews/implementing-cisco-cybersecurity-operations.html*
85 https://mva.microsoft.com/en-us/training-courses/windows-10-security-in-real-life-17127?l=Xz1vNy5XD_104300474
86 *https://www.microsoft.com/en-us/learning/course.aspx?cid=40367*
87 *https://www.microsoft.com/en-us/learning/course.aspx?cid=20744*
88 *https://training.linuxfoundation.org/training/linux-security/*
89 *https://www.sans.org/course/securing-linux-unix*

5.3.11. Risk and Security Management

5.3.11.1. *BSi - ISO 27005 Risk Manager*[90]

- Based around the ISO 27001 ISMS standard, this course provides the knowledge and skills to be able to manage an information security risk management process within the framework of both legislative requirements.
- Course cost from $2200 (bootcamp*).

5.3.11.2. (ISC)² - CISSP[91]

- The Certified Information Systems Security Professional (CISSP) course (and subsequent certification following successful completion of the exam) is aimed at experienced security practitioners, auditors, and risk management professionals.
- The course curriculum consists of eight domains covering multiple areas of information security, known as the Common Body of Knowledge (CBK):
  a) Security and Risk Management
  b) Asset Security
  c) Security Engineering
  d) Communications and Network Security
  e) Identity & Access Management
  f) Security Assessment & Testing
  g) Security Operations
  h) Software Development Security

- Course cost – from approx. $6575 (bootcamp* including exam cost), standalone exam cost $699.

5.3.12. (ISC)² - CISSP-ISSAP[92] */ CISSP-ISSEP*[93] */ CISSP-ISSMP*[94]

- Known as CISSP 'concentrations', these certifications build on knowledge attained through education/certification to the CISSP and build more extensive knowledge in particular areas.
- These concentrations are as follows:
  a) ISSAP – Architecture professional
     a. Course cost from $5075 (bootcamp* including exam cost), standalone exam cost $599.
  b) ISSEP – Engineering professional
     a. Course cost from $4750 (bootcamp* including exam cost), standalone exam cost $599.
  c) ISSMP- Management professional, standalone exam cost $599
     a. Course cost from $5075 (bootcamp* including exam cost), standalone exam cost $599.

5.3.12.1. (ISC)² - SSCP[95]

[90] *https://www.bsigroup.com/en-AE/ISOIEC-27001-Information-Security/Training-courses-for-ISO-27001/ISOIEC-270052011-Information-Security-Management-System-ISMS-Risk-Management-Course-/*
[91] *https://www.isc2.org/Certifications/CISSP*
[92] *https://www.isc2.org/Certifications/CISSP-Concentrations#accordionTitle-03684da978474ce1be5e87bcbb71f88c*
[93] *https://www.isc2.org/Certifications/CISSP-Concentrations#accordionTitle-d9d109c1cc3d4785960a065c5ac1dabf*
[94] *https://www.isc2.org/Certifications/CISSP-Concentrations#accordionTitle-d9d109c1cc3d4785960a065c5ac1dabf*
**other course options available*

- The Systems Security Certified Practitioner course (and subsequent certification exam) shows that the candidate has advanced levels of skills and knowledge to be able to implement, manage and monitor devices and infrastructure using industry best-practice processes and procedures.
- Similar to the CISSP, the curriculum consists of a number of different domains, with an emphasis on technical as opposed to management areas:
  a) Access Controls
  b) Security Operations & Administration
  c) Risk Identification, Monitoring & Analysis
  d) Incident Response & Recovery
  e) Cryptography
  f) Network and Communications Security
  g) Systems & Application Security

- Course cost from $6675 (bootcamp* including exam cost), standalone exam cost $599.

5.3.12.2. (ISC)^2 - CCSP[96]

- This course is designed to provide advanced skills and knowledge in the area of data, application and infrastructure management in the cloud, using best-practice policies and procedures.
- Course cost from $6575 (bootcamp* including exam cost), standalone exam cost $599.

5.3.12.3. (ISC)^2 - CSSLP[97]

- Aimed at application development teams, this course provides advanced levels of knowledge and skills relating to the software development life cycle (SDLC) to ensure that applications are developed, tested and managed following security best-practice.
- Course cost from $6675 (bootcamp* including exam cost), standalone exam cost $599.

5.3.12.4. CompTIA - CASP[98]

- An advanced course within its course curriculum, CompTIA's Advanced Security Practitioner (CASP) course builds on knowledge already gained though extended practical industry experience, and equips attendees to be able to apply advanced security principles and implement secure solutions to protect their organisation.
- Course $3695, exam cost $439.

5.3.12.5. CompTIA - Security+[99]

- This course has been designed to provide core knowledge and skills in many areas of security, which can be used to provide a

[95] https://www.isc2.org/Certifications/SSCP
[96] https://www.isc2.org/Certifications/CCSP
[97] https://www.isc2.org/Certifications/CSSLP
[98] https://certification.comptia.org/certifications/comptia-advanced-security-practitioner
*other course options available
[99] https://certification.comptia.org/certifications/security

provide a solid foundation upon which security professionals can develop their careers.

- Course cost from $3250 (bootcamp* including exam cost), standalone exam cost $330.

5.3.12.6. ISACA - CISM[100]

- The Certified Information Security Manager (CISM) course provides security and risk management professionals with a comprehensive understanding of the relationships between 'security' and 'the business' elements of an organisation, so that security programmes can be successfully aligned with wider business objectives.
- CISM demonstrates a deep understanding of the relationship between information security programs and broader business goals and objectives.
- Course cost from $3425 (bootcamp* including exam cost), standalone exam cost $760 (non-ISACA member).

5.3.12.7. ISACA – CRISC[101]

- The Certified in Risk and Information Systems Control (CRISC) course provides advanced information in the areas of design, implementation and monitoring of risk-based information security controls.
- It covers four main areas:
  a) Risk identification,
  b) Risk assessment and evaluation
  c) Risk response and mitigation
  d) Risk control monitoring and reporting
- Course cost from $2325 (bootcamp* including exam cost), standalone exam cost $760 (non-ISACA member).

5.3.13. Business Continuity

5.3.13.1. BSi - Introduction to ISO 22301 Business Continuity Management[102]

- This course is designed to provide attendees with information related to the key concepts of business continuity management (BCM) according to the international ISO 22301 standard.
- Course cost approx. $711.

5.3.13.2. BSi - Implementing an ISO 22301 Business Continuity Management System[103]

- This course teaches best practice and the steps to design and implement a BCM within an organisation, including the creation of relevant policies and supporting procedures/processes.
- Course cost approx. $2325.

5.3.13.3. BSi - ISO 22301 Business Continuity Lead Implementer[104]

---

100 http://www.isaca.org/Certification/Documents/CISM-Certification-Overview_bro_Eng_0217.PDF

101 http://www.isaca.org/Certification/Documents/CRISC-Certification-Overview_bro_Eng_0217.PDF

102 https://www.bsigroup.com/en-GB/iso-22301-business-continuity/iso-22301-training-courses/introduction-to-iso-22301-business-continuity-management/

103 https://www.bsigroup.com/en-GB/iso-22301-business-continuity/iso-22301-training-courses/implementing-an-iso-22301-business-continuity-management-system/

**other course options available*

104 https://www.bsigroup.com/en-GB/iso-22301-business-continuity/iso-22301-training-courses/lead-implementer-iso22301-business-continuity-management-system/

- Leading on from the course outlined in 6.3.1.2, this course is designed to provide appropriate levels of knowledge and skills to lead and manage the implementation of a BCM system.
- Course cost approx. $2584.

5.3.13.4. BSi - ISO 22301 Business Continuity Internal Auditor[105]

- This course is designed for those who are required to plan, manage, conduct and report against an audit of a BCM.
- Course cost approx. $1289.

5.3.13.5. BSi - ISO 22301 Business Continuity Lead Auditor[106]

- This course teaches the knowledge and skills required to lead an ISO22301 audit.
- Course cost approx. $2584.

5.3.13.6. BSi - Business Impact Analysis Training Course[107]

- In advance of creation of a BCM or disaster recovery plan (DRP), this course is designed to provide a practical understanding of the elements which comprise a business impact analysis (BIA).
- Course cost approx. $711.

5.4. Training Recommendations

5.4.1. Overview

5.4.1.1. Based on the assessment of current knowledge, technical competencies and skills outlined in deliverable 1, the assessment concluded that while the ISF's technical teams have a good amount of experience and skills in many areas, requirements exist for technical training in a number of areas outlined below:

a) Incident management processes and procedures
b) Memory forensics
c) Network forensics
d) Malware analysis
e) Network security
f) Apple Mac & Linux operating systems
g) Secure application development

5.4.1.2. Based on the information provided in section 5.3 and given the current levels of knowledge, skills and abilities within the ISF's technical teams, this section provides recommendations regarding training courses that the ISF's CERT/CISRT and SOC teams should attend to ensure that they have the required skills to be able to run at initial operating capability (IOC) in phase 1.

5.4.1.3. While a multitude of different course options have been identified in the previous section (classroom, 'live' online, self-paced online), the first two options provide the most comprehensive training experience for attendees for the majority of courses. It is recommended that self-paced online courses should be used to provide either introductory or refresher training.

[105] https://www.bsigroup.com/en-GB/iso-22301-business-continuity/iso-22301-training-courses/iso-22301-internal-auditor/
[106] *https://www.bsigroup.com/en-GB/iso-22301-business-continuity/iso-22301-training-courses/iso-22301-lead-auditor/*
[107] *https://www.bsigroup.com/en-GB/iso-22301-business-continuity/iso-22301-training-courses/Business-Impact-Analysis/*

5.4.1.4. A final decision as to which courses should be undertaken will be determined by several factors, these being cost, course scheduling and resource availability.

5.4.2. CSIRT Establishment and Management

5.4.2.1. It is recommended that those involved in the establishment of the CERT/CSIRT from a non-technical/management perspective make use of the free training modules provided by ENISA, given that they cover multiple areas and can be completed at any time.

5.4.2.2. While the Carnegie-Mellon courses would be beneficial to those new to the setup of a CERT/CSIRT, there is a cost involved and the courses are not run regularly, so may not fit in with the ISF's schedule.

5.4.3. Incident Management

5.4.3.1. As with section 5.4.2, ENISA provides a free training module in the area of incident management, as discussed in section 5.3.3.1.

5.4.3.2. However, it is recommended that the personnel who will be involved in initiating response to incidents also receive training from another provider. Although the additional training courses are not free, their course curricula will provide far more detail than the free course modules, which will assist the incident response teams in understanding the formal processes, steps and procedures they will need to undertake when the CERT/CSIRT commences operation.

5.4.4. Digital Forensics

5.4.4.1. As with sections 5.4.2 and 5.4.3, the ISF should take advantage of the free ENISA and Microsoft training modules in this area, either as a refresher for those with prior knowledge and experience or as an introduction for those unfamiliar with this specialist area.

5.4.4.2. Given the previously identified knowledge/skill gaps in the ID's forensic team and having reviewed the potential forensics courses available to fill these gaps, it is recommended that personnel working in this area attend the *MAC & IOS Forensic Analysis an Incident Response (FOR 518)* course un by the SANS organisation.

5.4.4.3. In addition, it is recommended that personnel attend SAN's *Memory Forensics in Depth (FOR526*) course, which will provide the knowledge and skills necessary to be able to carry out live device memory analysis tasks in support of larger investigations.

5.4.5. Threat Intelligence

5.4.5.1. Given the limited options available for training courses in this area (online courses provided by Pluralsight, Cybertraining 365 etc. do not cover this subject in any depth), the only alternatives for training are provided by either the course run by the SANS organisation (run in a number of locations worldwide) or the US-only based course run by R9B.

5.4.6. Malware Analysis

5.4.6.1. Following investigations into the available training courses in this area, the number of options is limited to those run by either SANS or the Black Hat (conference-based) organisation.

5.4.6.2. Given that this area is relatively new to the ISF's technical teams, it is recommended that the assigned personnel attend either the *A Practical Approach to Malware Analysis ad Memory Forensics* or *Malware Analysis Crash Course* which will provide the knowledge and skills to be able to carry out this role.

5.4.6.3. However, given the fact that course availability is limited to the scheduling of the Black Hat conference, it may be that given the required schedule for the ISF results in the only available course is that run by SANS.

5.4.7. Penetration Testing

5.4.7.1. Following analysis of current capabilities, it was determined that a number of individuals within the forensics team have significant knowledge, skills and experience in the areas of both defensive and offensive penetration testing operations.

5.4.7.2. To provide refresher training, personnel should make use of the free training modules provided by Cybrary (section 5.5.4.1). For those new to the area of penetration testing and requiring formal education, it is recommended that they attend the EC-Council *Certified Ethical Hacker* course, in addition to taking the CEH-practical assessment.

5.4.7.3. It is recommended at all those working in this area should take advantage of the free Metasploit training module which is provided by Offensive Security which will provide and excellent refresher into the capabilities of this tool.

5.4.7.4. For those with some knowledge and experience in this area who wish to acquire additional skills, it is recommended that they attend one of the several courses provided by Offensive Security. All of these courses are self-paced (albeit over a limited time-frame) and offer an optional timed-assessment which replicates a time-limited 'real' assessment.

5.4.7.5. To provide the required skills to be able to carry out vulnerability assessments and penetration tests against any web-based applications used by the ISF, it is recommended that personnel attend SAN's *Web App Penetration Testing and Ethical Hacking* course.

5.4.7.6. In addition to training, the creation of a virtual/physical testing environment would benefit all members of this team so that tools and techniques could be tested in a safe environment.

5.4.8. Network Defence

5.4.8.1. Dependent on their specific responsibilities in the area of general network defence for the ISFs infrastructure as part of a SOC, it is recommended that personnel new to this area (with a good level of knowledge/skill from a technical perspective) attend *the Managing Security Operations: Detection, Response and Intelligence* course run by SANS. For those who will be managing the SOC, it is suggested that they attend the SANS *Managing Security Operations* course.

5.4.8.2. As an alternative to the SANS courses (given the comparative high cost of this training), personnel could attend either the EC-Council *Certified Network Defender* or the CompTIA *Cybersecurity Analyst* courses.

5.4.9. Network Device Security

5.4.9.1.1. For those managing Cisco network devices and working as part of the proposed ISF SOC, it is recommended that personnel complete either the *Implementing Cisco Cybersecurity Operations* course or *CCNA Security* course.

5.4.9.1.2. For those managing other network devices (such as IDS/IPS appliances, SIEM appliances and firewalls), it is recommended that personnel complete the requisite training courses suggested by the vendor to ensure that they have the appropriate levels of knowledge and skill to secure and manage these devices can analyse the output from them.

5.4.10. Operating System Security

5.4.10.1. Given that the ISF is looking to move all its endpoints to the Microsoft Windows 10 operating system (OS), it is recommended that those who will be supporting/administrating this OS complete the free *Windows 10 Security in Real Life* course and also the online (paid) *Security Fundamentals* course, which will provide a solid foundation when looking to secure the Windows 10 operating system.

5.4.10.2. With regards to security management and monitoring for any Linux/Unix clients used by the ISF, attendance and a suitable training course, such as the Linux Foundation's *Linux Security or* SAN's *Securing Linux/Uni*' is recommended.

5.4.11. Risk and Security Management

5.4.11.1. Given the requirement to formalise risk management processes within the ISF, and considering that a member of the CERT committee already has a formal certification in risk management, it is recommended that additional personnel attend ISACA's CRISC course, which will enable them to gain the appropriate skills to be able to carry all risk management-activities.

5.4.11.2. From a security management perspective, and while not specifically relevant to the creation of a CERT/CSIRT, it is recommended that those in the ISF's IT Security team gain the knowledge and skills provided by the $(ISC)^2$ organisation and CompTIA. While the *Security+* course provides a foundation level of education in this area, the advanced *CISSP* course is suitable for team leaders/management level personnel and will provide considerable detail in the many areas encompassing the information/cyber security discipline. For those requiring additional information in areas of architecture, engineering or management, qualified CISSPs (requiring a successful exam pass) can take further courses and certifications in these areas.

5.4.11.3. For those at the ISF's higher management level who will be managing technical personnel in the field of security and who will not be required to have an advanced level of technical knowledge, ISACA's *CISM* course will be the most suitable.

5.4.11.4. For those involved in application development, attendance at the $(ISC)^2$'s CCSLP course will provide the required level of knowledge in areas of secure application development to ensure that any application

developed by the ISF's in-house application development team will conform to appropriate security standards/frameworks.

5.4.12. Business Continuity

5.4.12.1. Following investigation into suitable training courses in this area and to assist the ISF in formalising its business continuity and disaster recovery (BC & DR) strategy and plans, the BSi's *Implementing and ISO 22301 Business Continuity Management System* is a suitable course for those managing this formal process.

5.5. Training Providers

5.5.1. Overview

5.5.1.1. Given the courses and certifications discussed in section 5.3 and based on the recommendations provided in section 5.4, a number of training providers have been identified which can deliver this training in a number of different formats.

5.5.1.2. It should be noted that this list of organisations is not exhaustive but provides an indication of potential training providers in the marketplace that run a combination of classroom-based, remote 'live', and self-paced courses to provide the required training.

5.5.2. Classroom-based Lebanese Training Providers

5.5.2.1. *New Horizons*[108] – based in Beirut, this company provides classroom training in a wide variety of areas including cybersecurity.

5.5.2.2. *ISF Cyber Academy* – although this is planned as part of a separate project/contract, the implementation of this has not yet progressed further. IT is hoped that once established, this academy will provide training in not just technical areas but also elements of awareness education to all ISF personnel.

5.5.2.3. *Formatech*[109] - based in Beirut (and also Dubai), this company provides training in multiple areas of IT and security.

5.5.3. Classroom-based International Training Providers

5.5.3.1. *KADDB Cyber Security Academy (Jordan*) – currently at the early stages of implementation, it is expected that cyber security training courses will be run from this centre in early 2019. In terms of the expected breadth of courses to be provided, it is expected that *cybersecurity awareness, CISMP, DFIR associate, DFIR practitioner, ethical hacking associate* and *penetration test practitioner* courses will be provided. Additional courses may well be added to the catalogue and are expected to be similar to those currently provided by its training partner, PGI International[110].

5.5.3.2. *SANS (Dubai*[111]*/Abu Dhabi*[112]*/Riyadh*[113]*/Qatar*[114]*)* – given the SANS courses discussed in section 5.3, there are a number of locations in the GCC region that deliver their courses.

[108] https://www.newhorizons.com.lb/
[109] http://www.formatech.com.lb/courses-by-division-it
[110] https://www.pgitl.com/training/all-courses
[111] https://www.sans.org/information-security-training/by-location/emea/dubai-ae
[112] https://www.sans.org/information-security-training/by-location/emea/abu-dhabi-ae

5.5.3.3. *QA training*[115] *(UK)* – based in the UK, QA runs mainly classroom-based training course but also runs courses online through a 'live' simulcast feature. They provide training in many areas of cybersecurity in addition to courses which can result in formal certification (following completion of separate exam/assessment).

5.5.3.4. *InfoSec Institute*[116] - based in the US, this training providers offers classroom-based training in addition to an 'online' option for many of its courses. Similar to QA, they provide training in many areas of cybersecurity in addition to courses which can result in formal certification (following completion of separate exam/assessment).

5.5.3.5. *Simplilearn*[117] - offering both classroom-style and online learning, this company provides courses in many areas, both IT/security and business-related.

5.5.4. Online Training Providers

5.5.4.1. *Cybrary*[118] - the website provides free online training modules in a number of different areas of cyber security, in addition to a number of paid options (for practice labs and practice exams).

5.5.4.2. *SANS online*[119] - to complement the classroom-based courses run by SANS, they also offer a selection of on-demand, simulcast, v-live (evening training) and offline self-study courses.

5.5.4.3. *Pluralsight*[120] - this company provides paid-only online cybersecurity courses, focussing on course areas discussed in section 5.3 which lead to formal certification.

5.5.4.4. *Skillsoft*[121] - as with Pluralsight, this company provides paid-only training courses in many areas of both cybersecurity and general IT, with many training subject areas contained in its course catalogue.

5.5.4.5. Udemy[122] - this online training provider hosts a number of paid courses in different areas of security, including incident handling/response and malware analysis.

5.5.4.6. KnowBe4[123] – specialising in security education and awareness, this provider provides multi-lingual (including French and Arabic) interactive online training modules (using videos, games, posters and newsletters) in aspects of security that are both targeted at and relevant to 'end users' (i.e. those with lower levels of technical knowledge than administrators and technical teams). The training modules cover many different areas including password security, phishing awareness, social engineering, with the length of the visual material being short to retain viewer attention. In

[113] *https://www.sans.org/information-security-training/by-location/emea/riyadh-sa*
[114] *https://www.sans.org/information-security-training/by-location/emea/doha-qa*
[115] https://www.qa.com/hot-topics/cyber-security
[116] *https://www.infosecinstitute.com/courses/*
[117] *https://www.simplilearn.com/cyber-security/*
[118] *https://www.cybrary.it/catalog/*
[119] *https://www.sans.org/online-security-training*
[120] *https://www.pluralsight.com/browse/information-cyber-security*
[121] *https://www.skillsoft.com/content-solutions/it-training-portfolio/it-security-training/*
[122] *https://www.udemy.com/courses/it-and-software/network-and-security/*
[123] *https://www.knowbe4.com/*

addition to paid training and simulation packages, many free tools are also provided for use.

5.5.4.7. Wombat Security[124] - as with KnowBe4, this provider specialises in user education and awareness and provides multi-lingual courses to provide users with the information they need to stay safe when using networked devices. In addition to training modules, supporting tools and simulations are also provided for use.

[124] *https://www.wombatsecurity.com/*

6. CONCLUSIONS

6.1. Summary

6.1.1. Following on from the vision and roadmap discussed in deliverable 1b, this document has provided detailed examination of the relevant tasks, timeline, and training required to implement a CERT/CSIRT for the ISF.

6.1.2. The action plan and timetable identified four major phases which will enable the ISF to movie its CERT/CSIRT from initial operating capability (IOC) to eventual final operating capability (FOC).

6.1.3. In terms of the timeline from phase 1 onwards, it has been designed that way to provide a gradual move from initial operation of the CERT/CSIRT providing limited services to its constituency, to eventually providing a full suite of services.

6.1.4. It should be noted that while the total length of all phases is between 12-18 months, there is the possibility that FOC may be attained sooner once IOC is established and the maturity levels, technical capability, and service offering of the CERT/CSIRT increases.

6.1.5. Within each phase a number of key proposed activities have been identified which are key to the success of both that specific phase and the overall CERT/CSIRT implementation. As part of any project, additional tasks may well be identified as the project progresses, and should therefore be added to the project plan.

6.1.6. As part of this planning process, a number of ‘sub-projects’ were identified (section 2.2.16); it is recommended that these be run as distinct streams of activity under the overall programme/project.

6.1.7. It should be noted that the activities discussed as part of phase 0 (section 2.2) are crucial to initial success of the CERT/CSIRT, given that they establish the solid foundation upon which the incident response team (and supporting specialists) can both respond to and manage incidents in a structured and organised way, with all supporting infrastructure and applications in place.

6.1.8. This foundation and structured processes will avoid the potential for individuals to reactively ‘firefight’ incidents using their own methods.

6.1.9. In terms of being able to provide costs for the CERT/CSIRT implementation project, this task has been made more challenging by the fact that the majority of expected effort is being carried out by ‘internal’ ISF personnel as opposed to wholly by an external project team.

6.1.10. To illustrate the projected effort for each identified task (from section 2) within each phase, a number of different tables have been provided information showing an expected number of resources needed to complete each task together with an estimate of both the individual and combined effort required to complete the task.

6.1.11. Given that the majority of the task effort will be provided by ISF resources, it is expected that there will be some involvement from external resources to provide project support and implementation consultancy, given the ISF’s lack of experience when implementing a CERT/CSIRT.

6.1.12. Once the project plan has been created and all recommended tasks are reviewed in detail, a more detailed requirement for external consultancy support will be identified. The costs for this external support will vary depending on the exact requirement and the organisation/individual providing it.

6.1.13. As part of both the implementation of the CERT/CSIRT and also general security management for the ISF, a number of international standards and frameworks were identified.

6.1.14. These standards were grouped into specific areas (incident management, forensics, risk management, security management and business continuity) so as to clearly identify where they can best benefit the ISF.

6.1.15. Following on from the training requirements identified in earlier deliverables, a training master plan has been provided based on identified roles, available and recommended training courses and training providers.

6.1.16. Based on the identified roles (discussed in section 5.5.2) and services to be provided to the initially identified constituency, a number of courses have been identified provided by a selection of different training providers.

6.1.17. These identified courses have been grouped into a number of areas (CSIRT establishment and management, incident management, digital forensics, threat intelligence, malware analysis, penetration testing, network defence, network device security, operating system security, risk and security management and finally business continuity), so as to aid review.

6.1.18. Following identification of potential training courses, recommendations were then provided as to which course should be undertaken to provide the required knowledge and skills which can fill any gaps identified as part of the initial capability assessment. To aid review, these recommendations are also grouped in the same areas as per the previous section.

6.1.19. Given the recommendations provided, any final decision will be determined on the course schedule, personnel availability, and budget available. While it is accepted that some of the courses recommended are a relatively high cost, these providers are regarded as the best in the industry for providing high-quality courses.

6.1.20. Finally, a number of training providers were identified which could be used to provide the recommended training courses. These providers were identified as being both in and outside of Lebanon.

6.1.21. In addition, a number of online training providers were identified which provide either free or paid training modules. While some training modules are comprehensive and can provide the required knowledge to enable students to take certification exams, others can be used for introduction/refresher training.

6.2. Next Steps

6.2.1. Given the information provided in this and the previous two deliverables (1a & 1b), the ISF should now look to move to the next step and commence a formal programme/project comprising of activities in many areas which will lead to eventual implementation of its CERT/CSIRT.

6.2.2. As part of discussions surrounding the production of these deliverables, it was stated that some of the identified tasks in phase 0 are currently ongoing, and therefore from a timeline perspective it could be stated that phase 0 has already ‘commenced’.

6.2.3. Given that some of the phase 0 tasks are currently in progress, these tasks should be documented in a detailed programme/project plan, under the overall control of an appointed programme/project manager who will report up to the CERT committee.

6.2.4. The programme/project manager will act as a single point of contact (SPoC) for all current/future ISF-related activities relating to the CERT/CSIRT’s

implementation and for any external organisations who will be working with the ISF to provide input/assistance as required.

6.2.5. Given the multiple streams of activity identified (particularly during phase 0), it is recommended that a number of sub-projects be created in order to assist with co-ordination and management of these activities. While there should be one programme/project manager overseeing all activity relating to the CERT/CSRT & SOC creation, a requirement may exist for additional persons to manage these sub-projects. In addition, some of these sub-projects (for example the implementation of incident ticketing or information sharing applications or external vulnerability assessment) will require some input/assistance from external/third party organisations, with some also requiring co-ordination of activities with other project/programme elements.

7. APPENDICES

7.1. Appendix A – Summary of Expected CERT/CSIRT & SOC Resources

Team	Phase 1 IOC	Phase 2	Phase 3 FOC
Incident Response	6	8	9
Forensics	2	4	5
Information Assurance	2	3	4
Security Intelligence	2	3	4
Security Operations Centre (SOC)	6	8	4
Legal	1	1	9
Public Relations	1	1	1
Human Resources/Personnel	1	1	1

7.2. Appendix B - Suggested CSIRT Skills and Competencies

Category	Skill/Competency	
Reactive	Windows Forensics	Disk Imaging
	NTFS/FAT File Systems	Linux/Mac Forensics
	Malware Analysis	Reverse Engineering
	Log Analysis	Memory Forensics
	Network Forensics	Live Response (Single host)
	Enterprise Response (Sweep)	Incident Management
Compliance	ISO27001	Incident Response Plans
	CREST CSIR (computer security incident response)	NIST CSIR (computer security incident response)
	GDPR	ACPO Guidelines for digital evidence[125]
Tools/Languages	Python	Java
	Bash	C (#/++)
	X-Ways	EnCase
	FTK	Autopsy
	Volatility	Redline
	FTK Imager	Splunk
	PowerShell	WMI
	Wireshark	YARA
	Snort	NIDS/NIPS
	Regex	SIFT
	x32dbg/x64dbg/OllyDbg	IDA Pro
	Maltego	REMnux
	Nuix	
Proactive	Vulnerability Assessment	Penetration Testing
	User Awareness Testing	Social Engineering

[125] *http://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf*

7.3. Appendix C - Summary of Training Courses/Costs

Area	Course Title	Course Provider	Cost
CSIRT Establishment & Management	Legal & Co-operation	ENISA	Free
	Setting up a CSIRT	ENISA	Free
	Creating a Computer Security Incident Response Team	Carnegie Mellon	$1100
	Managing Computer Security Incident Response Teams	Carnegie Mellon	£3500
Incident Management	Operational	ENISA	Free
	Transits I	TF-CSIRT	$1000
	Transits II	TF-CSIRT	$1000
	CyberSec First Responder	Logical Operations	From £3495, exam $300
	Certified Incident Handler	EC-Council	From $670 (online), exam $199
	Fundamentals of Incident Handling	Carnegie Mellon	$5800
	Advanced Topics in Incident Handling	Carnegie Mellon	$6000
	CERT-Certified Computer Security Incident Handler	Carnegie Mellon	Exam $499
	CSX Practitioner	ISACA	Exam $400-$500
Digital Forensics	Technical	ENISA	Free
	Windows Security & Forensics	Microsoft	Free
	Windows Forensic Analysis	SANS	$6210, exam $729
	Advanced Digital Forensics, Incident Response and Threat Hunting	SANS	$6210, exam $729
	Mac and IOS Forensic Analysis and Incident Response	SANS	$6210, exam $729
	Memory Forensics in Depth	SANS	$6210, exam $729
	Advanced Network Forensics: threat Hunting, Analysis and Incident Response	SANS	$6210, exam $729
	Advanced Smartphone Forensics	SANS	$6210, exam $729
	CERT Certificate in Digital Forensics	Carnegie Mellon	$850
Threat Intelligence	Cyber Threat Intelligence	SANS	$5380, exam $729
	Cyber Threat Intelligence Analysis	Route9b	$4600

Malware Analysis	Reverse-Engineering Malware: Malware Analysis Tools and Techniques	SANS	$6210, exam $729
	MAC OS Malware Analysis for Reverse Engineers	Black Hat (USA)	$3400
	Malware Analysis Crash Course	Black Hat (USA)	$3600
	A Practical Approach to Malware Analysis and Memory Forensics	Black Hat (Europe)	$4729
	Advanced Malware Traffic Analysis: Adversarial Thinking	Black Hat (Europe)	$3424
Penetration Testing	Metasploit Unleashed	Offensive Security	Free
	Penetration Testing with Kali Linux	Offensive Security	$800
	Wireless Attacks	Offensive Security	$450
	Cracking the Perimeter	Offensive Security	$1200
	Certified Ethical Hacker	EC-Council	$2900, exam $550
	Certified Security Analyst	EC-Council	$2900
	Pentest+	CompTIA	$3250, exam $346
	Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques	SANS	$6210, exam $729
Network Defence	Security Operations Centre Analyst	QA	$2564
	Managing Security Operations: Detection, Response and Intelligence	SANS	$5820
	Continuous Monitoring and Security Operations	SANS	$6610, exam $729
	Certified Network Defender	EC-Council	$2595, exam $350
	CySA	CompTIA	$2475, exam $346
Network Device Security	Understanding Cisco Cybersecurity Fundamentals	Cisco	$3595, exam $300
	CCNA Security	Cisco	$3500, exam $300
	Implementing Cisco Cybersecurity Operations	Cisco	$3595, exam $300
Operating System Security	Windows 10 Security in Real Life	Microsoft	Free
	Security Fundamentals MTA	Microsoft	$40, exam $85
	Securing Windows Server 2016	Microsoft	$3000, exam £110
	Linux Security	Linux Foundation	$2950
	Securing Linux/Unix	SANS	$6610. Exam $729
Risk and Security	ISO 27005 Risk Manager	BSi	$2200
	CISSP	$(ISC)^2$	$6575, exam $699

Management	CISSP-ISSAP	$(ISC)^2$	$5075, exam $599
	CISSP-ISSEP	$(ISC)^2$	$4750, exam $599
	CISSP-ISSMP	$(ISC)^2$	$5075, exam $599
	CCSP	$(ISC)^2$	$6575, exam $599
	CSSLP	$(ISC)^2$	$6675, exam $599
	CASP	CompTIA	$3695, exam $439
	Security+	CompTIA	$3250, exam $330
	CISM	ISACA	$3425, exam $760
	CRISC	ISACA	$2325, exam $760
Business Continuity	Introduction to ISO 22301 Business Continuity Management	BSi	$711
	Implementing an ISO 22301 Business Continuity Management System	BSi	$2325
	Business Continuity Lead Implementer	BSi	$2584
	Business Continuity Internal Auditor	BSi	$1289
	Business Continuity Lead Auditor	BSi	$2584
	Business Impact Analysis Training Course	BSi	$711