ASSESSMENT OF CURENT PRACTICES AND HUMAN CAPACITIES IN INFORMATION SECURITY MANAGEMENT (DELIVERABLE 1a)

v1.0 OCTOBER 2018

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

Version Control

Version	Date	Comments
v0.1	*08/08/18*	*Initial Draft*
v0.5	*20/08/18*	*Draft updated and issued for initial review*
v0.7	*27/08/18*	*Draft updated and issued for secondary review*
v0.8	*13/09/18*	*Draft updated and issued for final review*
v0.9	*25/09/18*	*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 cybersecurity incidents/attacks against its infrastructure.

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

1.1.3. The first of these deliverables relates to an assessment of current practices and resource capacities within the ISF relating to information security management processes and procedures.

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 an independent assessment of current practices within the management of information security, together with an assessment of current resource capabilities.

1.3. Scope

1.3.1. The scope for the capacity and capability assessment covers a number of teams within ISF. These are listed below:

- **ISF (Information Division) department**
  - IT
    - IT administrators
    - Networks
    - IT security
    - Maintenance
    - Development/deployment
    - Archiving/backup
    - Warehouse/inventory
  - Forensics group
    - Digital forensics
    - Open-source intelligence & cyber investigations
    - R&D

- **ISF IT department**
  - Networking
  - Development/deployment
  - Support/maintenance
  - Archiving/backup
  - System administration
  - Warehouse/inventory

- **Cybercrime bureau**
  - Investigations
  - Technical/network analysts
  - Administration

2. RESEARCH METHODOLOGY

2.1.1. Given the well documented information/cybersecurity tenets of confidentiality, integrity, and availability, it should also be recognised that security can also be broken down into three main elements, these being people, process and technology (PPT), illustrated in Figure 1 below:

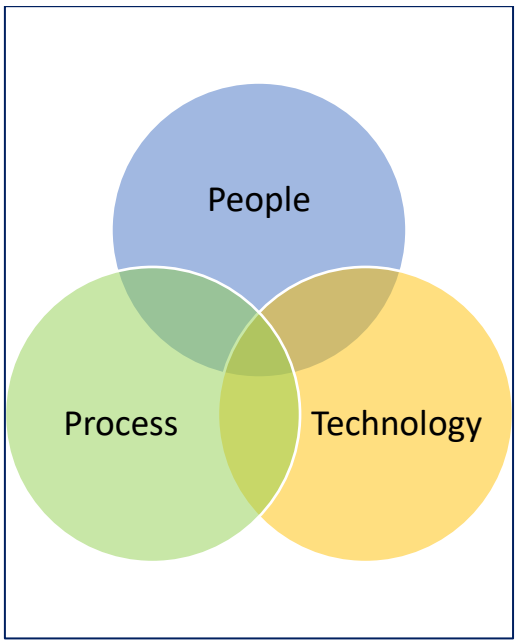

Figure 1 - The 'People/Process/Technology Triad'

2.1.2. As part of the capability assessment for the ISF, all three elements have been considered when carrying out both the initial information gathering and subsequent assessment phase. For security in any organisation to be effective in terms of information/cybersecurity, successful implementation of elements within each area is required.

2.1.3. As part of the discovery phase, an initial meeting was held with Major Mark Sawwan and Captain Claude El Weter to gain initial information relating to the ISF.

2.1.4. Subsequent to this meeting, copies of both the current version (v1.0.0) of the Digital Information Security Policy and the current 'security awareness' document were provided for review. In addition, a number of meetings were scheduled with the members of the CERT committee (shown in Figure 2) to provide further detailed information regarding their specific areas of operation, activities, resources, services and infrastructure.

2.1.5. Follow-up meetings were arranged where necessary to allow for discovery for additional information.

3. ISF ORGANISATION

3.1.1. The ISF employs approximately 30,000 personnel based in multiple locations within Lebanon.

3.1.2. A full organisational chart for the ISF can be found at the following website - http://www.isf.gov.lb/en/menu/19/our_centers

3.1.3. As per the scope identified in Section 1.3, this deliverable is focusing on *specific* departments within the ISF, specifically those provide IT management and security/cybercrime related services to the ISF.

3.1.4. To facilitate management and co-ordination of all activities relating to the establishment of an ISF CERT and other issues relating to security for the ISF, a cybersecurity committee was formed, consisting of seven members. These members represent multiple areas within the organisation who will provide either part-time or full-time resources into the planned ISF CERT.

3.1.5. The cybersecurity committee has a number of responsibilities:

a) To make a risk assessment and implement protection for IT systems
b) To prepare an emergency plan
c) To prepare a plan to create a CERT
d) To create and manage an incident response process
e) To provide a capability to monitor technology and threat intelligence websites and blogs
f) To create an IT security policy

3.1.6. The current capabilities of these teams will be discussed in Section 6. It should be noted that in terms of numbers for each specific team, the number stated represents an approximate estimation of the existing team members and depends on the roles and the responsibilities.

3.1.7. An organisation chart showing the members of this committee is shown below in Figure 2.

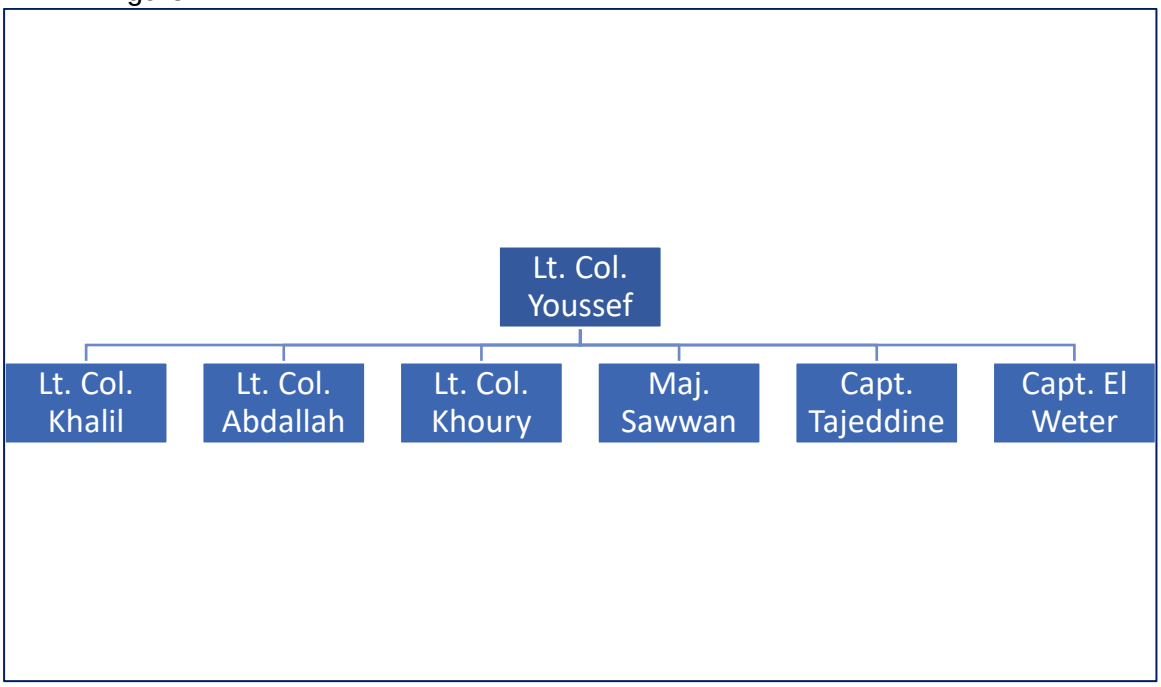

Figure 2 - ISF CERT committee organisation

4. CURRENT IT INFRASTRUCTURE

4.1. While the current IT infrastructure supports communications with all ISF units in the Beirut metropolitan area, only around half of ISF locations outside Beirut are connected to the ISF network infrastructure.

4.2. This means that many units outside of Beirut cannot communicate effectively and securely with ISF HQ, and results in an inability to provide email/web alerts and other information to these regional locations, which can subsequently be provided to those going to the police station. In addition, issues reported by both ISF personnel and the public (to the police stations in person) cannot be communicated by electronic means to a centralised support team.

4.3. Given the current issues impacting the ISF communications infrastructure, the technical design phase for the CERT will need to consider the potential communications infrastructure requirements to ISF locations outside of Beirut, with a separate project being initiated to implement any required infrastructure. This project, managed by the Communications department. has been initiated and is currently in the design phase.

4.4. In terms of the existing network infrastructure, there are a number of separate LANS in place. The ID department manages two LANs which are physically separated (air-gapped), with one of the LANs having no access to the internet. A separate third LAN is managed by the IT team, and provides access to the internet.

5. SECURITY MANAGEMENT

5.1. Governance

5.1.1. Prior to the formation of the ISF cybersecurity committee, there was no formal mechanism within the ISF to provide strategic governance and centralised operational management of cyber/information security. The cybersecurity committee will provide oversight of cybersecurity within the organisation, determine strategy, and provide tactical/operational direction to those implementing and managing information security within the organisation.

5.1.2. All elements included within the scope of the capability assessment (see Section 1.3) manage their own operational IT and security issues at present and have a reporting responsibility up to the General Directorate.

5.1.3. Whilst the ISF Intelligence Department (ID) IT team has a dedicated security team providing technical administration/management for firewall devices, security patching etc., the separate ISF IT team does not have the technical resources, knowledge, or experience to have a dedicated security team in place at present to manage the security-related elements of its infrastructure.

5.1.4. In terms of a governance future-state, this will be discussed as part of the CERT vision document (deliverable 1b).

5.2. Legislation

5.2.1. Relevant legislation relating to cybercrimes is not currently on the statute books of the Lebanese parliament, which makes both investigating and prosecuting cybercrime very challenging. Specific legislation relating to cybercrimes has now been approved and at the time of writing this document (Oct 2018) is due to be placed on the statue books within in the next 2-3 months.

5.2.2. However, the Code of Criminal Procedure (Article No. 328 of 7 August 2001), amended by Law No. 359 of 16 August 2001, currently provides a framework for current cybersecurity investigations.

5.3. Risk Management

5.3.1. From a risk management perspective, it would appear that different approaches are taken to manage information security risks to the ISF. Based on information provided during the discovery phase, it would appear that while some areas of the ISF have a relatively proactive approach to cybersecurity risk management given their level of maturity in this area, others have in many respects have ‘accepted’ potential risks to their information assets given that they are not able to implement appropriate controls to proactively mitigate risk, and are therefore reactive to incidents/attacks against its infrastructure.

5.3.2. This is in the main caused by budgetary, equipment or manpower resource constraints which result in the required technical controls either not being implemented, or that controls implemented cannot be monitored given the lack of suitably qualified resources. In addition, some applications use elements which have not been updated for some time, but are required for the application to work successfully.

5.3.3. At present, there are personnel on the cybersecurity committee who have formal certifications in risk management (ISO/IEC 27005) and information security management systems audit (ISO/IEC 27001), but in order to successfully implement a comprehensive risk management regime within ISF it is recommended that additional personnel from all areas within the scope of this capability assessment undergo formal training in risk management techniques.

This will provide all personnel with a standardised approach to risk relating to the ISF's information assets.

5.3.4. Following the completion of appropriate training courses, extensive information security risk assessments should be carried out (with assistance from external risk specialists as required) to ensure that all critical information assets are identified, potential vulnerabilities and threats assessed, and appropriate logical/technical, administrative and physical controls are implemented as required to mitigate and manage all identified risks accordingly. This process is illustrated below in Figure 3:

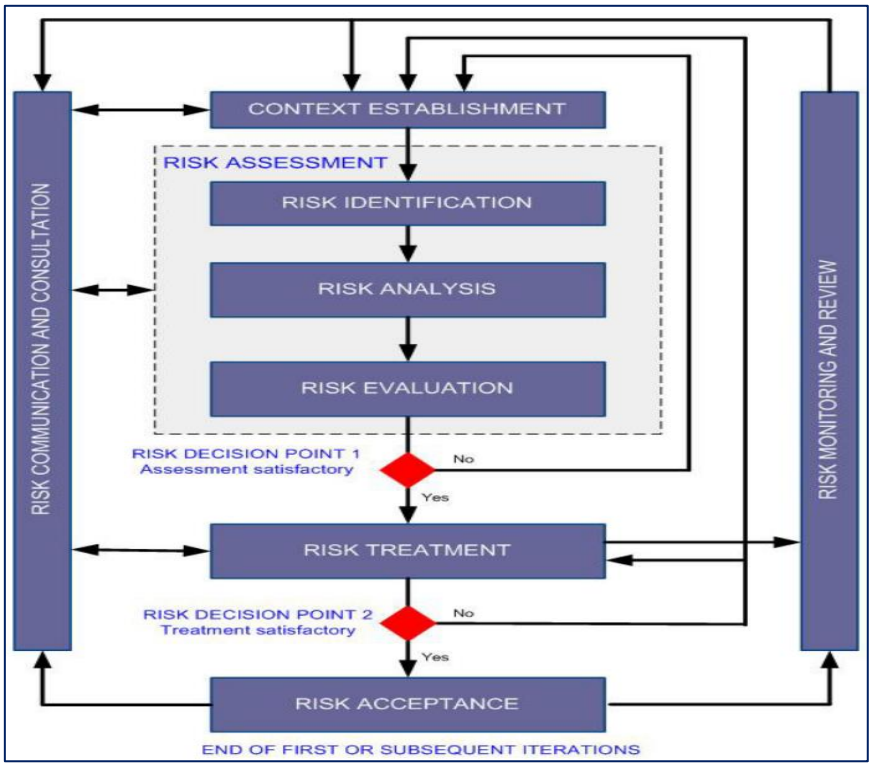

Figure 3 – ISO/IEC 27005 Risk Management Process[1]

5.3.5. The process illustrated above also highlights the requirement for a *continual* risk management process, given the ever-evolving threat environment.

5.3.6. Completion of a detailed risk assessment and subsequent implementation of required logical/technical and administrative controls to manage identified risk will also provide the most cost-effective use of both personnel resources and all implemented controls.

5.3.7. In addition, to the risk assessment process, a risk register should be implemented to provide visibility of all risks to information assets and facilitate ongoing management and review of all controls implemented to mitigate risk.

5.3.8. To ensure successful management of all potential information security risks, the ISF should create a role of senior responsible owner (SRO) also known as a chief risk officer (CRO), to oversee the process. The SRO/CRO will own/manage the risk register and will be responsible for co-ordination of all risk management-

[1] https://www.threatconnect.com/blog/threat-intelligence-within-risk-management/

related actions, including regular risk review and co-ordination of risk management activities.

5.4. Information Sharing

5.4.1. At present, an internal reporting mechanism exists within ISF which provides two-way reporting both up and down both the command structure.

5.4.2. A specific unit (such as the ISF ID dept.) can provide a report (e.g. to report a specific threat they have identified) to the General Directorate (GD). This information will then be disseminated by the GD to other ISF departments as appropriate.

5.4.3. While a number of 'memoranda of understanding' (MOU) exist between ISF and external entities (such as universities), there does not appear to be a platform for sharing information with entities outside of the ISF, such as critical national infrastructure elements (CNI) (financial institutions, electricity, gas, water, fuel, transport), or other government departments. Whilst this is not an initial requirement (given the CERT will be internal to the ISF), as the CERT's capabilities develop this will be a future requirement.

5.4.4. At present, the ISF uses social media to provide information to the general public, with Facebook and Twitter being the primary platforms currently in use. The ISF's website is currently is currently used for incident reporting (see section 5.9), and it is planned that website pages will be setup to provide cybersecurity-related alerts to the public. In addition, a mobile app will be developed to provide this information.

5.4.5. As part of a CERT design, the requirement for internal and external information sharing will need to be considered.

5.5. Policies and procedures

5.5.1. All information security policy documentation should also cascade down from an overarching information security *strategy*, the content of which provides a number of high level objectives. At present, a formal document defining an *ISF-specific* information security strategy does not exist.

5.5.2. While a Lebanese National Security Policy Guidelines[2] document (issued by OMSAR) currently exists, this document does not reference a separate national 'Cybersecurity Strategy' (document does not currently exist) which would document high-level security objectives for the state of Lebanon.

5.5.3. To support the policy guidelines document, a 'cybersecurity checklist'[3] (also issued by OMSAR) is provided to assist organisations with implementing security.

5.5.4. The current version of the ISF Digital Information Security Policy document (v1.0.0 dated Apr 27,2017) issued in May 2017, is comprised of many sections providing both factual and advisory information in multiple areas of IT security.

5.5.5. Given the purpose of the policy is to provide a framework within which information security is managed by the ISF, it would appear that many elements and processes referenced within it have not been implemented to date, but are part of a '*to-be*' future scenario.

[2] *http://www.omsar.gov.lb/Cultures/en-US/ResourcesSupport/SupportAdministration/Pages/NationalCyberSecurityPolicyGuidelines.aspx*

[3] *http://www.omsar.gov.lb/Cultures/en-US/ResourcesSupport/SupportAdministration/Documents/Cyber%20Security%20Checklist%20v1.0.pdf*

5.5.6. This policy document has been approved by the ISF Director-General and has been currently been issued to all ISF departments with responsibility for IT and network infrastructure management.

5.5.7. The current document is 60 pages in length and covers areas as shown below:

a) Security Policy guidelines
b) ISF Data Classification
c) ISF Personnel Classification
d) Access Control
e) Physical & Environmental Security
f) Secure Network Architecture and Network Access Control
g) Business Continuity & High Availability
h) User Responsibilities
i) Practical Security Measures

5.5.8. In order for any policy document to be effective, its content should contain no ambiguity and should contain consequences for policy non-conformance (i.e. measures of disciplinary action). Following review of the ISF security policy document, there would not appear to be any discernable consequences for users if they do not comply with areas such as password complexity/length or using correct data classifications, for example.

5.5.9. Given the extensive content within the current version of the policy document, and the requirement to provide visibility to all personnel using ISF managed devices and supporting network infrastructure, those users with minimal levels of technical knowledge may be overwhelmed with the information contained within it, and therefore not have a full understanding of their individual compliance requirements when accessing ISF networks.

5.5.10. To ensure that all users can have a good level of understanding of the elements directly relating to them, it is recommended these elements have their own individual policy documents as suggested below:

a) Acceptable Use Policy
b) Social Media Policy
c) Password Policy

5.5.11. To ensure clarity regarding other more technical elements discussed in the current version of the policy document, they should also be separated into their own individual policy document, as suggested below:

a) Access Control Policy
b) Physical and Environmental Security Policy
c) Encryption Policy
d) Wireless Policy
e) Network Security Policy
f) Data Classification Policy
g) Configuration Management Policy

5.5.12. Given the existence of the current document providing overall policy direction, it would appear that there are no supporting documents providing more detailed information in terms of practical application of the policy elements i.e. supporting processes and procedures, to ensure compliance to the policy content.

5.6. Compliance/Certification

5.6.1. While some elements of a security management system exist, such as secure network/device configuration and an overarching information security policy, the ISF does not have all the required elements in place to be able to either comply with, be certified against, a formal information security standard such as ISO/IEC 27001[4].

5.6.2. In addition, its risk management processes are not formalised to the extent that they are compliant with the ISO risk management standard, ISO/IEC 27005[5].

5.6.3. At present personal certifications in both ISO/IEC 27001 & 2005 are held by a member of the cybersecurity committee (Capt. El Weter). It would benefit the ISF to increase the number of people with certifications in this area, so as to assist the organisation in becoming initially compliant and eventually certified to internationally-recognised information security and risk management standards.

5.6.4. An alternative to the ISO/IEC standards family is that proposed by the National Institute of Science and Technology (NIST), namely the Cybersecurity Framework[6] (CSF), the core elements of which are shown in in Figure 4.

Figure 4 - The Key Elements of the Cybersecurity Framework - Source: NIST

5.6.5. NIST has similar standards to those of ISO, namely SP 800-53[7] (security standard) and SP 800-37[8] (risk management).

5.6.6. Given the complex requirements of becoming compliant with security standards, it is recommended that the ISF reviews all these standards/frameworks with a view to commencing a compliance project in due course, although it should be noted that these activities would be separate and distinct from those relating to the CERT implementation.

5.6.7. In the short-term, it is recommended that the ISF reviews advice relating to essential 'cyber hygiene' as suggested by the UK government's (National Cyber Security Centre) '10 steps to cybersecurity'[9], and potentially look to become compliant and potentially certified against 'Cyber Essentials'[10], which although a

[4] https://www.iso.org/isoiec-27001-information-security.html
[5] https://www.iso.org/standard/75281.html
[6] https://www.nist.gov/cyberframework/new-framework
[7] https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
[8] https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final
[9] https://www.ncsc.gov.uk/guidance/10-steps-cyber-security
[10] https://www.cyberessentials.ncsc.gov.uk/

foundation-level certification, provides an excellent first-step to further certification against the other standards discussed.

5.7. Security Culture

5.7.1. At present there does not appear to be any significant measure of a security culture within the organisation.

5.7.2. As mentioned in section 6.2 below, a formal and regularly scheduled awareness training programme does not currently exist, which results in ISF personnel not having a level of understanding of the potential threats/risks to them from a cybersecurity perspective.

5.7.3. In addition, a document providing general awareness 'tips' has been produced and issued to all ISF personnel. While this document provides some useful tips, in order to increase users' understanding it would be of benefit to provide some context/background as to *why* they need to carry out particular behaviours i.e. *why* they need to use passwords with a particular length, and *why* they should not follow suspicious links in email, for example.

5.8. Monitoring Capabilities

5.8.1. Current cybercrime analysis activities carried out are related to *post-event* in that following the initial report of an incident, analysis is carried out whether it be through technical means (e.g. device forensics) or through the use of open-source tools/dark-web research to determine the incident source and suspected threat actor.

5.8.2. At discussed further in section 6.3, some network/security monitoring capability is currently in use on ISF networks, from a perspective of general network management, application control, security incident and event monitoring (SIEM), intrusion detection/prevention devices (IDS/IPS) or behavioural monitoring.

5.8.3. However, it should be noted that the monitoring and control capabilities are not used on the entire network infrastructure, resulting in some areas having little or no visibility of unusual/anomalous activity occurring on servers, endpoints or across the network infrastructure.

5.9. Incident Reporting

5.9.1. At present there is a process through which the general public can report a cybercrime incident. Users can go to the ISF website (http://www.isf.gov.lb/en) and select the graphic shown in Figure 5. It should be noted that this website can also be used to report non-cybercrime incidents by selecting the required 'Report Type'.

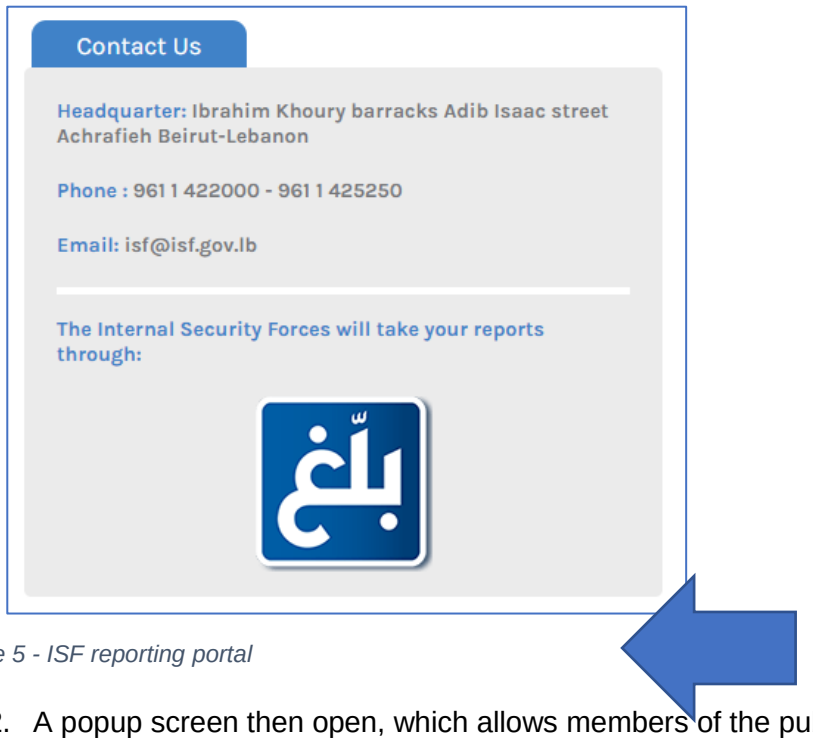

Figure 5 - ISF reporting portal

5.9.2. A popup screen then open, which allows members of the public to report a cybercrime related incident, shown in in Figure 6.

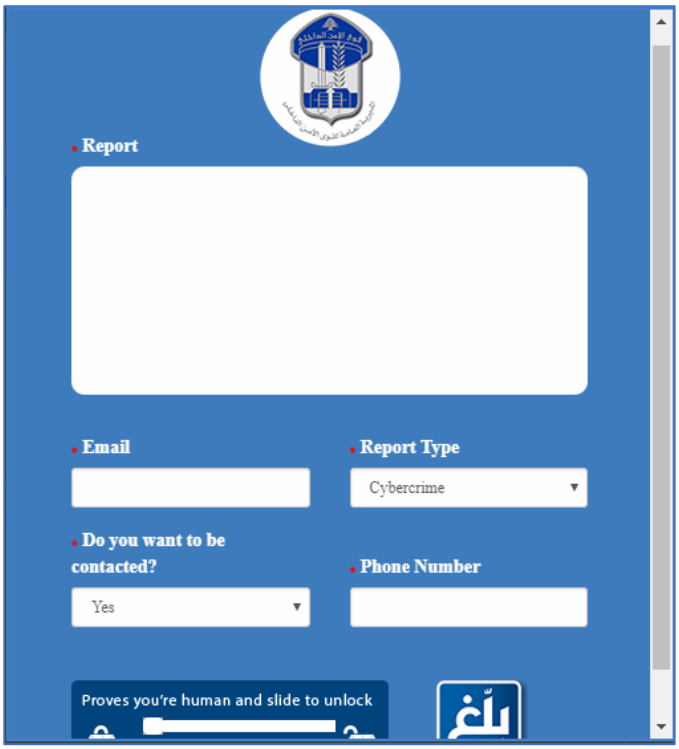

Figure 6 - Cybercrime reporting screen

5.9.3. The process for reporting/investigating a cybercrime is shown in Figure 7:

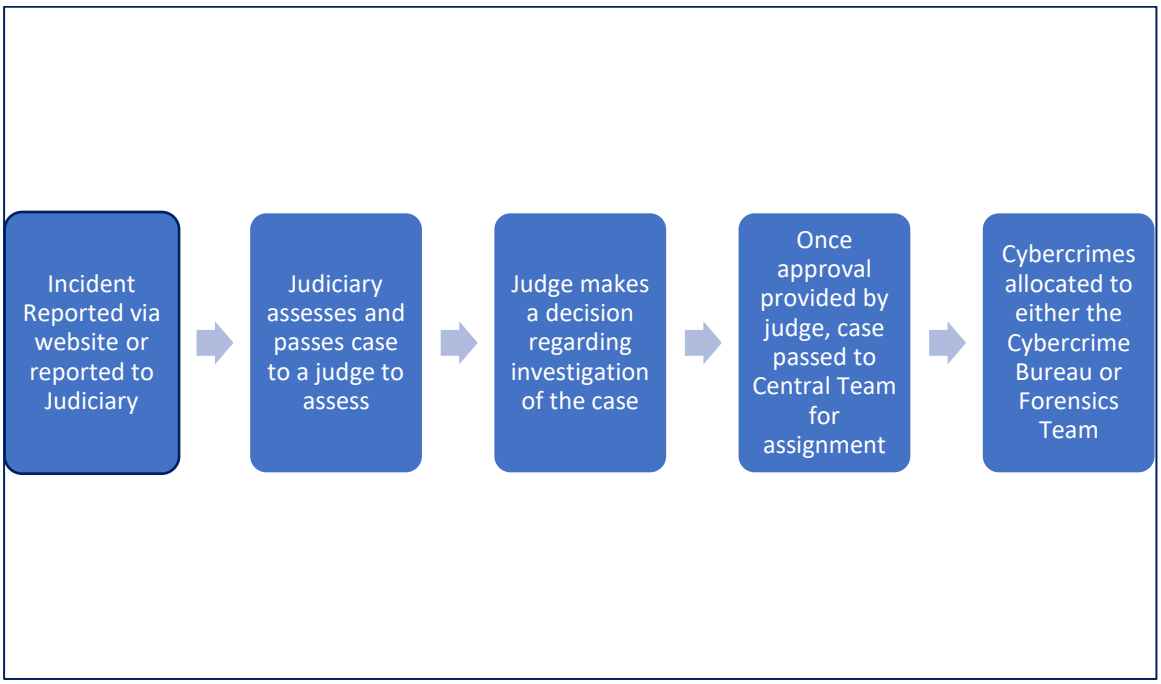

Figure 7 - Cybercrime reporting process

5.9.4. In some cases, following a report via the website an additional case will need to be raised (in non-electronic form) and submitted to the Judiciary.

5.9.5. For cases of reported cybercrime involving areas as terrorism, child pornography etc., following the initial report of a case investigation commences immediately, with judiciary approval provided automatically.

5.9.6. From a reporting perspective, reports are provided on a regular basis up the command structure to the General Directorate.

6. CURRENT CAPABILITIES

6.1. ISF IT Intelligence Department

6.1.1. The ISF's IT Intelligence Department (ID) is managed by Lt. Col. Youssef, and has multiple teams, these being server/endpoint administration, network administration, IT security (managed by Capt. El Weter), and maintenance.

6.1.2. From a network infrastructure perspective, the Intelligence Department has 2 distinct and separate networks to manage, one which provides external access to the internet (LAN 1) and a separate network (LAN 2) for ID-related business. LAN 2 provides external connectivity only via private/secured WAN connections, and prohibits users from accessing the 'unsecure' internet. LAN1 and LAN 2 are air-gapped and there is no physical connection between the two LANs.

6.1.3. The ISF LAN and LAN 2 are connected via a firewall which provides traffic access from LAN 2 to a specific application hosted on the ISF LAN. No other ports are open on this firewall, prohibiting access to other areas of LAN2, which minimises the risk of network/endpoint compromise for LAN2.

6.1.4. VPN access to LAN 2 is limited to a very small number of people and is only used for emergency remote support, where local support resources are unable to resolve issues. Given the remote access functionality available, there is the potential risk for the remote endpoint connecting into LAN 2 to be compromised by malware, therefore enabling remote access for a malicious threat actor. A two-factor authentication (2FA) solution is currently in the proof-of-concept stage – when fully implemented, this will increase security for any remote connections to the network and therefore mitigate some of the risk.

6.1.5. The Server/Endpoint Administration team consists of 5 people (including team leader, with 2 personnel on day shifts only and 2 providing out of hours (OOH) cover, ensuring 24/7 support. They are responsible for management of both physical/virtual servers and physical/virtual endpoint devices, storage management, software deployment via SCCM and all Active Directory functionality (GPO management/configuration, DNS for example).

6.1.6. In addition to management of on-site servers/endpoints, they are also responsible for management of a VDI-based application/desktop and off-site data storage, archiving and backup in multiple data centres. These data centres store critical applications and data, which is replicated between each one to ensure continuity of access to data in the event of an event/disaster resulting in the main DC going offline. An additional data centre is planned, which will provide additional disaster recovery (DR) and business continuity (BC) capability.

6.1.7. The majority of the Server/Endpoint team has formal certifications from Microsoft and have a good level of experience – the team leader has between 10-15 years' experience in this area.

6.1.8. The Network Administration team consists of 5 people (including the team leader) and provide management/administration/installation for all network-related devices and cabling (routers, switches, copper/fibre cabling installation, VOIP devices).

6.1.9. All firewall devices are classified as next-generation firewalls (NGFW) to ensure that they have the latest level of functionality.

6.1.10. To ensure continued accuracy of the network device configuration, an audit is carried out on an annual basis by and external third party.

6.1.11. The team has formal certification from Cisco and have many years of experience in managing/administration network devices (the team leader has 10 years' experience).

6.1.12. The IT Security team consists of 5 people (including team leader) and provides coverage for both office hours and OOH/weekend coverage. They provide management/administration for all security related devices such as firewalls, port security on switches, physical/virtual server and endpoint security, patch management and proactive vulnerability monitoring.

6.1.13. From a certification perspective, the team has certifications from multiple security vendors but at present none have the security generalist certifications such as (ISC)²'s Certified Information Systems Security Professional (CISSP), ISACA's CISM etc.

6.1.14. From a pro-active threat monitoring perspective, a member of the team reviews security alert updates from the US-CERT website, in addition to reviewing alerts from Microsoft, Cisco etc. and a number of information security websites/blogs. If required, alerts are then provided to other team members and other teams, to ensure that any critical/urgent patches are installed without delay.

6.1.15. From a patch management perspective, a testing/development LAN does not currently exist, resulting in operating system and vendor firmware and application software patches being deployed directly onto production/live LANs.

6.1.16. In terms of network device security, port security has been enabled to only permit devices with authorised MAC addresses to connect to the network. While this provides some measure of security, the ability to spoof MAC addresses means that this control can be overcome. While an 802.1X (network access control) solution can be implemented to increase network level security, the additional complexity of having managing the required authentication certificates and overarching public key infrastructure (PKI) creates additional management overhead. A project to implement 802.1X was previously attempted and subsequently cancelled given the identified complexities of certificate management.

6.1.17. In terms of vulnerability monitoring, the solution utilised by the ID IT team provides active monitoring of the network/server/workstation devices and provides alerts to enable patching of vulnerable servers/endpoints to be carried out.

6.1.18. File and email sandboxing capabilities also exist to block potentially malicious file types from infecting endpoints and the infrastructure.

6.1.19. In addition, encryption and data loss prevention (DLP) solutions have been implemented, which provide measures of confidentiality to data at rest and in transit, and to prevent data leakage from the organisation.

6.1.20. To provide visibility of security incidents and events, a security incident/event manager (SIEM) solution has been implemented initially as a proof-of-concept, in advance of planned full deployment in due course. Once implemented, the main challenge will be to not only to ensure that once installed and configured appropriately to ensure that incidents and event logs are collected from the relevant devices, but also to ensure that the analyst team has the appropriate level of knowledge, skills and experience to be able to interpret the information provided.

6.1.21. At present both intrusion detection and prevention devices (IDS/IPS) devices are in use on the production networks. These are used in conjunction with the NGFWs in place on the network. In a similar way to the SIEM solution discussed

in 5.3.18, following initial implementation, the main challenge to ensure that personnel with relevant knowledge and skills can interpret the information provided and analyse it accordingly.

6.1.22. The Maintenance team consists of 13 people, including 2 team leaders. They are responsible for carrying out basic troubleshooting tasks and device installation tasks. Given the basic nature of their role there is no requirement for them to have advanced technical qualifications, and have a minimum requirement of the CompTIA A+ certification.

6.2. Forensics Group

6.2.1. The Forensics group, managed by Maj. Sawwan, consists of three specialist teams, these being Digital Forensics (DF), Open Source Intelligence (OSINT)/Cyber Investigations (CI), and Research & Development (R&D).

6.2.2. The group numbers 15 people (5 x DF, 6 x OSINT/CI, 3 x R&D).

6.2.3. The Forensics group have dealt with over 2,100 new cases in 2018 to date which is on average 10 per day. The cases dealt with are regarded as 'national-level' and relate to suspected terrorism and suspected nation-state level attackers.

6.2.4. With regards to the digital forensics specialists, 2 have expert level knowledge/experience in data recovery, phone data extraction and SSD/DVR elements, with the other members of the team having good knowledge/experience in this area. All members of the team have a high level of both knowledge and experience in mobile and PC forensics

6.2.5. With regards to the OSINT/CI specialists, all personnel have high level of knowledge and skills and have been certified in training courses run by CEPOL, EUROPOL and UNODC.

6.2.6. The R&D specialists carry out vulnerability assessment/penetration testing, offensive/defensive security activities. They have attended multiple training courses and have extensive experience. One member of the team has presented at the prestigious 'Black Hat' security conference.

6.2.7. In terms of resourcing requirements for the proposed ISF CERT, it is expected that the Forensics team will provide the specialist resources as required (i.e. not full time initially), effectively providing a 'virtual' forensics team to the CERT. As the CERT develops its capabilities and as more forensics specialists are recruited from the ISF resource pool, it is expected that the Forensics team will provide dedicated full-time resources to the CERT i.e. a 'physical' team.

6.2.8. In terms of expected training requirements as part of the CERT implementation, it is expected that while all members of the Forensics group have high/excellent knowledge and skills in their specialist areas, that levels of knowledge and skills could be improved in the area of formal incident response, to ensure that the personnel are able to follow the full end-to-end process for successful management of all incidents.

6.2.9. Additionally, while the group has good knowledge and skills in PC operating systems, few have high levels of knowledge/skills in the area of Apple Mac and Linux operating systems. While training is currently planned for the former operating system, training in the latter (i.e. Linux) will be required to ensure that all specialists have the required level of knowledge and skills to meet future requirements. Additional training of benefit to this team would include memory, server and network forensics.

6.3. Cybercrime Bureau

6.3.1. The Cybercrime Bureau (CCB), led by Lt. Col. Khoury, is responsible for management of the majority of investigations where cybercrimes are suspected. Examples of case areas in which they work are suspected electronic fraud such as email hacking, social media, account credential theft, banking fraud, sextortion and child pornography. The team also carry out other activities including dark web analysis to support their investigations.

6.3.2. Dependent on the suspected perpetrator of the alleged cybercrimes (i.e. terrorist group, nation state attacker), the case may be passed to the Forensics group team to provide the lead in the investigatory process given their experience in this area and the equipment/tools available.

6.3.3. If the CCB retains control of an investigation, they are able to utilise resources from the Forensics team to support any ongoing investigations.

6.3.4. The bureau currently consists of approximately 50-55 team members. They have 10 teams of investigators (consisting of a lead investigator and assistant) and approximately 7-8 technical analysts to provide support to the investigators. The remaining members of the bureau provide administrative/logistical support to the investigators/analysts.

6.3.5. The CCB has a team which is involved with application development. At present, this team carries out application design, development and test, a situation which is far from ideal as there is no independent verification of the use of secure coding techniques. As opposed to using in-house techniques to carry out these tasks, these technical resources could be better utilised by carrying out requirements analysis and providing integration (where required) for external COTS (commercial-off-the shelf) applications, which would provide far better value for money.

6.3.6. Unlike their counterparts in the Forensics group, the CCB's technical specialists do not have the same level of knowledge and experience in areas such as digital forensics and malware analysis, and should therefore be regarded as technical generalists as opposed to specialists in a particular area. In addition, they also lack the required technical tools to be able to carry out these tasks.

6.3.7. From a networking infrastructure perspective, it should be noted that at present the CCB does not have the ability to utilise either physically (air-gapped) or logically (using VLANS) networks although this is planned as part of the future infrastructure design.

6.4. ISF IT Department

6.4.1. The ISF's IT department is headed by Col. Skaini and is managed by Lt. Col. Abdallah. It consists of 8 sections, these being as follows:

a) Registry/document management
b) System Administration
c) Networking
d) Development
e) Deployment
f) Support/maintenance
g) Archiving
h) Warehouse/inventory

6.4.2. The ISF's IT department has implemented a web portal which provides a number of public services including the ability to report cybercrimes.

6.4.3. In terms of current data storage, the ISF currently has its servers physically located in the same area of the support/maintenance team. There are plans in place to create a secure data-centre which will include firewalls, SIEM and host/network IPS devices, although it is expected that this will take at least 6 months before this is fully operational. Once the data-centre is fully operational, it is planned that a second data-centre (providing disaster recovery/business continuity) will be implemented in an alternate location.

6.4.4. The registry is manned by 12 personnel and receives documents from all ISF locations, and distributes all relevant documentation as required. They also act as a 'first line' support desk, receiving calls from users when they wish to report an IT issue. This support process is discussed in section 8.1.

6.4.5. The system administration team provides support for approximately 50 servers and associated services. It is manned by 3 people who provide daily cover, with an additional 3 people providing support for all databases. The team holds technical certifications from Microsoft (MCP, MCSE). At present the administration team has a high turnover of people given the short-term length of their postings, and therefore requires additional resources to back-fill positions. This team is also responsible for security management of all servers (AV updates/patches etc.).

6.4.6. The networking team consists of 4 people and currently has no team leader/officer in post to manage the team. They are responsible for management of all networking devices included switches, routers and firewalls. From a network security perspective, there is currently no control in terms of network access control (802.1x), and at present any unauthorised device can be connected to the network and potentially monitor traffic on a particular network segment. This team holds technical certifications (CCNA/CCNP) and each member has between 3-4 years of experience.

6.4.7. The development team is responsible for both development and test of all in-house IT applications used by ISF. This team has a number of sub-teams which look after specific application areas:

a) Human resource applications – 5 people
b) Asset management – 4 people
c) Document management – 3 people
d) Salary applications – 3 people

There is currently no strategy for centralised application development and most importantly there is currently no development/test environment in place – applications and written/tested and eventually deployed directly onto the production network which is a major risk.

6.4.8. The deployment team is currently working the capacity of development that deployment. There are a number of sub-teams as shown below:

a) Web development – 5 people
b) Medical applications (for pharmaceutical/medical centres) – 5 people
c) Criminal records database & 'wanted' people alerting – 4 people

6.4.9. The support/maintenance team (15 personnel) provides administration and support for approximately 2500 endpoints i.e. desktops and laptops. This team is required to support multiple operating system (Windows XP, Windows 7, Windows 8, Windows 10). Given that extended support for Windows XP ended in 2014, there have been no patches for this operating system for 4 years, resulting in multiple vulnerabilities and desktop endpoints being open to exploitation. While mainstream support for Windows 7 ended in January 2015, Microsoft is expected to provide patches until January 2020. Windows 8 mainstream support ended in January 2018, but security patches are expected to be provided until January 2023. It was stated that upgrades for all endpoints (and servers) is currently on hold given delays in the approval of Microsoft licence agreements, which is outside of the control of the ISF.

6.4.10. From an ongoing training perspective, it was stated that all technical members of the IT team undergo ongoing training, in terms of attendance at technical workshops, vendor conferences, formal training at both the ISF police academy and in Europe and the US.

6.4.11. At present there is no formal 'security team' element in existence. This team would provide the IT team with specialist cybersecurity knowledge and skills and would provide qualified technical people to manage all security elements of the ISF's IT infrastructure. They would also be able to provide specialist input into issue analysis and management of such elements as firewalls, SIEM and IDS/IPS appliances.

7. FUTURE TRAINING REQUIREMENTS

7.1. Technical

7.1.1. Given the levels of technical expertise in all groups from a general support, administration and management perspective, future requirements for qualified and experienced security analysts should be considered, given the current proof-of-concept implementation of the SIEMs and planned implementation of IDS/IPS appliances in both the ID IT team and the ISF IT team.

7.1.2. Once in operation, these applications/appliances will provide vast amounts of data, and it will be necessary to have personnel in place who can analyse and interpret the data provided and carry out the necessary actions accordingly.

7.1.3. In addition, training in Linux, Android and Mac operating systems would be of great benefit to all members of the forensics team, and would ensure that all members have the same levels of knowledge/skills in all areas in which they will be providing forensics investigatory support.

7.1.4. It should be noted that given the time constraints to carry out a detailed analysis of technical training requirements, it is recommended that a comprehensive training needs analysis process be instigated to ensure that all future ISF IT needs, not solely from a security perspective, are fully met.

7.2. User Security Awareness

7.2.1. An information security awareness document has been produced, providing some basic tips to users regards staying safe when online. This awareness document has been provided to all ISF personnel. As at August 2018, while some training courses have taken place at the ISF Police Academy for selected personnel, this training has not taken place on a regular basis and not all ISF personnel have received this training.

7.2.2. Given the lack of a regular awareness training programme there is no mechanism to provide confirmation that the any messages being communicated are both understood by the user community and also being implemented in everyday activity to keep the ISF's networks secure.

7.2.3. To ensure that all ISF personnel have awareness in the basic elements of information/cybersecurity, an appropriate training module should be introduced to the Police Academy's basic training programme and supported with ongoing training/awareness updates to all ISF personnel, whatever their role within ISF. This training will promote best practice both within the ISF and can also be used to promote awareness to other organisations.

8. CURRENT SUPPORT PROCESSES

8.1. ISF IT

8.1.1. At present the ISF IT department operates a multi-tier support model:

a) Initial call is received by the Registry– given the non-technical nature of their role they simply take details of the enquiry and pass the call to the support team.
b) The support team reviews the call and provides initial technical support to the user.
c) If necessary, the support team requests additional assistance from other technical teams in the IT department so that the support call can be resolved. Once resolved, the call is 'closed'.

8.1.2. At present no centralised support ticket system exists, which would provide a centralised point of documenting all support calls, monitoring call progress from receipt to resolution, a potential knowledge-base, and also an audit/reporting trail to detect issue trends.

8.1.3. After 15:30 on weekdays and during weekends, the IT department provides a single support resource (allocated from the IT department resource pool). In many cases, the out-of-hours (OOH) resource can provide only basic levels of support to users, given that their own area of knowledge/skills/experience, might not match the issue/problem being reported. Given that the ISF's police stations operate 24x7, a lack of specialist IT support during OOH periods has significant impact on swift resolution of many support calls.

8.2. ISF ID IT

8.2.1. Unlike the ISF IT department, all support calls received are initially processed by a member of the support team with technical knowledge/skills before being forwarded to a member of the specialist teams as necessary. There is no requirement to users to make initial contact with a non-technical team as per the ISF IT department's process.

8.2.2. At present, there is no formal ticketing system for support calls, which means that there is no audit trail for calls received/resolved, no provision for management reporting and no ability to identify issue trends and provide a knowledge-base for the support team.

8.2.3. After 15:30 on weekdays and during weekends, each team within the ID department provides suitably qualified technical cover. This ensures that all areas have support 24x7.

9. SPECIALIST RECRUITMENT

9.1. Requirements

9.1.1. Given the nature of information security, there is a requirement for individuals to be specialists in many different areas to ensure full coverage within the ISF.

9.2. Timeline

9.2.1. From a recruitment and training perspective, all ISF personnel are required to attend an initial basic training course, lasting approximately 6 months.

9.2.2. As the course nears completion, trainees undergo selection tests and, if selected, join one of the specialist teams on probation and undergo specialist training.

9.2.3. Following completion of initial training, ISF personnel undergo a 3 month 'work-experience' phase, spending time with all areas of the ISF to provide practical understanding of the various roles and activities within that area.

9.2.4. It should be noted that the lead-time from initial recruitment to being a fully operational specialist is between 9-12 months, dependent on the particular specialism and the training required. In some cases, it may take longer for a specialist resource to be fully operational.

10. CONCLUSIONS

10.1. Summary

10.1.1. The purpose of this document was to provide an independent assessment of the current practices and human capacities within the ISF relating to information security management.

10.1.2. In order to provide clarity in terms of the proposed recommendations, these have been divided up into three sections, namely people, process and technology, as previously discussed in Section 2.1.1.

10.1.3. While many elements reviewed as part of the assessment have good foundations, ISF should now build on these foundations and develop standardised policies, processes and procedures.

10.1.4. They should also encourage other areas providing IT support to adopt these processes and standardise the ways of working from an IT security perspective.

10.1.5. Subsequent deliverables will document a vision and high level roadmap for the implementation and operation of a CERT.

10.2. People

10.2.1. At present, the ISF has approximately 100 personnel (see Section 6 for resource breakdown by team) in various roles to support its network support/helpdesk, infrastructure, network devices, servers, and workstations and provide specialist investigations and forensics tasks.

10.2.2. Given the separation of networks (given the specific requirements of the ID department), there are a number of roles which are effectively duplicated i.e. there are teams managing and supporting the ‘same’ elements, albeit in a separated network. Given this situation, it would appear that the technical resources are not being utilised efficiently at present.

10.2.3. While the ID IT team has a dedicated IT security team in place, the separate ISF IT team has no security specialists in place who can provide specialist knowledge and advise in this area. Dependent on a potential re-organisation of resources as part of the planned CERT implementation, it is recommended that either a separate security operations team be created within the ISF IT team, or a single security team be assigned to provide the required specialist knowledge for all ISF managed networks.

10.2.4. As discussed in Section 5.7, the lack of a security culture within ISF is resulting in a significant lack of awareness by the majority of ISF personnel. Together with the issue of relevant policies to users and the introduction of relevant and regular awareness training, this will encourage a culture of security both within the organisation and outside the organisation, given that ISF personnel will hopefully encourage ‘safe’ cybersecurity practices for their families and friends.

10.2.5. From a training perspective, a requirement for training was identified in some of the teams included in the scope of the assessment. This ranged from specialist training in areas of forensics to more ‘general’ technical in operating systems (Linux, Mac, Android). Given the requirement to adopt standardised/formal incident management processes, an additional training requirement exists for those allocated to this area of operation.

10.2.6. In terms of recruitment, a decision will need to be made in terms of future recruitment of specialists into the CERT, given the timeline for both the ISF initial basic and subsequent specialist training.

10.3. Process

10.3.1. As discussed in Section 5.2, the lack of formal legislation is hindering the investigation and prosecution of cyber-related crimes and those related to data privacy/protection. While the passing of any legislation will outside the sphere of control of the ISF, once this is in place, the process for both investigation and prosecution of these crimes will be significantly aided.

10.3.2. From a risk management perspective (see Section 5.3), while the level of maturity in the risk management process is good in some areas it is significantly low in others. ISF should use the both the current processes in place, together with the presence of formally qualified persons in this area, to encourage the use of formal risk management processes across all areas of the ISF's IT estate, as this will ensure that once information assets, vulnerabilities and risks have been identified, appropriate controls are put in place to manage any identified risks. The additional appointment of an SRO will formalise this overall approach to risk management.

10.3.3. As discussed in Section 5.5, it is recommended that the current version of the Digital Information Security Policy document be split down into elements which are relevant for 'normal' ISF users, and those which are relevant for technical/support teams. Once issued to users, they should be required to both *understand* and *comply* with these policies, with consequences for non-compliance such as disciplinary action being initiated. In terms of the technical policy documents, supporting process/procedure documents should be created to provide standardised methods for completion of build, configuration, or administration tasks.

10.3.4. From a compliance perspective, it is recommended that a review is carried out of international standards to determine how the ISF can become initially compliant, and eventually certified to them. As discussed in Section 5.6.6, a good starting point would be to review the '10 steps to security' document provided by the UK government and the Cyber Essentials governance standard, issued by the UK's IASME[11] organisation.

10.3.5. In terms of the IT support processes in use within the ISF, the lack of a centralised support-ticket system results in a lack of co-ordination of support calls, ability to provide management information and importantly a knowledge base for information sharing between support teams. It is strongly recommended that a separate project be initiated to investigate the requirements for this element and implement accordingly.

10.4. Technology

10.4.1. As discussed in Section 4., given the current limitations in communications infrastructure almost half of the ISF locations cannot connect the ISF network. This results in 'electronic' communication with these locations being impossible, and any future incident reporting/alert communications not being possible via secure means.

10.4.2. It is recommended that a separate project be initiated to understand the specific infrastructure requirements for these remote locations so that they can become connected to the ISF LAN in due course.

[11] *IASME – Information Assurance for Small and Medium Enterprises* https://www.iasme.co.uk/the-iasme-standard/

10.4.3. While all endpoints, servers and network devices managed by the ID department are fully supported by the respective vendor, many endpoints on the ISF IT-managed network are currently running un-supported operating systems. Given the potential vulnerabilities that exist from running operating systems which are no longer supported, there is a significant risk that these vulnerabilities can be exploited leading to compromise of the entire ISF IT network. This issue should be addressed as a matter of urgency, although it is accepted that elements of this issue are outside the ISF's control, given the issue relating to a licencing agreement between Microsoft and OMSAR.

10.4.4. At present the ISF website provides a portal which will allow members of the public to report a cybercrime. Together with continued use of social media platforms such as Facebook and Twitter, the creation of a website providing alerts (based on acquired threat intelligence) will significantly increase visibility of cybercrime to the public and help with improving general awareness in this area.

10.4.5. As discussed in Section 5.8.2, the ISF (specifically the ID dept.) currently has a number of security applications in pilot/proof-of-concept stage. Given the proposed implementation of SIEM and IDS/IPS appliances as part of the planned data centre for the ISF IT department, this will increase the ability of the ISF to provide pro-active information, but the ability to do this will be dependent on the skills of those who will be required to analyse and interpret the information provided.