# TECHNICAL CODE

## INFORMATION AND NETWORK SECURITY - CAPABILITY DEVELOPMENT AND CAPACITY BUILDING



**Developed by**

Malaysian Technical Standards Forum Bhd

**Registered by**

MCMC

Registered date:

# MCMC MTSFB TC GXXX:2021

## Development of technical codes

The Communications and Multimedia Act 1998 ('the Act') provides for Technical Standards Forum designated under section 184 of the Act or the Malaysian Communications and Multimedia Commission ('the Commission') to prepare a technical code. The technical code prepared pursuant to section 185 of the Act shall consist of, at least, the requirement for network interoperability and the promotion of safety of network facilities.

Section 96 of the Act also provides for the Commission to determine a technical code in accordance with section 55 of the Act if the technical code is not developed under an applicable provision of the Act and it is unlikely to be developed by the Technical Standards Forum within a reasonable time.

In exercise of the power conferred by section 184 of the Act, the Commission has designated the Malaysian Technical Standards Forum Bhd (MTSFB) as a Technical Standards Forum which is obligated, among others, to prepare the technical code under section 185 of the Act.

A technical code prepared in accordance with section 185 shall not be effective until it is registered by the Commission pursuant to section 95 of the Act.

For further information on the technical code, please contact:

**Malaysian Communications and Multimedia Commission (MCMC)**
MCMC Tower 1
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8688 8000
Fax: +60 3 8688 1000
http://www.mcmc.gov.my

OR

**Malaysian Technical Standards Forum Bhd (MTSFB**)
MCMC Centre of Excellence (CoE)
Off Persiaran Multimedia
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8320 0300
Fax: +60 3 8322 0115
http://www.mtsfb.org.my

**Contents**

## Committee representation

This technical code was developed by Security, Trust and Privacy Working Group of the Malaysian Technical Standards Forum Bhd (MTSFB) which consists of representatives from the following organisations:

Communications Convergence Professional Society

Cyber Intelligence Sdn Bhd

CyberSecurity Malaysia

K2Baseline Sdn Bhd

Kaapagam Technologies Sdn Bhd

Malaysia Digital Economy Corporation (MDEC) Sdn Bhd

Maxis Broadband Sdn Bhd

MEASAT Broadcast Network Systems Sdn Bhd

National Cyber Security Agency

Telekom Malaysia Berhad

Universiti Teknikal Malaysia Melaka

## Foreword

This technical code for Information and Network Security - Capability Development and Capacity Building (‘this ‘Technical Code’) was developed pursuant to section 185 of the Act 588 by the Malaysian Technical Standards Forum Bhd (MTSFB) via its Security, Trust and Privacy Working Group.

This Technical Code is an extension to the MCMC MTSFB TC G009, *Information and Network Security - Requirements.*

This Technical Code shall continue to be valid and effective from the date of its registration until it is replaced or revoked.

# INFORMATION AND NETWORK SECURITY - CAPABILITY DEVELOPMENT AND CAPACITY BUILDING

## 0. Introduction

This Technical Code provides the organisational requirements for the development of cyber security practitioners and professionals to ensure the competencies are relevant, retained and recognised.

The prevailing environment of uncertainty, along with surrounding cyber threats, is restricting economic development. The spectre of potential threats hinders key digital ecosystem players from pursuing cyber-related commercial and public development initiatives. Such situations require a huge number of skilled workforces to ensure the progress of various industries and sectors will not be obstructed unexpectedly.

Threats grow with the rapid expansion of data-driven technologies such as convergence of web, cloud, mobile and Internet of Things (IoT). As these technologies expand in use, so do the risks, making cyber risk management imperative to organisations today.

Protecting against targeted threats without disrupting business innovation and growth is an increasingly critical business, economic and social imperative. The need and demand for both physical infrastructure and human capital is more pressing than ever before.

The following are the benefits of this Technical Code:

a) to improves the preparedness and readiness of organisations in overcoming the cyber security related threats by upskilling their personnel in cyber security skills and knowledge;

b) to enhances the brand and reputation of the organisation; and

c) to develop competent manpower in the area of cyber security to enhance the security of information infrastructure.

## 1. Scope

This Technical Code specifies the requirements for the development of ethical, competent and recognised cyber security workforce.

This includes the identification of Knowledge, Skills and Attitude (KSA), certified credentials and commitment to Continuing Professional Development (CPD) of cyber security workforce.

The requirements of this Technical Code are generic and intended to be applicable for all organisations regardless of its size, type or nature.

This Technical Code is designed to be used by organisations:

a) to provides cyber security personnel with the right KSA and experience through attaining certified credentials;

b) to guide organisations in planning, implementing and reviewing capability development programs; and

c) to develop cyber security practitioners and professionals that are technically capable and proficient.

## 2. Normative references

The following normative references are indispensable for the application of this Technical Code. For dated references, only the edition cited applies. For undated references, the latest edition of the normative references (including any amendments) applies.

MCMC MTSFB TC G009, *Information and Network Security - Requirements*

## 3. Abbreviations

For the purposes of this Technical Code, the following abbreviations apply.

| | |
|---|---|
| CPD | Continuing Professional Development |
| ICS | Industrial Control System |
| ICT | Information and Communications Technology |
| IoT | Internet of Things |
| JPK | Department of Skills Development |
| KSA | Knowledge, Skills and Attitude |
| MBOT | Malaysia Board of Technologists |
| SOP | Standard of Procedures |

## 4. Terms and definitions

For the purposes of this Technical Code, the following terms and definitions apply.

### 4.1 Cyber security practitioner

Cyber security practitioner is personnel with specific cyber security technical skillsets and proficient in the operation.

### 4.2 Cyber security professional

Cyber security professional is personnel with strategic capability in strategizing, planning and executing cyber security initiatives.

## 5. Cyber Security Capability Development and Capacity Building Framework

The Cyber Security Capability Development and Capacity Building Framework deployed under this Technical Code is established with reference to the ISO/IEC 17024 on people certifications, ISO 9000 series on processes and ISO/IEC 27001 on security management as depicts in Figure 1.

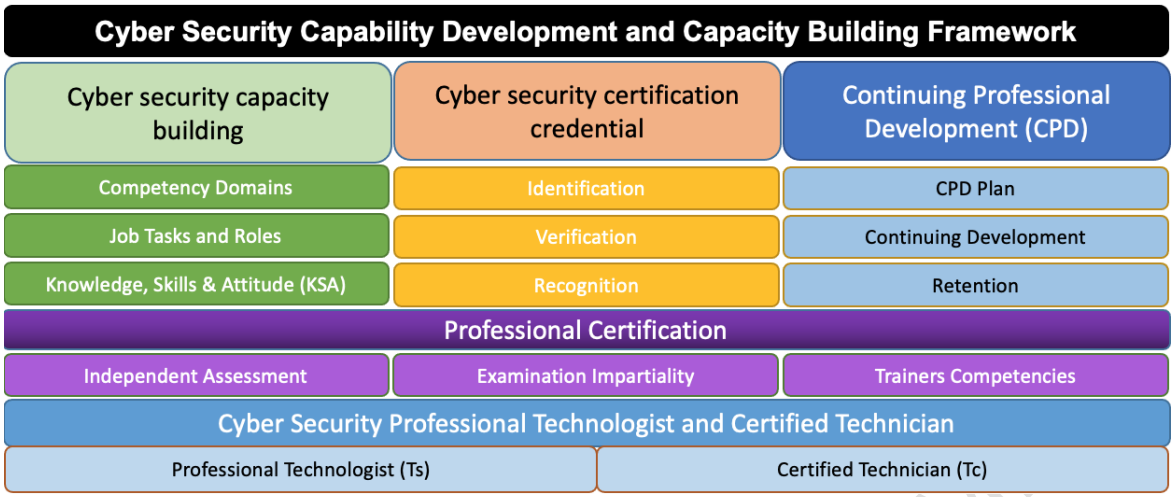


**Figure 1. Cyber Security Capability Development and Capacity Building Framework**

This framework also is the extension on People (Category 3) of the MCMC MTSFB TC G009, *Information and Network Security - Requirements.* Therefore, requirements defined in it shall be complied by the organisation.

The framework measures an individual's ability to "do" a given task and understand "why" it is being done taking context into consideration, rather than solely relying on knowledge-based assessments.

The framework is written in a manner that enables "transferability of skills" between job functions so that a flexible lifelong learning roadmap is possible with multiple changes of career in the cyber security field. This is based on the requirements of industry as identified via industry focus group workshops.

The framework outlines the requirements of:

a) cyber security capacity building;

b) certification credentials; and

c) CPD;

d) professional certification; and

e) cyber security professional technologist and certified technician.

## 6. Requirements of cyber security capacity building

Cyber security capacity building is for the organisation to have the right cyber security domains with the appropriate job roles and tasks. The cyber security building also helps the organisation to identify the required KSA for their cyber security practitioners and professionals.

The benefit of cyber security capacity building for the organisation are as follows:

a) the right identification of cyber security competencies;

b) clear definition of job roles and required tasks; and

c) well-defined requirements of KSA.

The relevant knowledge and skills should be recognised by the Department of Skills Development (JPK) under the Act 652, *National Skills Development Act 2006*.

### 6.1 Cyber security domains

#### 6.1.1 Cyber security technical competencies

The organisation shall identify the required cyber security technical competencies domains related to technical skills and knowledge of cyber security practitioners and professionals to conduct their tasks.

The technical competencies domains should include the following but not limited to:

a) digital forensics;

b) incident handling and response;

c) security assurance;

d) cryptography;

e) governance, risk and compliance;

f) threat and vulnerability management;

g) cyber threat intelligence;

h) cloud security; and

i) security architecture.

#### 6.1.2 Cyber security generic competencies

The organisation shall identify the required cyber security generic competencies domains related to cyber security soft skills in delivering services and consultations.

The generic competencies domains should include the following but not limited to:

a) people skills such as leadership, mentoring and coaching, diversity management, communications and strategic thinking;

b) process skills such as change management, organisational management, information management, financial management and conflict management; and

c) business skills such as entrepreneurship, Information and Communications Technology (ICT) literacy, customer services, partnership and innovation.

### 6.2 Cyber security job roles and tasks

The organisation shall define the required job roles and tasks based on the identified domains that is applicable to the organisation.

### 6.3 Knowledge, Skills and Attitudes (KSA)

The organisation shall identify the required KSA for each job roles and tasks required.

The KSA is a standard base and means of acknowledging the required competencies for the job role and task. KSA enables qualitative and quantitative measurements of professional criteria and serves as the reference guide for the organisation.

The Knowledge (K) should provide a set of Knowledge elements for the competency area. This is what one should "know".

The Skills (S) should provide a set of Skills elements for the competency area. This is what one should be "able to do".

The Attitude (A) should provide a set of Attitude elements for the competency area. This is what traits one should exhibit. Unlike the K and S elements, it is not expected that an assessment method should explicitly measure these, but rather that a training program should blend them into the fabric of the learning. This must be evaluated when the training program is submitted for evaluation.

The KSA is documented in KSA Descriptor which consist of a list of underpinning KSA of identified work roles and tasks.

Example of KSA Descriptors is provided in Annex A.

## 7. Requirements of certification credentials

Certification credential is the requirements for the organisation to recognise the right competencies and certifications for their cyber security practitioners and professionals.

The function of organisation with regards to certification credential are:

a) identification of the required certification credential;

b) verification of the certification credential; and

c) recognition of the certification credential.

The organisation shall identify the required certification credentials applicable to the organisation and it shall be certified by the certification body. Example of the required certification credentials are provided in Annex B.

The organisation shall verify the certification credentials based on following criteria.

a) Certification examination is impartial.

b) Assessment is validated by third parties.

c) Certification credential is valid and has not expired.

d) Certification credential is recognised by a certification body.

e) Certification credential is genuine.

The organisation should perform the verification of the certification credential based on the following methods:

a) the certification body is certified with ISO/IEC 17024 or equivalent international standards;

b) the certification body and the certification credential are recognised by the government or authorised bodies; and

c) the certification credential is verifiable via the official website or official letters from the certification body for expiry, recognition and genuinity.

The organisation or cyber security professional should be registered with the Malaysia Board of Technologists (MBOT) as professional technologist under the Cyber Security Technology Field.

## 8. Requirements of Continuing Professional Development (CPD)

The CPD is a program to maintain the certification credential of cyber security professional in the organisation. The CPD ensure cyber security professional continuously updated and be relevant to the industry in addressing cyber security at the organisation, national and international levels.

The benefits of CPD for the organisation and the cyber security professional are as follows:

a) raise profile and credibility;

b) increase reputation;

c) networking;

d) recognition;

e) build confidence;

f) talent retention;

g) career advancement;

h) increase revenue potential; and

i) continuing education.

The organisation shall provide a yearly CPD plan associated with the certification credential requirements from a recognised body to ensure cyber security professional demonstrates personal commitment to practice cyber security and professionalism in a responsible way. Example of CPD plan is as shown in Annex C.

## 9. Professional certification

The professional certification is required for an organisation to develop capable manpower in managing cyber security and to assure qualification to perform cyber security job roles and tasks.

The benefit of professional certification for the organisation and the cyber security professional are as listed below:

a) capable and qualified cyber security resources;

b) trustworthy cyber security resources; and

c) ethical cyber security resources.

The professional certification shall be provided by the certification body with the following criteria.

a) Independent assessment - the formation of a judgement, separate and independent from any personal or professional biases and prejudice

b) Examination impartiality - examination related decisions should be based on objective criteria, rather than on the basis of bias, prejudice, or preferring the benefit to one person over another for improper reasons.

c) Trainers' competencies - a requirement that trainers have the necessary knowledge and skills to deliver and teach the training content

## 10. Cyber security professional technologist and certified technician

Cyber security certified technician is a recognition by the organisation for their cyber security practitioner at the national level.

Cyber security professional technologist is a recognition by the organisation for their cyber security professionals at the national level.

The benefits of both cyber security professional technologist and certified technician are as follows:

a) develop, foster and maintain a national culture of security;

b) establish an effective mechanism for cyber security knowledge dissemination at the national level;

c) validate minimum requirements and qualifications for cyber security professionals; and

d) help to retain cyber security professional in the organisation

Under the Act 768, *Technologists and Technicians Act 2015*, a recognised cyber security professional should be admitted as a professional technologist which carries the title prefix of "Ts." and a recognised cyber security certified technician which carries the title prefix of "Tc.", with the MBOT.

# Annex A
(informative)

## Knowledge, Skills and Attitude (KSA) descriptors

**Table A.1. KSA elements for digital forensic first responder**

| Element code | KSA element |
|---|---|
| K1 | Understanding of digital evidence identification |
| K2 | Understanding of digital evidence collection |
| K3 | Understanding of digital evidence acquisition |
| K4 | Understanding of digital evidence preservation |
| K5 | Understanding of legal requirements for digital evidence |
| S1 | Is able to physically disassemble digital devices |
| S2 | Is able to conduct acquisition from digital devices |
| S3 | Is able to preserve digital evidence |
| S4 | Is able to document the entire digital evidence handling process |
| A1 | Meticulous in all matters relating to evidence collection, acquisition, preservation and reporting |
| A2 | Display patience and calm in all matters dealing with evidence collection, acquisition, preservation and reporting |
| A3 | Apply a structured approach to identify and assess evidence in line with defined policy and Standard of Procedures (SOPs) |
| A4 | Maintain ethical conduct and act as a role model including showing respect in the execution of duties related to Forensic |
| A5 | Use judgement, make decisions and apply solutions with confidence |

**Table A.2. KSA elements for penetration tester**

| Element code | KSA element |
|---|---|
| K1 | Knowledge of cyber security standards and framework |
| K2 | Understanding of various types of vulnerabilities and exploits |
| K3 | Knowledge of enumeration, processes security tools and technologies |
| K4 | Knowledge of cyber defence strategies |
| S1 | Is able to define the scope of penetration testing and identify relevant activities required |
| S2 | Is able to perform reconnaissance and information gathering |
| S3 | Is able to perform vulnerability analysis and identify the impact level. |
| S4 | Is able to conduct a vulnerability assessment using appropriate tools and software and document the finding |
| S5 | Is able to produce technical and management report outcome of security assessment with recommended solutions based on industry best practices. |
| S6 | Is able to conduct an exploit using appropriate tools and software and document the finding |
| A1 | Work collaboratively within a team, but also must have initiative to work independently as required, to identify, gather information and conduct attacks related to penetration testing |
| A2 | Meticulous in the design, implementation & review of policies and procedures |
| A3 | Demonstrate dedication and passion for continuous learning and professional |
| A4 | Apply a structured approach to analyse and assess vulnerabilities and exploits |
| A5 | Uphold ethical conduct & act as a role model in the execution of duties |
| A6 | Keep abreast of the latest trends, tools and vulnerabilities in the area of penetration testing |

**Table A.3. KSA elements for Industrial Control System (ICS) security analyst**

| Element code | KSA element |
|---|---|
| K1 | Knowledge of fundamentals of ICS security |
| K2 | Knowledge of the various types of ICS vulnerabilities |
| K3 | Knowledge of ICS security assessment methodologies |
| K4 | Knowledge of ICS defense strategies |
| K5 | Knowledge of ICS governance implementation |
| S1 | Is able to identify, classify and investigate potential weakness points |
| S2 | Is able to perform ICS security assessment |
| S3 | Is able to identify the ICS Security defense strategies and the implementation |
| A1 | Work collaboratively within a team, but also must have the initiative to work independently as required, to identify, gather information and conduct attacks related to testing |
| A2 | Meticulous in choosing the right types of security assessment, methodologies and tools |
| A3 | Demonstrate dedication and passion for continuous learning and professional development |
| A4 | Apply a structured approach to analyse and assess vulnerabilities and exploits |
| A5 | Maintain ethical conduct and act as a role model in the execution of duties related to security assessment |
| A6 | Remain up to date with the latest trends, tools and vulnerabilities in the area of security assessment |

# Annex B
(informative)

## Certification credential

**Table B.1. Certification credentials from Malaysia certification body**

| No. | Certification credential | Certification body |
|---|---|---|
| 1 | Global ACE Certified Cyber Defender Associate (CCDA) | CyberSecurity Malaysia |
| 2 | Global ACE Certified Secured Applications Practitioner (CSAP) | CyberSecurity Malaysia |
| 3 | Global ACE Certified Penetration Tester (CPT) | CyberSecurity Malaysia |
| 4 | Global ACE Certified Digital Forensics First Responder (CDFFR) | CyberSecurity Malaysia |
| 5 | Global ACE Certified Information Security Management System (CISMS-Auditor) | CyberSecurity Malaysia |
| 6 | Global ACE Certified IP Associates (CIPA) | CyberSecurity Malaysia |
| 7 | Global ACE Certified IT Associates (CITA) | CyberSecurity Malaysia |
| 8 | Global ACE Certified Information Security Awareness Manager (CISAM) | CyberSecurity Malaysia |

**Table B.2. Certification credentials from relevant international certification bodies**

| No. | Certification credential | Certification body |
|---|---|---|
| 1 | Certified Secure Computer User (CSCU) | International Council of Electronic Commerce Consultants (EC-Council) |
| 2 | Certified Ethical Hacker (CEH) | International Council of Electronic Commerce Consultants (EC-Council) |
| 3 | Computer Hacking Forensic Investigator (CHFI) | International Council of Electronic Commerce Consultants (EC-Council) |
| 4 | Certified Network Defence Architect (CNDA) | International Council of Electronic Commerce Consultants (EC-Council) |
| 5 | Certified Chief Information Security Officer (CCISO) | International Council of Electronic Commerce Consultants (EC-Council) |
| 6 | Security5 | International Council of Electronic Commerce Consultants (EC-Council) |
| 7 | EC-Council Certified Security Analyst (ECSA) | International Council of Electronic Commerce Consultants (EC-Council) |
| 8 | EC-Council Certified Incident Handler (ECIH) | International Council of Electronic Commerce Consultants (EC-Council) |
| 9 | EC-Council Certified Security Specialist (ECSS) | International Council of Electronic Commerce Consultants (EC-Council) |
| 10 | Licensed Penetration Tester (LPT) | International Council of Electronic Commerce Consultants (EC-Council) |

**Table B.2. Certification credentials from relevant international certification bodies** *(continued)*

| No. | Certification credential | Certification body |
|---|---|---|
| 11 | EC-Council Network Security Administrator (ENSA) | International Council of Electronic Commerce Consultants (EC-Council) |
| 12 | EC-Council Disaster Recovery Professional (EDRP) | International Council of Electronic Commerce Consultants (EC-Council) |
| 13 | EC-Council Certified Security Programmer (ECSP) | International Council of Electronic Commerce Consultants (EC-Council) |
| 14 | CompTIA A+ | Computing Technology Industry Association (CompTIA) |
| 15 | CompTIA Network+ | Computing Technology Industry Association (CompTIA) |
| 16 | CompTIA Security+ | Computing Technology Industry Association (CompTIA) |
| 17 | CompTIA Advance Security Practitioners (CASP) | Computing Technology Industry Association (CompTIA) |
| 18 | CompTIA Server+ | Computing Technology Industry Association (CompTIA) |
| 19 | CompTIA Linux+ | Computing Technology Industry Association (CompTIA) |
| 20 | Certified Information Systems Auditor (CISA) | Information Systems Audit and Control Association (ISACA) |
| 21 | Certified Information Security Manager (CISM) | Information Systems Audit and Control Association (ISACA) |
| 22 | Certified in Risk and Information Systems Control (CRISC) | Information Systems Audit and Control Association (ISACA) |
| 23 | Cisco Certified Network Associate Security (CCNA® Security) (Associate Level) | CISCO Systems (CISCO) |
| 24 | Cisco Certified Network Professional Security (CCNP® Security) (Professional Level) | CISCO Systems (CISCO) |
| 25 | Certified Information Privacy Professional (CIPP) | International Association of Privacy Professionals (IAPP) |
| 26 | Certified Information Privacy Manager (CIPM) | International Association of Privacy Professionals (IAPP) |
| 27 | Certified Information Privacy Technologist (CIPT) | International Association of Privacy Professionals (IAPP) |
| 28 | Certified Information System Security Professional (CISSP) | International Information System Security Certification Consortium, Inc. (ISC)2 |
| 29 | Systems Security Certified Practitioner (SSCP) | International Information System Security Certification Consortium, Inc. (ISC2 |
| 30 | Certified Secure Software Lifecycle Professional (CSSLP) | International Information System Security Certification Consortium, Inc. (ISC)2 |
| 31 | DEV 304 Software Security Awareness | Escal Institute of Advanced Technologies (SANS) |
| 32 | DEV 522 Defending Web Applications Security Essentials (GWEB) | Escal Institute of Advanced Technologies (SANS) |
| 33 | DEV 536 Secure Coding for PCI Compliance | Escal Institute of Advanced Technologies (SANS) |

**Table B.2. Certification credentials from relevant international certification bodies** *(continued)*

| No. | Certification credential | Certification body |
|---|---|---|
| 34 | DEV 541 Secure Coding in Java/JEE (4-days course) (GSSP-JAVA) | Escal Institute of Advanced Technologies (SANS) |
| 35 | DEV 543 Secure Coding in C & C++ | Escal Institute of Advanced Technologies (SANS) |
| 36 | DEV 544 Secure Coding in .NET (4-days course) (GSSP-.NET) | Escal Institute of Advanced Technologies (SANS) |
| 37 | FOR 408 Computer Forensic Investigations - Windows In-Depth (GCFE) | Escal Institute of Advanced Technologies (SANS) |
| 38 | FOR 508 Advance Computer Forensic Analysis & Incident Response (GCFA) | Escal Institute of Advanced Technologies (SANS) |
| 39 | FOR 558 Network Forensics | Escal Institute of Advanced Technologies (SANS) |
| 40 | FOR 563 Mobile Device Forensics | Escal Institute of Advanced Technologies (SANS) |
| 41 | FOR 610 REM: Malware Analysis Tools & Techniques (GREM) | Escal Institute of Advanced Technologies (SANS) |
| 42 | LEG 523 Law of Data Security and Investigations (GLEG) | Escal Institute of Advanced Technologies (SANS) |
| 43 | MGT 512 SANS Security Leadership Essentials For Managers with Knowledge Compression (GSLC) | Escal Institute of Advanced Technologies (SANS) |
| 44 | SEC 501 Advance Security Essentials - Enterprise Defender (GCED) | Escal Institute of Advanced Technologies (SANS) |
| 45 | SEC 502 Perimeter Protection In-Depth (GCFW) | Escal Institute of Advanced Technologies (SANS) |
| 46 | SEC 503 Intrusion Detection In-Depth (GCIA) | Escal Institute of Advanced Technologies (SANS) |
| 47 | SEC 504 Hacker Techniques, Exploits and Incident Handling (GCIH) | Escal Institute of Advanced Technologies (SANS) |
| 48 | MGT 525 Project Management and Effective Communications for Security Professionals and Managers (GCPM) | Escal Institute of Advanced Technologies (SANS) |
| 49 | SEC 301 Intro to Information Security (GISF) | Escal Institute of Advanced Technologies (SANS) |
| 50 | SEC 401 SANS Security Essentials Bootcamp Style (GSEC) | Escal Institute of Advanced Technologies (SANS) |
| 51 | SEC 505 Securing Windows (GCWN) | Escal Institute of Advanced Technologies (SANS) |
| 52 | SEC 506 Securing Linux/Unix (GCUX) | Escal Institute of Advanced Technologies (SANS) |
| 53 | SEC 540 VoIP Security | Escal Institute of Advanced Technologies (SANS) |
| 54 | SEC 542 Web App Pen Testing and Ethical Hacking (GWAPT) | Escal Institute of Advanced Technologies (SANS) |
| 55 | SEC 560 Network Pen Testing and Ethical Hacking (GPEN) | Escal Institute of Advanced Technologies (SANS) |
| 56 | SEC 566 Implementing& Auditing the Twenty Critical Security Controls - In-Depth (GCCC) | Escal Institute of Advanced Technologies (SANS) |
| 57 | SEC 617 Wireless Ethical Hacking, Pen Testing and Defences (GAWN) | Escal Institute of Advanced Technologies (SANS) |
| 58 | SEC 660 Advance Penetration Testing, Exploits, and Ethical Hacking (GXPN) | Escal Institute of Advanced Technologies (SANS) |

**Table B.2. Certification credentials from relevant international certification bodies** *(concluded)*

| No. | Certification credential | Certification body |
|---|---|---|
| 59 | FOR 572: Advance Network Forensics: Threat Hunting, Analysis, and Incident Response (GNFA) | Escal Institute of Advanced Technologies (SANS) |
| 60 | FOR 578: Cyber Threat Intelligence (GCTI) | Escal Institute of Advanced Technologies (SANS) |
| 61 | SEC 575: Mobile Device Security and Ethical Hacking (GMOB) | Escal Institute of Advanced Technologies (SANS) |
| 62 | ICS 410: ICS/SCADA Security Essentials (GICSP) | Escal Institute of Advanced Technologies (SANS) |
| 63 | Associate Business Continuity Professional (ABCP) | Disaster Recovery Institute International (DRII) |
| 64 | Certified Business Continuity Professional (CBCP) | Disaster Recovery Institute International (DRII) |
| 65 | Master Business Continuity Professional (MBCP) | Disaster Recovery Institute International (DRII) |
| 66 | Certified Business Continuity Auditor (CBCA) | Disaster Recovery Institute International (DRII) |
| 67 | Certified Business Continuity Lead Auditor (CBCLA) | Disaster Recovery Institute International (DRII) |

# Annex C
(informative)

## Continuing Professional Development (CPD) plan

**Table C.1. CPD categories and plans**

| No | Category | CPD activities | Recommended CPD hours | Yearly maximum hours per category |
|---|---|---|---|---|
| 1 | Continuous education activities recognised | a) Conferences, seminars, workshops<br>b) Chapter programs, meetings and related activities<br>c) Formal learning such as post graduate studies or professional certifications<br>d) In-house cyber security training | 6 CPD hours per day | 20 hours |
| | | Webinars | 1 CPD hour per day for 1 webinar session | |
| 2 | Certification training | Attending cyber security training course | 6 CPD hours per day | 30 hours |
| 3 | Passing related professional examinations. | Encourage members to obtain other professional certifications. | 5 CPD hours per certification | 10 hours |
| 4 | Vendor based seminars/events | Vendor based seminars/events related to cyber security. | 1 CPD hour per session | 2 hours |
| 5 | Book review. | Provide 250-words review and submit to the organisation | 2 CPD hours per review | 4 hours |
| 6 | Review cyber security white papers. | The papers must have educational aspects. | 1 CPD hour per review | 2 hours |
| 7 | Publication of articles, monographs and books | a) Journal/ conference paper<br>b) Magazine/article<br>c) Books<br>d) Book chapter | a) 8 CPD hours per paper<br>b) 4 CPD hours<br>c) 10 CPD hours<br>d) 6 CPD hours | 20 hours |
| 8 | Contributions to the information security community | Include works performed that contribute to the information security profession (i.e. research development, certification review manual development, Knowledge Centre Contributor) | 2 CPD hours per categories | 10 hours |
| 9 | Teaching / lecturing / presenting | Development and delivery of educational presentations related to cyber security; | 2 CPD hours for each hour presentation | 20 hours |
| 10 | Current work in cyber security domain | Functional job in cyber security field | CPD is prorated based on month | 12 hours |
| 11 | Examination questions development | Develop examination question for Global ACE Certification only | 2 CPD for each accepted Question | 10 hours |

## Bibliography

[1] ISO 9001, *Quality Management Systems*

[2] ISO/IEC 17024, *Principles and requirements for a body certifying persons against specific requirements, and includes the development and maintenance of a certification scheme for persons*

[3] ISO/IEC 27005, *Information technology - Security techniques - Information security risk management*

[4] ISO/IEC 27001, *Information technology - Security techniques - Information security management systems - Requirements*

[5] ISO/IEC 27002, *Information technology - Security techniques - Code of practice for information security controls*

[6] ISO/IEC 27004, *Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and evaluation*

[7] Act 652, *The National Skills Development Act 2006*

[8] Act 768, *Technologists and Technicians Act 2015*

[9] OIC-CERT Journal of Cyber Security, 2018, 1.1:32-40, *Developing a Competency Framework for Building Cybersecurity Professionals*

[10] Global Accredited Cybersecurity Education Certification, *The Global ACE Certification*

[11] Global Accredited Cybersecurity Education (ACE) Scheme, *Fostering International Collaboration and Engagement, Consultancy Support Services (CS2) Limited Nigeria*

[12] *Guideline to Determine Information Security Professionals Requirements for the CNII Agencies / Organisations*

[13] *Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA)*

## Acknowledgements


**Members of the Security, Trust and Privacy Working Group**

| | |
|---|---|
| Mr Thaib Mustafa (Chairman) | Telekom Malaysia Berhad |
| Prof Dr Shahrulniza Musa (Vice Chairman) | Universiti Kuala Lumpur |
| Mr Lee Hwee Hsiung (Draft lead) | CyberSecurity Malaysia |
| Ms Norkhadhra Nawawi (Secretariat) | Malaysian Technical Standards Forum Bhd |
| Ms Koh Hsi-Pin | Communication Convergence Professional Society |
| Raj Kumar Kunhiraman | Cyber Intelligence Sdn Bhd |
| Mr Ruhama Mohammed Zain | CyberSecurity Malaysia |
| Mr Cheng Wai Kok | K2Baseline Sdn Bhd |
| Mr Clement Arul | Kaapagam Technologies Sdn Bhd |
| Mr Omar Mazlan | Malaysia Digital Economy Corporation (MDEC) Sdn Bhd |
| Mr Lee Han Ther | Maxis Broadband Sdn Bhd |
| Mr Mohamad Isa Razhali | MEASAT Broadcast Network Systems Sdn Bhd |
| Mr Harme Mohamed/<br>Ms Azleyna Ariffin/<br>Ms Siti Hajar Roslan | National Cyber Security Agency |
| Mr Mohd Azrin Md Nor | Telekom Malaysia Berhad |
| Prof Rabiah Ahmad | Universiti Teknikal Malaysia Melaka |


**MALAYSIAN TECHNICAL STANDARDS FORUM BHD**

MCMC Centre of Excellence (CoE)
Off Persiaran Multimedia, Jalan Impact
63000 Cyberjaya,
Selangor Darul Ehsan

Tel: (+603) 8320 0300
Fax: (+603) 8322 0115
Website: www.mtsfb.org.my