

Date: 27/05/2013

**Guideline to Determine Information Security Professionals Requirements for the CII Agencies / Organisations**

### **Contact Information**

For further clarification, please contact CyberSecurity Malaysia at [ispd@cybersecurity.my](mailto:ispd@cybersecurity.my).

<b>Contents</b>	<b>Page</b>
Tables .....	4
Figures .....	5
Foreword .....	6
Acknowledgement .....	7
<b>1 Background.....</b>	<b>8</b>
<b>2 Introduction.....</b>	<b>9</b>
2.1 Objective.....	9
2.2 Scope .....	9
2.3 Applicability .....	10
2.4 How to Use this Guideline? .....	11
<b>3 Information Security Management Framework .....</b>	<b>13</b>
3.1 Overview.....	13
3.2 Definition .....	13
<b>4 Roles and Responsibilities of Information Security Professionals .....</b>	<b>18</b>
4.1 Overview.....	18
4.2 Chief Information Security Officer (CISO).....	19
4.3 Information Security Operations .....	20
4.4 Information Security Audit & Information Security Compliance .....	22
<b>5 Competency Guideline for Information Security Professionals .....</b>	<b>24</b>
5.1 Overview.....	24
5.2 Information Security Professionals.....	24
5.3 Hiring and Employment procedures for Information Security Professionals.....	28
<b>6 Recommended Number of Information Security Professionals Within a CNII Agency / Organisation.....</b>	<b>29</b>
6.1 Overview.....	29
6.2 Recommendation on the Number of Information Security Professionals .....	29
6.3 Outsourcing of Information Security functions .....	30
<b>Appendix A: Definition of Critical National Information Infrastructure (CNII).....</b>	<b>33</b>
<b>Appendix B: List of Certifications.....</b>	<b>34</b>
<b>Appendix C: References .....</b>	<b>37</b>
<b>Appendix D: Abbreviated terms .....</b>	<b>39</b>
<b>Appendix E: Case Studies .....</b>	<b>41</b>
Case Study 1 – A Large Organisation .....	41
Case Study 2 – A Medium Organisation .....	42
Case Study 3 – A Small Organisation .....	43

## Tables

Table 1 - Mapping of Information Security Domains to Specific Roles and Responsibilities .....	18
Table 2 - Responsibilities to Embed Information Security Controls in Respective Departments .....	21
Table 3 - Number of Information Security Professionals to Hire .....	29

**Figures**

Figure 1 - Overview of the Guideline ..... 11

Figure 2 - Flow Chart to Illustrate the use of the Guideline ..... 12

Figure 3 - Information Security Management Framework ..... 13

Figure 4 - Information Security Professionals Requirements ..... 16

## Foreword

The cyber security threat landscape has been evolving significantly with the emergence of new technologies that introduce new threats along with various motivational factors for cyber attacks to occur. Out of 9,986 incidents reported to CyberSecurity Malaysia's Cyber999 Help Centre in 2012, intrusion and fraud made up 83% of total incidents reported to Cyber999. This can be worrisome for Critical National Information Infrastructure (CNII) sectors as attacks targeted to these sectors would have devastating impacts to the nation. In protecting these sectors, it is utmost important for the CNII agencies/organisations to have qualified information security professionals in safeguarding their critical information assets.

The publication of this Guideline is another important step towards achieving MOSTI's vision to utilise, deploy and diffuse science, technology and innovation for knowledge generation, wealth creation and societal well-being. I am pleased that CyberSecurity Malaysia has taken up the challenge through engagement with industry players and government agencies to realise the Guideline.

The publication of this guideline was stemmed through the decision made in the National Cyber Crisis Management Meeting (NCCMC) in year 2012 deliberating the significance of having qualified information security professionals in CNII agencies/organisations.

This Guideline is not prescriptive in nature, but its provisions encompass critical aspects in hiring qualified information security professional as one of the safeguards to protect the CNII agencies/organisations. It is hoped that this Guideline able to assist organisations in protecting their ICT's operating environment whilst preserving the confidentiality, integrity and availability of their information.

Therefore, I believe this Guideline will be instrumental in promoting and disseminating best practices for capacity building and grooming of information security professionals in Malaysia. It will certainly be a source of reference that could be readily and easily accessed by policy makers, researchers and practitioners.

I am confident that the recommendations in this Guideline will provide a vital framework for the CNII agencies/organisations in Malaysia to have qualified information security professionals in their respective organisations. As such, an initiative such as this Guideline is important so that the CNII agencies/organisations in Malaysia can gain a better understanding of the strategies involved in capacity building.

Thank you.

Dr. Abdul Rahim Bin Ahmad

Under Secretary  
ICT Policy Division  
Ministry of Science, Technology & Innovation (MOSTI)

## **Acknowledgement**

We hereby thank CyberSecurity Malaysia for these enlightening efforts and those who have made this Guide-line possible. Also, thank you to all participants of the Review Committee and the National Cyber Security Co-ordination Committee (NC3) members for their valuable inputs, feedback and comments.

Jabatan Peguam Negara  
Majlis Keselamatan Negara, Jabatan Perdana Menteri  
Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia, Jabatan Perdana Menteri  
Unit Permodenan Tadbiran & Perancangan Pengurusan Malaysia (MAMPU)  
Kementerian Pertahanan  
Kementerian Penerangan, Komunikasi dan Kebudayaan  
Kementerian Dalam Negeri  
Kementerian Kesihatan Malaysia  
Kementerian Kewangan  
Kementerian Pengangkutan Malaysia  
Kementerian Perdagangan Dalam Negeri, Koperasi & Kepenggunaan  
Kementerian Pertanian & Industri Asas Tani  
Kementerian Perusahaan Perladangan & Komoditi  
Kementerian Tenaga, Teknologi Hijau dan Air  
Kementerian Luar Negeri  
Jabatan Audit Negara Malaysia  
Jabatan Perkhidmatan Awam Malaysia  
Angkatan Tentera Malaysia  
Polis DiRaja Malaysia  
Suruhanjaya Komunikasi dan Multimedia Malaysia  
Suruhanjaya Pengangkutan Awam Darat  
Suruhanjaya Perkhidmatan Air Negara  
Suruhanjaya Sekuriti  
Suruhanjaya Tenaga  
Bank Negara Malaysia  
Lembaga Perlesenan Tenaga Atom  
Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT)  
Petroliam Nasional Berhad (PETRONAS)  
Khazanah Nasional Berhad  
MIMOS Berhad  
Universiti Tenaga Nasional (UNITEN)

## 1 Background

The National Cyber Security Policy (NCSP) emphasizes on capacity and capability building through Policy Thrust 4 on Culture of Security and Capacity Building (led by MOSTI). This policy thrust has several initiatives of which one of them is derived from the decision made during the National Cyber Crisis Management Committee (NCCMC) Meeting held in November 2012. This decision prompted for a guideline to be developed to identify the minimum requirements and qualifications for those who are involved in information security in Critical National Information Infrastructure (CNII) agencies / organisations. This is to ensure that they have appropriate qualified information security professionals to secure their ICT operating environment.

For definition of CNII, please refer to Appendix A.

This Guideline is not mandatory and serves only as a guide to assist a CNII agency / organisation in determining the Information Security Professionals requirements in terms of roles & responsibilities, competency and the minimum number of Information Security Professionals.

For avoidance of doubt, any requirements wherever mentioned in this Guideline is not to be construed as mandatory.

The CNII agencies / organisations may choose to outsource some of the information security functions. However, the responsibility to ensure adherence to information security requirements still rest within the CNII agencies / organisations.

Note: This Guideline makes reference to *MS ISO/IEC 27001:2007 Pengurusan Sistem Keselamatan Maklumat (Information Security Management System – ISMS)* for the definition and domains of information security.



# Guideline to Determine Information Security Professionals Requirements for the CNII Agencies / Organisations

## 2 Introduction

### 2.1 Objective

The objective of the Guideline to Determine Information Security Professionals Requirements for the CNII Agencies / Organisations (thereafter referred to as “the Guideline”) is to determine the requirements for Information Security Professionals for a CNII agency/organisation. This Guideline should be used when:

- i. A CNII agency / organisation wishes to set up a team of Information Security Professionals
- ii. A CNII agency / organisation wishes to assess the adequacy of its current Information Security Professionals

To achieve the above, there are three areas of the Information Security Professional requirements that a CNII agency/organisation should address:

- i. Roles & Responsibilities of Information Security Professionals
- ii. Competency of Information Security Professionals
- iii. Minimum number of Information Security Professionals

For each area, there are specific requirements recommended in this Guideline to be used by a CNII agency/organisation.

### 2.2 Scope

This Guideline is intended to cover the following areas:

- i. Information Security Management Framework
- ii. Roles and Responsibilities of Information Security Professionals
- iii. Competency Guideline for Information Security Professionals
- iv. Recommended Number of Information Security Professionals within a CNII agency / organisation

**Section 3** *Information Security Management Framework* defines the relevant areas which need to be addressed to provide an effective Information Security function within a CNII agency / organisation. It also defines Guiding Principles for Information Security Professionals.

**Section 4** *Roles and Responsibilities of Information Security Professionals* defines in detail the roles and responsibilities of an Information Security Professional based on the Information Security Management Framework.

**Section 5** *Competency Guideline for Information Security Professionals* defines the competency criteria for Information Security Operations, Information Security Compliance and Information Security Audit. It also defines Hiring and Employment procedures for Information Security Professionals.

**Section 6** *Recommended Number of Information Security Professionals within a CNII agency / organisation* provides a recommended indicative number of Information Security Professionals in a CNII agency / organisation based on the IT department resources.

## **2.3 Applicability**

This Guideline is not mandatory and serves as a guide to assist the CNII agency / organisation in determining the Information Security Professionals requirements in terms of the minimum number of Information Security Professionals, roles & responsibilities and competency requirements.

### Who should use the Guideline:

This Guideline can be used by the Management (decision maker) and the Information Security Professionals of CNII agencies / organisations to determine the roles and responsibilities, competency requirements and the Number of Information Security Professionals in their agency / organisation.

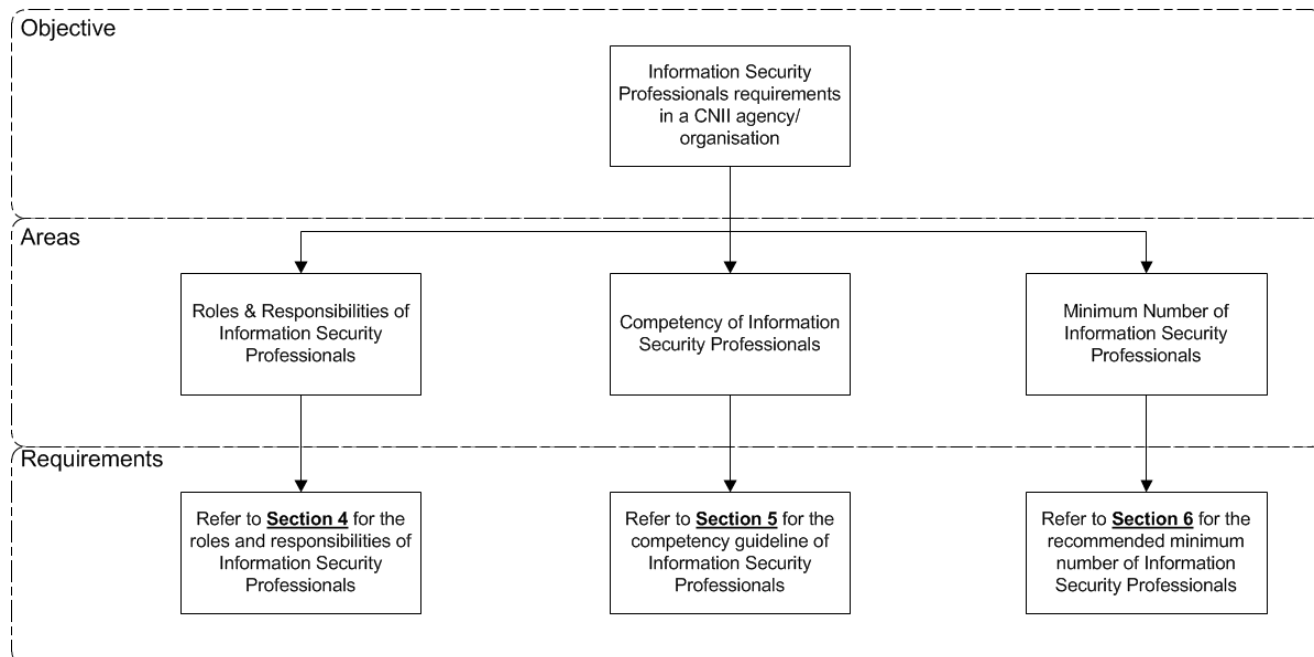
## 2.4 How to Use this Guideline?

To understand how to use this Guideline, please refer to the table below:

Ref	What is your objective in using this Guideline?	Where to find?
1	Defining Information Security Governance Structure in a CNII agency / organisation.	Refer to <b>Section 3.1 Information Security Management Framework</b>
2	Defining the Roles and Responsibilities for Information Security Professionals in a CNII agency / organisation.	Refer to <b>Section 4 Roles and Responsibilities</b>
3	Defining the competencies for Information Security Professionals in a CNII agency / organisation.	Refer to <b>Section 5 Competencies for Information Security Professionals</b>
4	Identifying the recommended number of Information Security Professionals in a CNII agencies / organisation.	Refer to <b>Section 6 Recommended Number of Information Security Professionals within an CNII agency / organisation</b>

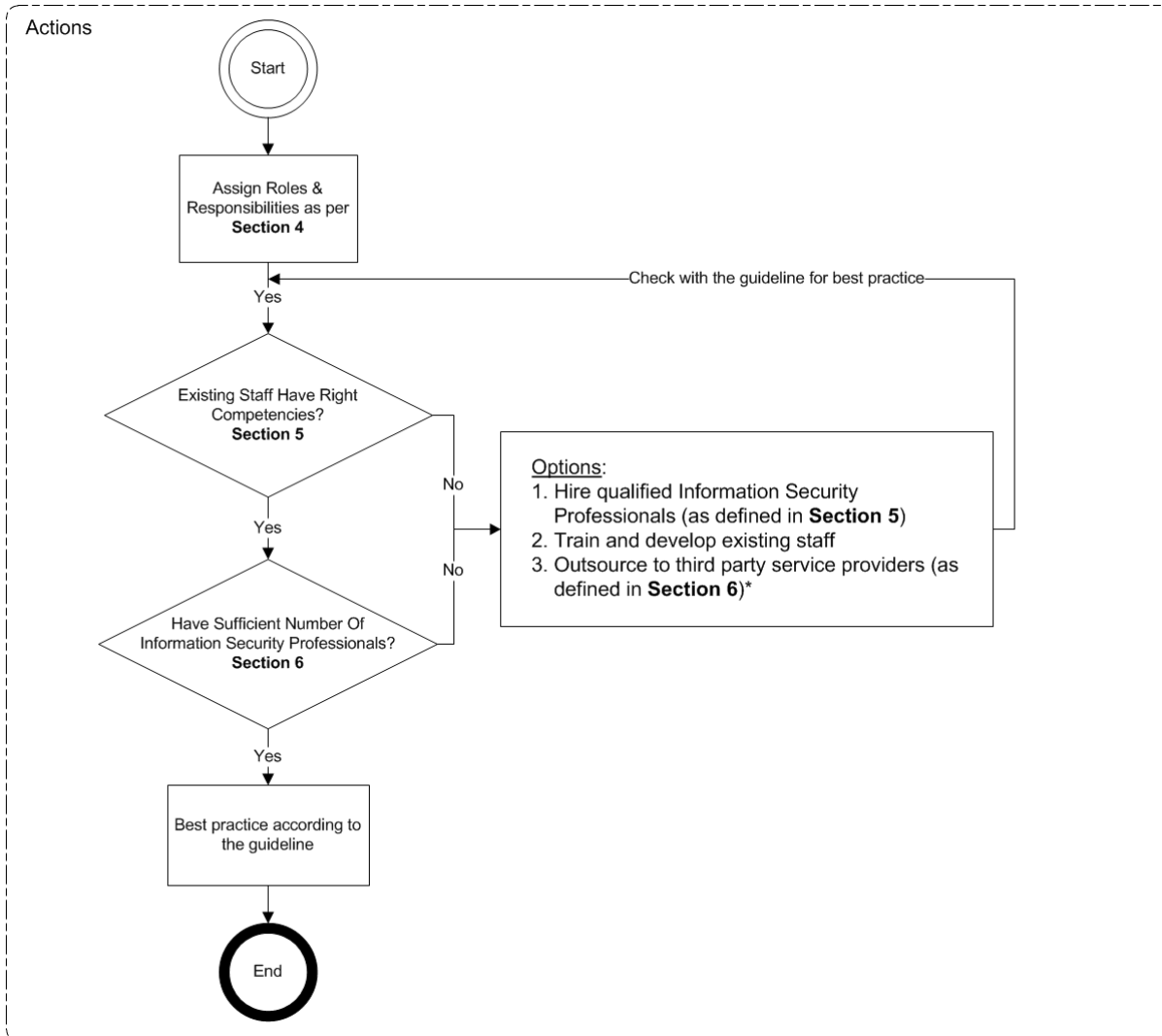
The flow charts below illustrate how the Guideline can be used. The first flowchart provides a brief overview of the several sections. The second flowchart illustrates how to use the Guideline.

**Figure 1 - Overview of the Guideline**



The flow chart below illustrates the actions which should be performed to comply with the Guideline:

**Figure 2 - Flow Chart to Illustrate the use of the Guideline**



**Actions**

The activities as defined in the flowchart Figure 2 need to be undertaken by a CNII agency / organisation to comply with the requirements as stated in the **Section 4, 5 and 6** in the Guideline.

\*Outsourcing: In the event some of the Information Security functions defined in Section 4 are outsourced, please refer to **Section 6** for further guidance.

### 3 Information Security Management Framework

#### 3.1 Overview

This section defines the relevant areas which need to be addressed to provide an effective Information Security function within a CNII agency / organisation, which comprises the following:

- i. Definition of Information Security
- ii. People
- iii. Policies

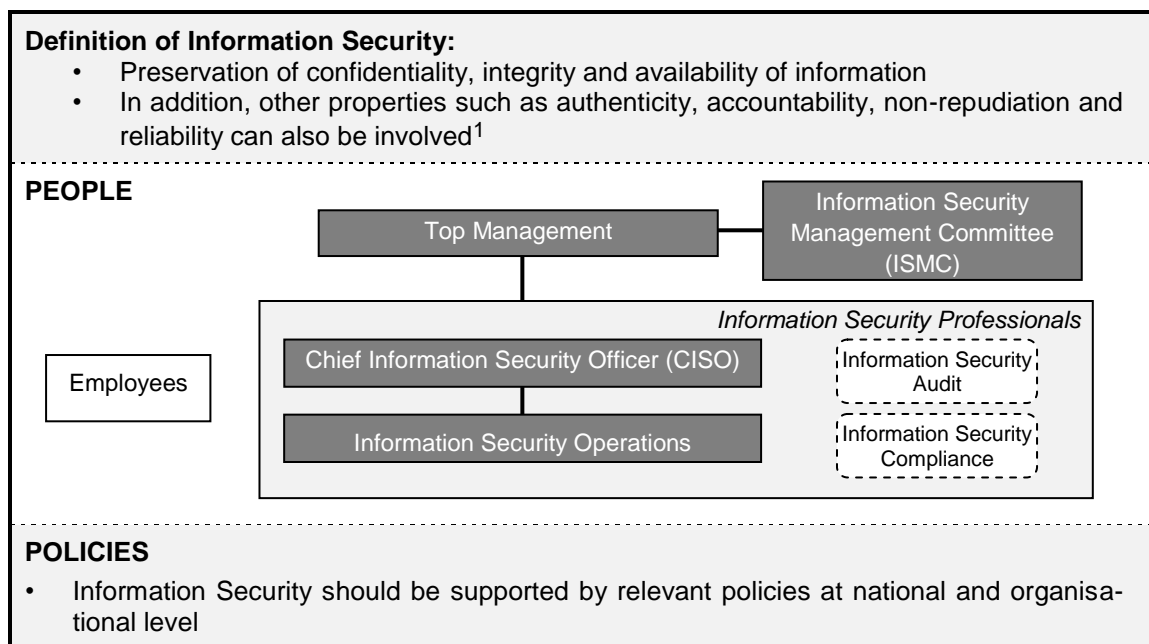
#### 3.2 Definition

##### 3.2.1 Information Security Management Framework

Information is an asset that is essential to an organisation’s business and consequently needs to be suitably protected, especially in the increasingly interconnected business environment. As a result of this increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities. Therefore the information needs to be protected against the risk of loss, operational discontinuity, misuse, unauthorised disclosure, inaccessibility and damage.

Within this Guideline an Information Security Management Framework has been developed to cover all relevant areas to provide a more effective and efficient Information Security within an organisation.

**Figure 3 - Information Security Management Framework**



This Information Security Management Framework reflects an overall management approach to ensure that strategies, directions and instructions are carried out systematically and are part of the business objectives.

<sup>1</sup> ISO/IEC 27001:2007 Information technology — Security techniques — Information security management systems — Requirements

The framework is a combination of definitions, organisation structure (people) with roles and responsibilities as well as policies, standards and guidelines required to establish the level of information security.

Below are the descriptions of each element of the Information Security Management Framework.

### **3.2.1 (a) Information Security:**

Information Security is defined as:

- i. Preservation of confidentiality, integrity and availability of information;
- ii. In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved<sup>2</sup>.

### **3.2.1 (b) People**

#### **i. Information Security Management Committee (ISMC)**

Information Security Management Committee (ISMC) comprises the senior management of the CNII agency / organisation. This role can be embedded into the existing senior management committee of the CNII agency / organisation. The roles of the ISMC are as follows:

- Provide oversight over Information Security within the CNII agency / organisation
- Define a governance structure within the organisation to fulfil the requirements for Information Security
- Ensure adequate resources are allocated to perform the Information Security functions
- Endorse Information Security policies
- Receive reports of Information Security violations
- Approve waivers of non-compliance to Information Security policies

Note: In reference to the Information Security Management Framework (Figure 3) for the CNII agencies in the Malaysia public sector the areas to be addressed by the Information Security Management Committee can be taken up by the *Jawatankuasa Keselamatan ICT* (JKICT).<sup>3</sup>

#### **ii. Top Management**

The role of Top Management can be undertaken by e.g. Chief Executive Officer (CEO), Chief Operating Officer (COO), Chief Technology Officer (CTO) or Chief Information Officer (CIO) and is subject to the organisation structure of the CNII agency / organisation. The roles of the Top Management in relation to Information Security are as follows:

- Appointment of the CISO
- Decide which Information Security functions can be outsourced and which need to be undertaken in-house based on the performed risk assessment

Note: In reference to the Information Security Management Framework (Figure 3) for the CNII agencies in the Malaysia public sector, the roles of the Top Management in this Guideline can be undertaken by the *Ketua Pegawai Maklumat* (CIO) or someone appointed by the *Ketua Setiausaha* (KSU).<sup>3</sup>

<sup>2</sup> ISO/IEC 27001:2007 Information technology — Security techniques — Information security management systems — Requirements

<sup>3</sup> Dasar Keselamatan ICT, Unit Pemodenan Tadbiran Dan Perancangan Pengurusan Malaysia (MAMPU), Jabatan Perdana Menteri

### iii. Information Security Professionals

#### a. Definition:

Information Security Professional is defined as:

- Information security practitioners who conform with the requirements of this Information Security Professional Guideline; and
- Information security practitioners with specific roles and responsibilities in Information Security Operation, Information Security Compliance and Information Security Audit.

Information Security Professional comprises of the following roles:

- **Chief Information Security Officer (CISO)**  
The role of a CISO is to define Information Security strategic direction, develop and maintain policies and establish roles and responsibilities for Information Security within the organisation. The Chief Information Security Officer may report to either the Chief Executive Officer (CEO), Chief Operating Officer (COO), Chief Technology Officer (CTO) or Chief Information Officer (CIO) of an organisation and is subject to the organisation structure of the CNII agency / organisation.
- **Information Security Operations**  
The role of an Information Security Professional performing Information Security Operations is to:
  - Manage and implement appropriate access rights to applications, systems, databases and network
  - Implement and maintain network security
  - Perform incident management
  - Ensure that the relevant Information Security controls are implemented and embedded in the respective departments performing daily operations
- **Information Security Audit & Information Security Compliance**  
In smaller CNII agencies / organisations these two functions may be combined. Essentially their role is to monitor compliance by the staff of the agency / organisation to the Information Security policies, standards, and procedures. Information Security Professional with the role of audit or compliance shall be independent from day-to-day Information Security Operations.

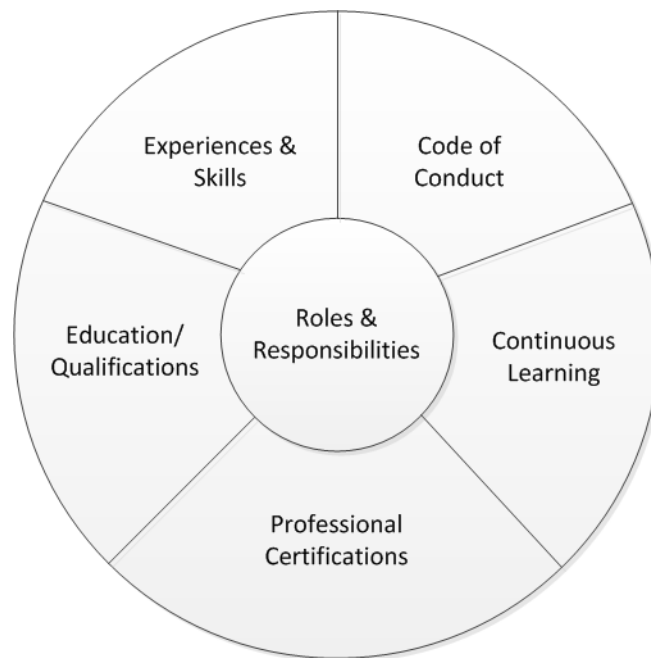
Note: In reference to the Information Security Management Framework (Figure 3) for CNII agencies / organisations in the Malaysia public sectors, the role of CISO can be taken up by the Pegawai Keselamatan ICT (ICTSO); the role of Information Security Compliance and Information Security Audit can be performed by MAMPU or *Audit Dalam*<sup>4</sup> or appointed parties;

#### b. Information Security Professional Requirements:

The following diagram shows the requirements for an Information Security Professional:

---

<sup>4</sup> Dasar Keselamatan ICT, Unit Pemodenan Tadbiran Dan Perancangan Pengurusan Malaysia (MAMPU), Jabatan Perdana Menteri



**Figure 4 - Information Security Professionals Requirements**

1. **Education / Qualifications**  
Preferably a degree holder in information security, computer science, information technology, management information system, business information system, business, accounting, economic or equivalent and adequate experience of information security work corresponding with their Information Security position; relevant certification in the information security.
2. **Professional Certifications**  
Certified by a recognised local or international information security certification body e.g. ISACA, (ISC)<sup>2</sup>, EC Council, CompTIA or SANS.
3. **Experiences and Skills**
  - **Chief Information Security Officer (CISO):**  
Depending on the seniority of the position, adequate number of years of information security work experience in the following domains<sup>5</sup>:
    - Information Security Governance
    - Information Risk Management and Compliance
    - Information Security Program Development and Management
    - Information Security Incident Management
  - **Information Security Operations:**  
Depending on the seniority of the position, adequate experience of direct information security work in two or more of the eleven (11) information security domains defined under Section 4
4. **Continuous Learning**
  - Obtained sufficient Continuing Professional Development (CPD) or Continuing Professional Education (CPE) in accordance with the requirement of their information security professional certification body
  - Keep up to date with the current developments in Information Security
  - Participate in related Information Security groups, activities and demonstrates information sharing

<sup>5</sup> CISM domains



- capabilities
- Publish journals and / or articles related to Information Security
- Networking with Information Security organisations

## 5. Code of Conduct

Information Security Professional is expected to exhibit a high standard of ethical conduct in their professional relationships in accordance with their professional certification code of conduct and employment requirements.

In the event of outsourcing Information Security functions, service provider(s) shall have Information Security Professionals who conform to the requirements set out in this Guideline.

## iv. CNII agencies / organisations employees

All CNII agencies / organisations employees need to comply with the Information Security policies, standards and procedures.

### 3.2.1 (c) Policies:

Information Security Policies are essential components supporting the Information Security Management Framework. Policies are the overall intention and direction as formally expressed by management and external parties. It sets out the broad control requirements in a given area which need to be communicated and understood by employees and relevant external parties in performing their activities.

A CNII agency / organisation's Information Security policies should include the following:

#### National level Policies

- Arahan MKN No. 24: Dasar dan Mekanisme Pengurusan Krisis Siber Negara
- Memorandum Jemaah Menteri Pelaksanaan Pensijilan MS ISO/IEC 27001:2007

#### Organisational level Policies

- Relevant regulatory guidelines in accordance with the relevant sector (e.g. Bank Negara Malaysia, Malaysian Communications and Multimedia Commission)
- For Malaysia public sectors
  - *Dasar Keselamatan ICT*
  - *Garis Panduan Kepakaran ICT Sektor Awam Malaysia*
- Best Practices

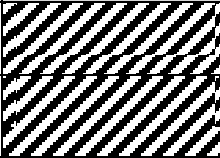



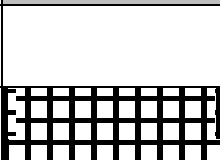
## 4 Roles and Responsibilities of Information Security Professionals

### 4.1 Overview

In this section we have set out the defined roles for Information Security Professionals (CISO, Information Security Operations, Information Security Audit and Information Security Compliance) and have mapped them to the respective Information Security domains which they need to address within their responsibilities.

The Table 1 below shows the mapping of the Information Security role to the respective Information Security domain and describes the specific responsibilities of the Information Security Professional.

**Table 1 - Mapping of Information Security Domains to Specific Roles and Responsibilities**

No.	Information Security Domains	Information Security Roles	Responsibilities
1	Security Policy	Chief Information Security Officer	
2	Organising Information Security	Chief Information Security Officer	
3	Asset Management	Information Security Operations	
4	Human Resources Security	Information Security Operations	
5	Physical and Environmental Security	Information Security Operations	
6	Communications and Operations Management (including Network Security)	Information Security Operations	
7	Access Control	Information Security Operations	
8	Information Systems Acquisition, Development and Maintenance	Information Security Operations	
9	Information Security Incident Management	Information Security Operations	
10	Business Continuity Management	Information Security Operations	
11	Compliance	Information Security Audit and Compliance	

 **Chief Information Security Officer**

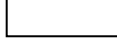
Responsible for the following:

- Define Information Security strategic direction, develop and maintain policies and establish roles and responsibilities for Information Security within the organisation as detailed in **Section 4.2**

 **Information Security Operations – To Perform**

Responsible for the following:

- Perform specific functions as detailed in **Section 4.3.1**
- Ensure that security and controls meet the information security objectives and are implemented in accordance with policies and procedures by the relevant personnel in the respective department(s)
- Provide Information Security advice and specifications where required

 **Information Security Operations – Embedded by Respective departments**

Responsible for the following:

- Ensure that security and control objectives are implemented by the relevant personnel in the respective department(s), as detailed in **Section 4.3.2**
- Provide Information Security advice and specifications where required

 **Information Security Audit & Information Security Compliance**

Responsible for the following:

- Perform specific functions as detailed in **Section 4.4.1** and **4.4.2**

The detailed Information Security responsibilities that need to be performed by the Information Security Professionals are for:

- Chief Information Security Officer in **Section 4.2**
- Information Security Operations in **Section 4.3**
  - Information Security Operations – To Perform in **Section 4.3.1**
  - Information Security Operations – Embedded by Respective departments in **Section 4.3.2**
- Information Security Audit and Information Security Compliance are defined in **Section 4.4.1 and 4.4.2**

The Information Security functions that need to be embedded in the respective departments (e.g. Human Resource, Finance or Risk Management) are also defined in **Section 4.3.2**.

The baseline for Information Security and the functions which at least need to be fulfilled in-house (cannot be outsourced) are defined in **Section 6 – Outsourcing**.

## **4.2 Chief Information Security Officer (CISO)**

The CISO will be responsible for the following domains:

### **4.2.1 Security Policy**

#### **4.2.1 (a) Information Security Policy**

- Set the strategic direction and clear policies for information security that is in line with business objectives and demonstrate support for, and commitment to, information security through the issuance and maintenance of an Information Security Policy across the organisation.
- Ensure that security controls are documented and embedded in the Information Security Policy, standards and guidelines.
- Allocate sufficient resources to implement, maintain and improve information security management processes.
- Establish training and awareness programmes to ensure that all personnel who are assigned information security responsibilities are competent to perform the required tasks.

### **4.2.2 Organisation of Information Security**

#### **4.2.2 (a) Internal Organisations**

- Approve the Information Security Policy, assign security roles, and co-ordinate and review the implementation of security across the organisation.
- Ensure information security activities are in compliance with the Information Security Policy.
- Identify responses to remediate activities that are not in compliance with policies, standards or best practices.
- Co-ordinate the implementation of information security controls.
- Recommend appropriate actions in response to identified information security incidents and initiate audits where necessary
- Establish a source of specialist information security advice if necessary and make available within the organisation.
- Develop contacts with external security specialists or groups, including relevant authorities, to keep up with industrial trends, monitor standards and assessment methods and provide suitable liaison points when handling information security incidents.
- Encourage a multi-disciplinary approach to information security.
- Provide security-related technical architecture advice for planning and development purposes.

#### **4.2.2 (b) External Parties**

- Approve the level of access of external parties to any of the organisation's information processing facilities and processing and communication of information.
- Perform risk assessment when there is a business need for working with external parties that may require access to the organisation's information and information processing facilities, or when obtaining or providing a product and service from or to an external party.
- Define and agree on the controls in an agreement with the external party.

### **4.3 Information Security Operations**

#### **4.3.1 To Perform the Following Information Security Functions**

Information Security Operations encompasses the day-to-day routine tasks related to information security function. Information Security Operations applies the policies and procedures defined under the Information Security Management Framework, ensures that security and control objectives are implemented by the relevant personnel in the respective department(s), and to provide Information Security advice and specifications where required.

Specifically, the roles and responsibilities of Information Security Operations for each domain will encompass the following:

##### **4.3.1 (a) Communications and Operations Management (Including Network Security)**

- Implement the correct and secure operations of information processing facilities.
- Implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.
- Minimise the risk of systems failures.
- Protect the integrity of software and information.
- Maintain the integrity and availability of information and information processing facilities.
- Protect information in networks and the supporting infrastructure.
- Prevent unauthorised disclosure, modification, removal or destruction of assets, and interruption to business activities.
- Maintain the security of information and software exchanged within an organisation and with any external entity.
- Ensure the security of electronic commerce services, and their secure use.
- Detect unauthorised information processing activities.

##### **4.3.1 (b) Access Control**

- Control access to information, information processing facilities, and business processes on the basis of business and security requirements.
- Implement formal procedures to ensure authorised user access and prevent unauthorised access to information systems.
- Control access to both internal and external networked services.
- Implement appropriate interfaces in place between the organisation's network and networks owned by other organizations, and public networks.
- Restrict access to application software, operating systems and databases to authorised users by implementing and using security facilities.
- Monitor user access and their activities including privilege users by reviewing log files.
- Implement appropriate protection when using mobile computing and consider the risks of working in an unprotected environment.
- Implement protection to the teleworking site.

#### 4.3.1 (c) Information Systems Acquisition, Development and Maintenance

- Undertake system security requirements analysis.
- Define the specifications for the applications including input data validation, control of internal processing and output data validations for the new system.
- Control access to the program source code
- Make sure that the defined security requirements are embedded into the systems.
- Undertake a technical vulnerability assessment and penetration testing for the new system.

#### 4.3.1 (d) Information Security Incident Management

- Implement the procedures for reporting the different types of event and weakness that might have an impact on the security of organisational assets to all employees, contractors and third party users.
- Implement responsibilities and procedures to handle information security events and weaknesses effectively once they have been reported.
- Apply process of continual improvement to the response, monitoring, evaluating, and overall management of information security incidents.
- Collect evidence, when required, to ensure compliance with legal requirements.
- Undertake corrective and preventive action.

#### 4.3.2 To Ensure that Relevant Information Security Controls are Embedded in Respective Departments Operational Procedures

In addition, Information Security Operations are responsible to ensure that the information security policies and standards are implemented and embedded in the respective departments. The Table 2 shows the detailed roles of the Information Security Professionals as well as the responsibilities of the respective department for the respective domains.

**Table 2 - Responsibilities to Embed Information Security Controls in Respective Departments**

Information Security Domains	Information Security Professionals responsibility	Responsibility of respective department in regards to Information Security
<b>4.3.2 (a)</b> Asset Management	Ensure that the responsibility for assets is established and owners are identified for all assets in respective departments for maintenance of appropriate controls.  Ensure that information classification and handling procedures are practised and embedded in the respective departments in their daily operations.	Develop and implement the respective Information Security policies and procedures in regards to the Asset Management domain.  Develop and implement a policy for information classification and handling procedures.
<b>4.3.2 (b)</b> Human Resources Security	Ensure that human resources security controls and practices are implemented and embedded in the Human Resource policy by the Human Resource department prior to employment, during employment and termination or change of employment of the organisation's staff.	Develop and implement policies and procedures for human resources security controls and practices for prior to employment, during employment and termination or change of employment of the organisations' staff.

<b>4.3.2 (c)</b> Physical and Environmental Security	Ensure that physical and environmental security controls and practices are implemented and embedded in the respective departments to protect information processing facilities and equipment from physical and environment threats.	Develop and implement policies and procedures for physical and environmental security controls and practices to protect information processing facilities and equipment from physical and environment threats.
<b>4.3.2 (d)</b> Information Systems Acquisition, Development and Maintenance	Ensure that information systems acquisition, development and maintenance security controls and practices are implemented and embedded in the system development life cycle.	Develop and implement policies and procedures for information systems acquisition, development and maintenance security controls and practices for the system development life cycle.
<b>4.3.2 (e)</b> Business Continuity Management	Ensure that Information Security is embedded within the BCM programme.	Responsible for implementing Information Security practices within their BCM programme of the respective department.

## 4.4 Information Security Audit & Information Security Compliance

### 4.4.1 Information Security Audit

In most cases Information Security Audit and Information Security Compliance can be combined as one function. However, in a bigger CNII agency / organisation these functions may be separated.

Audit is an independent function that reports to the Audit Committee or equivalent. It involves the verification of compliance against security policies, standards, legal and regulatory requirements. Information Security Audit involves the independent, risk-based assessment of the adequacy and integrity of controls in the ICT environment.

The following shows the area of focus of Information Security Audit:

- Governance and Management of IT
- Information System Acquisition, Development and Implementation
- Information Systems Operations, Maintenance and Support
- Protection of Information Assets<sup>6</sup>

Information Security Audit is undertaking the following functions for each of the focused areas defined above:

- Assess an organisation's compliance with security objectives, policies, standards and processes.
- Provide impartial assessment and reports covering security investigations, information risk management and investment decisions to improve an organisation's information risk management.
- Provide an independent opinion on whether control objectives are being met within an organisation.
- Identify and recommend responses on the organisation's systemic trends and weaknesses in security.

### 4.4.2 Information Security Compliance

Compliance is a function reporting to management which reviews the legal, regulatory and contractual requirements as well as to evaluate compliance issues / concerns within the organisation. The function can be combined with Information Security Audit or it also can be undertaken by Information Security Operations.

<sup>6</sup> CISA domains

**4.4.2 (a) Compliance with Legal Requirements**

- Ensure the design, operation, use, and management of information systems comply with statutory, regulatory, and contractual security requirements.
- Seek advice on specific legal requirements from the organisation's legal advisers, or suitably qualified legal practitioners.

**4.4.2 (b) Compliance with Security Policies and Standards and Technical Compliance**

- Review regularly the security of information against the appropriate security policies.
- Review the technical platforms and information systems for compliance with applicable security implementation standards and documented security controls.

## **5 Competency Guideline for Information Security Professionals**

### **5.1 Overview**

This section defines the following:

- i. Competency Criteria (General and Specific)
  - a. Information Security Chief Information Security Officer (CISO and Information Security Operations)
  - b. Information Security Compliance
  - c. Information Security Audit
- ii. Hiring and Employment

### **5.2 Information Security Professionals**

#### **5.2.1 General Requirements for Chief Information Security Officer (CISO) and Information Security Operations**

The following defines the general requirements for CISO and Information Security Operations.

Academic Qualifications: The following qualifications are preferred:

Degree in Computer Science, Information Technology, Information Systems, Engineering, Business Information System, Management Information System, Information Science or equivalent.

Certifications: ISACA® Certified Information Systems Auditor (CISA), ISACA® Certified Information Security Manager (CISM), (ISC)²® Certified Information Systems Security Professional (CISSP) or equivalent.

Working Experience: Working knowledge and understanding of information security concepts and technologies.

Skills:

- i. Good interpersonal, verbal, technical writing and communication skills
- ii. Ability to approach a problem by using a logical and systematic approach
- iii. Ability to be flexible and to be able to multi-task (within Information Security Operations and / or other tasks) and prioritise when necessary
- iv. Ability to work well within a team whilst at the same time demonstrating initiative and the ability to work without supervision

#### **5.2.2 Specific Requirements for Information Security Operations**

In addition to the general requirements stated above, specific requirements have also been identified for Information Security Professionals working in Information Security Operations in the following Information Security Domains:

##### **5.2.2 (a) Communications and Operations Management (Including Network Security)**

Relevant knowledge and experience in network security and server / desktop security management.

- Network security includes the following areas:
  - Basic network protocol (TCP IP, OSI Seven layers. IPv4 and IPv6)
  - Network security threat and vulnerabilities, controls to protect
  - Network security architecture and design
  - First responder network security incident management
  - Firewall, routers and switches rules and security configuration
  - Monitoring of network security
  - Patch management



- Up-to-date with current trends and emerging technologies (Cloud computing, )
- Server /desktop security includes the following areas:
  - Managing operating system security, database security. application security
  - Managing security for system interfaces
  - Batch processing
  - Backup and media handling
  - Patch management
  - System hardening
  - Endpoint security
  - Content security (DLP)
  - Email and web security, DNS
  - Monitoring of server / desktop security

Relevant professional certifications may include but are not limited to the following:

- Certified Wireless Network Professional (CWNP®) - Certified Wireless Network Administrator (CWNA)
- Certified Wireless Network Professional (CWNP®) - Certified Wireless Network Security Professional (CWSP)
- CompTIA® A+ CE
- CompTIA® Advanced Security Practitioner (CASP)
- CompTIA® Network+ CE
- Critical Infrastructure Institute (CII) - Professional Critical Infrastructure Professional (PCIP)
- EC-Council - Certified Ethical Hacker (CEH)
- GIAC Certified Intrusion Analyst (GCIA)
- GIAC Security Leadership (GSLC)
- ISACA® Certified Information Security Manager (CISM)
- (ISC)2® Certified Information Systems Security Professional (CISSP)
- (ISC)2® Certified Authorization Professional (CAP)
- (ISC)2® Information Systems Security Architecture Professional (CISSP-ISSAP)
- (ISC)2® Systems Security Certified Practitioner (SSCP)

### **5.2.2 (b) Access Control**

Relevant knowledge and experience in access controls and related fields.

- User access management includes the following areas:
  - User registration
  - Privilege management
  - User password management
  - Review of user access rights.
- Technical areas of access controls includes the following:
  - Network layer
  - Operating systems layer
  - Database layer
  - Applications layer

Relevant professional certifications may include but are not limited to the following:

- Certified Wireless Network Professional (CWNP®) - Certified Wireless Network Administrator (CWNA)
- Certified Wireless Network Professional (CWNP®) - Certified Wireless Network Security Professional (CWSP)
- CompTIA® Network+ CE
- CompTIA® Security+ CE
- EC-Council - Certified Ethical Hacker (CEH)

- GIAC Certified Firewall Analyst (GCFW)
- GIAC Information Security Fundamentals (GISF)
- GIAC Security Leadership (GSLC)
- ISACA® Certified Information Security Manager (CISM)
- ISACA® Certified Information Systems Auditor (CISA)
- (ISC)2® Certified Information Systems Security Professional (CISSP)
- (ISC)2® Certified Authorization Professional (CAP)
- (ISC)2® Information Systems Security Architecture Professional (CISSP-ISSAP)
- (ISC)2® Systems Security Certified Practitioner (SSCP)
- ITIL® Intermediate Certificate: Operation Support & Analysis (OSA)

### **5.2.2 (c) Information Systems Acquisition, Development and Maintenance**

Relevant knowledge and experience in security requirements for system development lifecycle.

- Security requirements for information system development
- Security control of applications including input data validation, control of internal processing and output data validations
- Management of security of system files including protection of system test data and access control to program source code
- Security of system development and support processes including change control procedures and security management of internal and outsourced software development
- Data migration, software testing, application security, systems security and related fields.

Relevant professional certifications may include but are not limited to the following:

- CompTIA® Advanced Security Practitioner (CASP)
- Critical Infrastructure Institute (CII) - Professional Critical Infrastructure Professional (PCIP)
- GIAC Security Leadership (GSLC)
- International Institute of Business Analysis (IIBA®) - Certified Business Analysis Professional (CBAP)
- ISACA® Certified Information Security Manager (CISM)
- (ISC)2® Certified Information Systems Security Professional (CISSP)
- (ISC)2® Certified Authorization Professional (CAP)
- (ISC)2® Information Systems Security Engineering Professional (CISSP-ISSEP)
- (ISC)2® Systems Security Certified Practitioner (SSCP)
- ITIL® Intermediate Certificate: Operation Support & Analysis (OSA)
- SABSA (Sherwood Applied Business Security Architecture) Foundation Certificate
- TOGAF® 9 Certified

### **5.2.2 (d) Information Security Incident Management**

Relevant knowledge and experience in incident management, forensics investigations and preservation of data including:

- Information security incident reporting
- Collecting and preservation of digital evidence
- Information security incident root cause analysis
- Corrective and preventive action for continual improvement

Relevant professional certifications may include but are not limited to the following:

- CERT®-Certified Computer Security Incident Handler (CSIH)
- Critical Infrastructure Institute (CII) - Professional Critical Infrastructure Professional (PCIP)

- DRI International - Associate Business Continuity Professional (ABCP)
- DRI International - Certified Business Continuity Professional (CBCP)
- EC-Council - Computer Hacking Forensic Investigator (CHFI)
- GIAC Certified Forensic Examiner (GCFE)
- GIAC Certified Incident Handler (GCIH)
- GIAC Security Leadership (GSLC)
- ISACA® Certified Information Security Manager (CISM)
- (ISC)2® Certified Information Systems Security Professional (CISSP)
- (ISC)2® Systems Security Certified Practitioner (SSCP)
- ITIL® Intermediate Certificate: Operation Support & Analysis (OSA)

### **5.2.3 Information Security Audit and Information Security Compliance**

#### **5.2.3 (a) General Requirements**

The following defines the general requirements for Information Security Professionals working in Information Security Audit and Information Security Compliance.

Academic Qualifications: The following qualifications, degrees or joint degrees are preferred:

Degree in Computer Science, Information Technology, Information Systems, Engineering, Business Information System, Management Information System, Information Science or equivalent, or:

Joint degree in Finance, Business Administration, Management Information System, Risk Management with Computer Science, Information Technology, Information Systems, Engineering, Business Information System, or Information Science.

Certifications: ISACA® Certified Information Systems Auditor (CISA) or equivalent, ISACA® Certified Information Security Manager (CISM), Certified ISO/IEC 27001 Lead Auditor (ISMS Lead Auditor) or equivalent.

Working Experience: Experience in information system audit, information technology risk management, information security, information technology, compliance, internal/external audit or other relevant fields.

Skills:

- i. Good verbal and written communications skills.
- ii. Ability to approach a problem by using a logical and systematic approach.
- iii. Ability to be flexible and to be able to multi-task and prioritise when necessary
- iv. Ability to work well within a team whilst at the same time demonstrating initiative and the ability to work without supervision

For additional information regarding specific certifications recommended for Information Security Professionals, please refer to **Appendix B: List of Certifications**.

## **5.3 Hiring and Employment procedures for Information Security Professionals**

### **5.3.1 Overview**

Having qualified information security professionals is a requirement for all organisations especially to ensure the organisation's specific security and business objectives are met. Within the hiring procedures it needs to be ensured that information security management and the Human Resource department works together closely to find the best professional for the job and mitigate risk throughout the organisation by hiring Information Security Professionals.

The following sections are organised as follows:

- i. Hiring Procedures
- ii. During Employment
- iii. Termination Procedures

**Note:** If there is Human Resource Security procedures defined within the agency / organisation there is a need to follow the existing standards. Otherwise the agency / organisation can refer to ISO/IEC 17799:2005 where appropriate controls are defined.

### **5.3.2 Hiring Procedures:**

Within the hiring procedures prior to employment it is recommended to perform several Human Resource Security Procedures to ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities. All candidates for employment, contractors and third party users should be adequately screened, especially for sensitive jobs.

Examples for Security Screening procedures prior to employment are as follow:

- i. Independent identify check
- ii. Background verification check
- iii. Reference check
- iv. Check on the Curriculum Vitae to confirm the claimed qualifications
- v. Check of criminal records
- vi. Need to sign a "Non-Disclosure Agreement"

### **5.3.3 During Employment:**

During the employment the policies of the company need to ensure that the personnel comply with the laws, code of conduct and standards, rules and regulations. Also Management must ensure that the personnel is encouraged to further education in the area of expertise and attends relevant professional training. Personnel should also participate in industry focus group to enrich knowledge and familiarity with up-to-date technologies.

### **5.3.4 Termination Procedures:**

Management must ensure the access rights for information processing facilities is revoked before the employment terminates. Personnel shall return the access identification, cards, and keys along with company assets before the employment terminates.

## 6 Recommended Number of Information Security Professionals Within a CNII Agency / Organisation

### 6.1 Overview

The CNII agencies / organisations need to cover and fulfil all areas of responsibilities as stated in Section 3 and 4. The agencies / organisation can either have internal staff to fulfil the roles or they can outsource these areas to external service providers.

Section 6.2 provides recommendations on the Number of Information Security Professionals a CNII agency / organisation should hire to undertake the Information Security functions. In the event of outsourcing certain Information Security functions, Section 6.3 provides Guiding Principles on Outsourcing.

### 6.2 Recommendation on the Number of Information Security Professionals

Based on a survey on a variety of Malaysian companies and taking the size, complexity and risk of a CNII agency / organisation under consideration, the following table provides an indicator for the recommended number of Information Security Professionals a CNII agency / organisation need to hire.

**Table 3 - Number of Information Security Professionals to Hire**

Number of Resources in ICT department	Number of Information Security Professionals
10 or less	At least 1 person
11 - 49	At least 2 - 3 person
50 – 100	At least 5 person
more than 100	At least 5% or more of total number of IT Professionals

This recommendation is based on a survey of 45 respondents from various sectors and is only focusing on the number of resources in the ICT department.

Different factors need to be taken in consideration to define the Number of Information Security Professionals within a CNII agency / organisation (e.g. size of the organisation, number of personnel, risk level of CNII agency / organisation, complexity of applications and criticality of information).

Information Security Professionals in CNII agencies / organisations will need to undertake the responsibilities as defined in Section 4.

However:-

- CNII agency / organisation may choose to outsource some of the functions. The decision to outsource should be based on availability of existing resources, skills and competency and must be subjected to a formal risk assessment process as defined in Section 6.3.;
- CNII agency / organisation should still have at least one information security professional who is responsible for overseeing the work for the outsourced party.

In some instances, the Information Security Professional may have other roles within the ICT department but these roles should not be in conflict with their information security roles.

Further Guidance on how to apply this Guideline for your organisation is available in Appendix D: Case Studies

## **6.3 Outsourcing of Information Security functions**

This section provides further guidance in the event some Information Security functions need to be outsourced.

### **6.3.1 Definition of Outsourcing**

Outsourcing is an arrangement when a CNII agency / organisation engages a third party service provider to provide the CNII agency / organisation with a service that is currently being performed in-house or is not being performed.

### **6.3.2 Guiding Principles for Outsourcing**

CNII agencies / organisations may outsource in the event:-

- not enough number of internal Information Security Professional in-house
- required skill set is not available within the CNII agency / organisation

When outsourcing, it is important to ensure that there is a transfer of skill and knowledge from the outsourced party to the internal Information Security Professionals.

Before deciding which areas can be outsourced, the management of the CNII agency / organisation is required to perform a risk assessment to evaluate the information security risk and impact to the organisation in terms of the ability to maintain the appropriate internal controls.

#### **6.3.2 (a) Risk Management processes:**

As part of the risk management processes the following activities should be undertaken:

- Risk assessment (before outsourcing):**  
The CNII agencies / organisation should undertake the following:
  - Identify and analyse risks related to outsourcing that particular function in Information Security.
  - Evaluate high risk areas of Information Security which are critical and therefore should not be outsourced.
- Risk Management:**  
Upon deciding on the area to outsource CNII agencies / organisations should undertake the following:-
  - Perform due diligence of service provider
  - Include in service agreement the requirements the service provider has to fulfil (e.g. confirm to Information Security policies and standards, BCM plan and right to audit)
  - Develop a Contingency plan in the event the Outsourcing is not available
  - Develop procedures for monitoring the third party service providers compliance to the agreed service agreement

Typically the following Information Security functions should not be outsourced:

- Chief Information Security Officer (CISO):**

The function of a CISO is as follows:

- Aligning Information security strategy to the overall business strategy
- Defining Information Security policies and standards and is overall responsible for Information Security in the CNII agency / organisation.
- Monitoring the governance of the third party service provider.

Therefore CISO should not be outsourced.

ii. Access Management:

The function of access management is the assignment of user-id and passwords. Outsourcing this role to a third party will increase the risk of unauthorised access to the CNII agency / organisations information.

*Although the roles are outsourced to external service providers, there must be at least one person (or more depending on the number of resources as indicated in Table 3) in-charge of the Information Security role internally. This Information Security Professional will receive reports and updates from the external service providers and is responsible for information security in the CNII agency / organisation. The designated Information Security Professional(s) may not be a full-time role but their other role should not be in conflict with their Information Security role.*





## **Appendix A: Definition of Critical National Information Infrastructure (CNII)**

*"CNII is defined as those assets (real and virtual), systems and functions that are vital to the nations that their incapacity or destruction would have devastating impact on:*

- *National economic strength; Confidence that the nation's key growth area can successfully compete in global market while maintaining favourable standards of living.*
- *National image; Projection of national image towards enhancing stature and sphere of influence.*
- *National defence and security; guarantee sovereignty and independence whilst maintaining internal security.*
- *Government capability to functions; maintain order to perform and deliver minimum essential public services.*
- *Public health and safety; delivering and managing optimal health care to the citizen.*

*The National Cyber Security Policy seeks to address the risks to the Critical National Information Infrastructure (CNII) which comprises the networked information systems of ten critical sectors. The CNII sectors are:*

- *National Defence and Security*
- *Banking and Finance*
- *Information and Communications*
- *Energy*
- *Transportation*
- *Water*
- *Health Services*
- *Government*
- *Emergency services*
- *Food and Agriculture"*

Source: National Cyber Security Policy (2005)

## Appendix B: List of Certifications

**Disclaimer:** This list is indicative only and non-exhaustive, in alphabetical order, and related specifically to Information Security. Application/Platform/Vendor specific certifications are not listed in this list. However Information Security Professionals are encouraged to attend vendor specific trainings and certifications when applicable to the ICT environment or day-to-day operations in their organisation. Please refer to the service providers (Application/Platform/Vendor) for their list of official certifications.

This Guideline makes reference to **Jadual 1.3 Contoh Senarai Pensijilan Profesional Mengikut Bidang Pengkhususan** from the document *Garis Panduan Kepakaran ICT Sektor Awam Malaysia* released by Jabatan Perkhidmatan Awam (JPA) Malaysia.<sup>7</sup>

### Management related certifications

- ISACA<sup>®</sup> Certified Information Security Manager (CISM)
- ISACA<sup>®</sup> Certified Information Systems Auditor (CISA)
- (ISC)<sup>2</sup><sup>®</sup> Certified Information Systems Security Professional (CISSP)
- (ISC)<sup>2</sup><sup>®</sup> Information Systems Security Management Professional (CISSP-ISSMP)

### Technical related certifications

- CERT<sup>®</sup>-Certified Computer Security Incident Handler (CSIH)
- Certified Wireless Network Professional (CWNP<sup>®</sup>) - Certified Wireless Network Administrator (CWNA)
- Certified Wireless Network Professional (CWNP<sup>®</sup>) - Certified Wireless Network Security Professional (CWSP)
- CompTIA<sup>®</sup> Advanced Security Practitioner (CASP)
- CompTIA<sup>®</sup> A+ CE
- CompTIA<sup>®</sup> Network+ CE
- CompTIA<sup>®</sup> Security+ CE
- Critical Infrastructure Institute (CII) - Professional Critical Infrastructure Professional (PCIP)
- DRI International - Associate Business Continuity Professional (ABCP)
- DRI International - Certified Business Continuity Professional (CBCP)
- EC-Council - Computer Hacking Forensic Investigator (CHFI)
- EC-Council - Certified Ethical Hacker (CEH)
- GIAC Certified Firewall Analyst (GCFW)
- GIAC Certified Forensic Examiner (GCFE)
- GIAC Certified Incident Handler (GCIH)
- GIAC Certified Intrusion Analyst (GCIA)
- GIAC Security Leadership (GSLC)
- GIAC Information Security Fundamentals (GISF)
- ISACA<sup>®</sup> Certified Information Systems Auditor (CISA)
- (ISC)<sup>2</sup><sup>®</sup> Certified Authorization Professional (CAP)
- (ISC)<sup>2</sup><sup>®</sup> Systems Security Certified Practitioner (SSCP)
- (ISC)<sup>2</sup><sup>®</sup> Certified Information Systems Security Professional (CISSP)
- (ISC)<sup>2</sup><sup>®</sup> Information Systems Security Engineering Professional (CISSP-ISSMP)
- (ISC)<sup>2</sup><sup>®</sup> Information Systems Security Architecture Professional (CISSP-ISSAP)
- (ISC)<sup>2</sup><sup>®</sup> Information Systems Security Engineering Professional (CISSP-ISSEP)
- ISO/IEC 27001 Certified Lead Auditor
- ITIL<sup>®</sup> Intermediate Certificate: Operation Support & Analysis (OSA)
- MILE2<sup>®</sup> Certified Penetration Testing Engineer

<sup>7</sup> Garis Panduan Kepakaran Ict Sektor Awam Malaysia, Jabatan Perkhidmatan Awam (JPA) Malaysia

**Appendix B: List of Certifications (cont'd)**

Qualifications	Information Security Management					
	Chief Information Security Officer	Information Security Operations				Information Security Compliance & Information Security Audit
		Access Control	Communications and Operations Management	Information Security Incident Management	Information Systems Acquisition, Development, and Maintenance	
<b>Management Related Certifications</b>						
ISACA® Certified Information Security Manager (CISM)	X					
ISACA® Certified Information Systems Auditor (CISA)	X					
(ISC)2® Certified Information Systems Security Professional (CISSP)	X					
(ISC)2® Information Systems Security Management Professional (CISSP-ISSMP)	X					
<b>Technical Related Certifications</b>						
CERT®-Certified Computer Security Incident Handler (CSIH)				X		
Certified Wireless Network Professional (CWNP®) - Certified Wireless Network Administrator (CWNA)		X	X			
Certified Wireless Network Professional (CWNP®) - Certified Wireless Network Security Professional (CWSP)		X	X			
CompTIA® A+ CE			X			
CompTIA® Advanced Security Practitioner (CASP)			X		X	
CompTIA® Network+ CE		X	X			
CompTIA® Security+ CE		X				
Critical Infrastructure Institute (CII) - Professional Critical Infrastructure Professional (PCIP)			X	X	X	
DRI International - Associate Business Continuity Professional (ABCP)				X		

**Guideline to determine Information Security Professionals Requirements for the CNII Agencies / Organisations**

DRI International - Certified Business Continuity Professional (CBCP)				X		
EC-Council - Certified Ethical Hacker (CEH)		X	X			
EC-Council - Computer Hacking Forensic Investigator (CHFI)				X		
GIAC Certified Firewall Analyst (GCFW)		X				
GIAC Certified Forensic Examiner (GCFE)				X		
GIAC Certified Incident Handler (GCIH)				X		
GIAC Certified Intrusion Analyst (GCIA)			X			
GIAC Information Security Fundamentals (GISF)		X				
GIAC Security Leadership (GSLC)		X	X	X	X	
IREB <sup>®</sup> Certified Professional for Requirements Engineering (CPRE)						
ISACA <sup>®</sup> Certified Information Security Manager (CISM)		X	X	X	X	X
ISACA <sup>®</sup> Certified Information Systems Auditor (CISA)		X				X
(ISC)2 <sup>®</sup> Certified Information Systems Security Professional (CISSP)		X	X	X	X	X
(ISC)2 <sup>®</sup> Certified Authorization Professional (CAP)		X	X	X	X	
(ISC)2 <sup>®</sup> Information Systems Security Architecture Professional (CISSP-ISSAP)		X	X			
(ISC)2 <sup>®</sup> Information Systems Security Engineering Professional (CISSP-ISSEP)					X	
(ISC)2 <sup>®</sup> Information Systems Security Management Professional (CISSP-ISSMP)		X	X	X	X	X
(ISC)2 <sup>®</sup> Systems Security Certified Practitioner (SSCP)		X	X	X	X	
ISO/IEC 27001 Certified Lead Auditor						X
ITIL <sup>®</sup> Intermediate Certificate: Operation Support & Analysis (OSA)		X		X	X	
MILE2 <sup>®</sup> Certified Penetration Testing Engineer			X			

## Appendix C: References

<b>US</b>	<b>Published</b>
Information Assurance Workforce Improvement Program	December 2005
ISO/IEC 27037 - Information technology — Security techniques (Experience)	October 2012
ISC2 - Hiring Guide to the Information Security Profession	January 2008
ISC2 – Career Impact Survey	January 2012
Legal, Ethical, and Professional Issues in Information Security	December 2007
National Security Professionals and Interagency Reform: Proposals, Recent Experience, and Issues for Congress	September 2011
National Strategy for the Development of Security Professionals	July 2007
<b>Canada</b>	
British Columbia Information Security Policy	October 2012
<b>Singapore</b>	
National Information Competency Framework (NICF)	2012
<b>UK</b>	
CESG Certification for IA Specialists	May 2012
IISP Information Security Skills Framework	July 2010
<b>Hong Kong</b>	
Hong Kong Office of the Government Chief Information Officer (OGCIO) IT Security Guidelines	September 2012
<b>Korea</b>	
Electronic Financial Transaction Act (EFTA)	June 2012
Enforcement Decree of EFTA	May 2012
<b>Australia/New Zealand</b>	
Australian Government - Protective Security Policy Framework (PSPF)	January 2011
Australian Government - Information Security Management Protocol	July 2011
Australian Information Security Manual	September 2012
New Zealand Information Security Manual	June 2011
<b>ISO</b>	
MS ISO/IEC 27001:2007 Information technology – Security techniques – Information security management system – Requirements ISO/IEC 27002:2005 Information technology – Security techniques – In-	

formation security management system – Code for practice for information security management	
<b>Malaysia</b>	
Garis Panduan Kepakaran ICT Sektor Awam Malaysia, Jabatan Perkhidmatan Awam (JPA) Malaysia	2010
Dasar Keselamatan ICT, Unit Pemodenan Tadbiran Dan Perancangan Pengurusan Malaysia (MAMPU), Jabatan Perdana Menteri	May 2010

## **Appendix D: Abbreviated terms**

(ISC) <sup>2</sup>	International Information Systems Security Certification Consortium
CEO	Chief Executive Officer
CII	Critical Infrastructure Institute
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNII	Critical National Information Infrastructure*
COO	Chief Operations Officer
CPD	Continuing Professional Development
CPE	Continuing Professional Education
CSM	CyberSecurity Malaysia
CWNP	Certified Wireless Network Professional
DLP	Data Loss Prevention
DNS	Domain Name Services
GIAC	Global Information Assurance Certification
ICT	Information and Communications Technology
ICTSO	ICT Security Officer
IEC	International Electrotechnical Commission
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISACA	Information Systems Audit and Control Association
ISMC	Information Security Management Committee
ISMS	Information Security Management System
ISO	International Standards Organisation
ITIL	Information Technology Infrastructure Library
JKICT	Jawatankuasa Keselamatan ICT
JPA	Jabatan Perkhidmatan Awam
MKN	Majlis Keselamatan Negara

## Guideline to determine Information Security Professionals Requirements for the CII Agencies / Organisations

MOSTI	Ministry of Science, Technology and Innovation
MyMIS	Malaysian Public Sector ICT Management Security Handbook
NCCMC	National Cyber Crisis Management Committee
NC3	National Cyber Security Coordination Committee
NCSP	National Cyber Security Policy
OSI	Open Systems Interconnection
SABSA	Sherwood Applied Business Security Architecture
TCP IP	Transmission Control Protocol Internet Protocol
TOGAF	The Open Group Architecture Framework



## Appendix E: Case Studies

### Overview

We have included three illustrative case studies below to assist CNII agencies / organisations in determining the appropriate number of Information Security Professionals in their agency / organisation and the reporting structure. We have categorised them as Large, Medium, and Small.

Case Study 1 – A Large Organisation

Company A – This organisation is a major conglomerate in Malaysia

Case Study 2 – A Medium Organisation

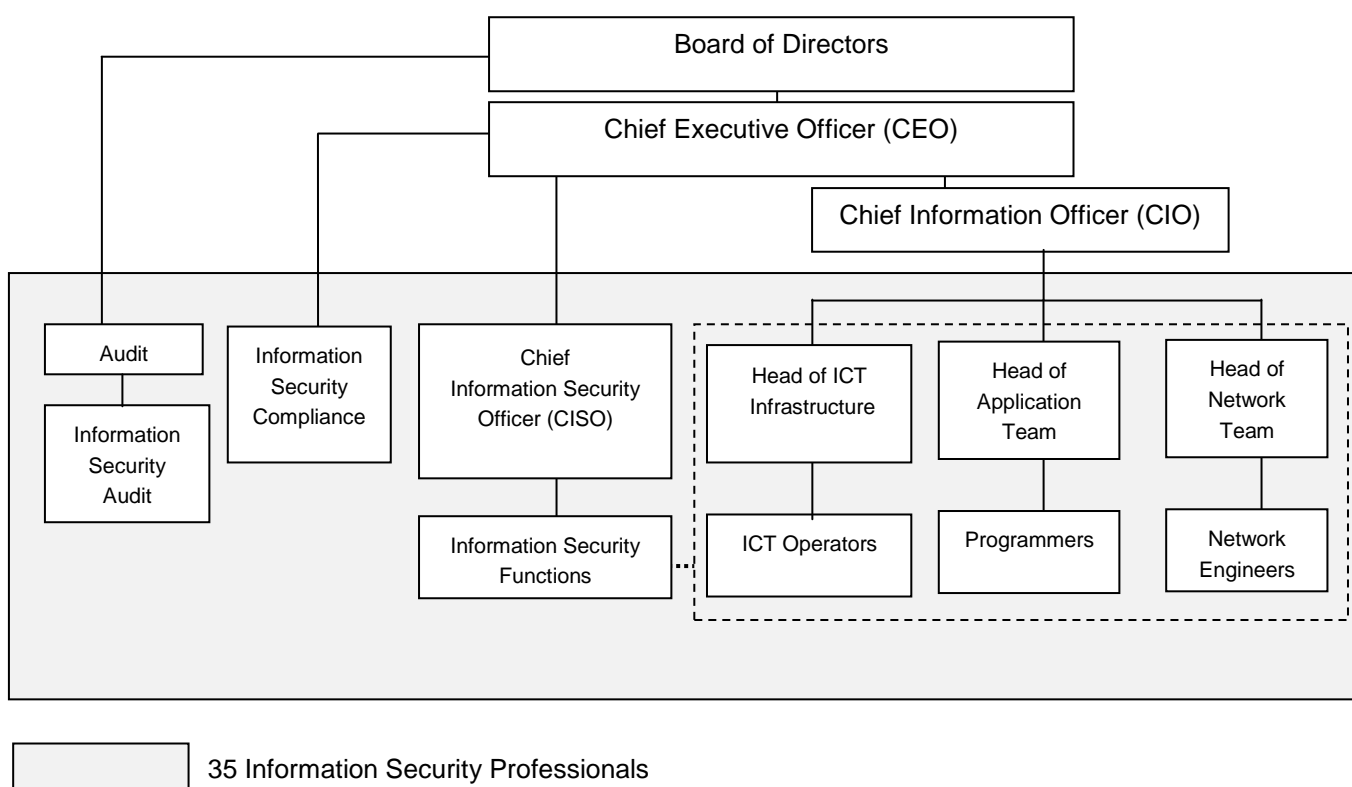
Company B – This organisation is a medium-sized CNII organisation with a few branches across Malaysia

Case Study 3 – A Small Organisation

Company C – This organisation is a small-sized CNII agency

### Case Study 1 – A Large Organisation

Company A – This organisation is a major conglomerate in Malaysia with more than five thousand people. The number of the ICT Professionals in Company A across Malaysia is around seven hundred people, of which 5% or thirty five people are Information Security Professionals.

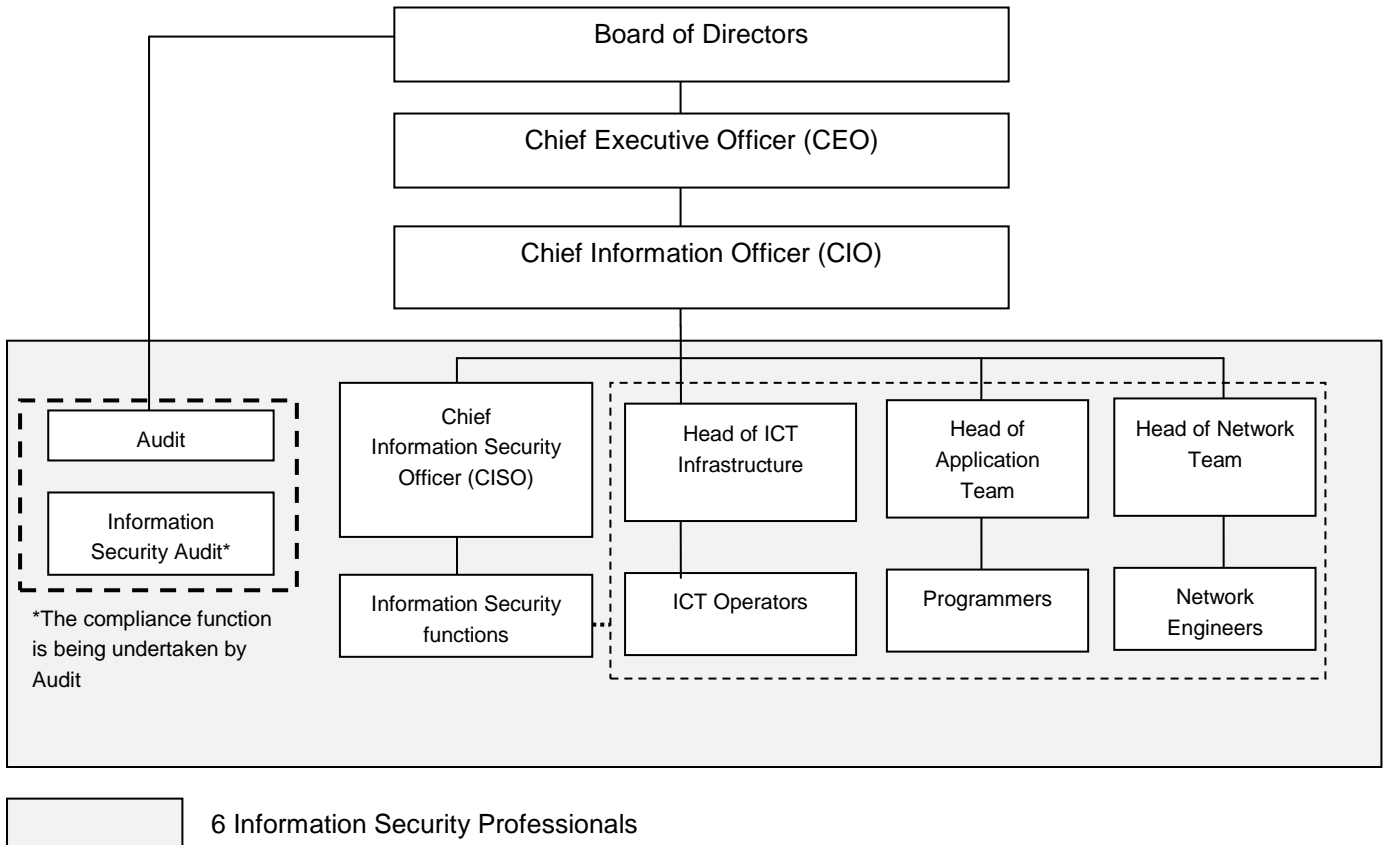


**Case Study 2 – A Medium Organisation**

Company B – This organisation is a medium-sized CNII organisation with a few branches across Malaysia with just over one thousand employees.

The number of the ICT Professionals in Company B is around one hundred people, of which six people are Information Security Professionals.

**Note:** In this example, Information Security Compliance can be combined with Information Security Audit due to the size of the organisation



**Case Study 3 – A Small Organisation**

Company C – This organisation is a small-sized CNII agency.

The number of the ICT Professionals in Company C in Malaysia is around twenty people, of which two people are Information Security Professionals.

**Note:** In this example, Information Security Compliance can be combined with Information Security Audit due to the size of the organisation

