## Course 1 – Security Awareness Training for Administrators & Security Professionals (SAASP)

**Duration** – 1 day

**Course Content** – Course will give attendees a realistic view of the current threat landscaping that shall lead professionals for a better understanding of what needs to be protected beyond the traditional defence and the legal obligations. Attendees will gain expertise on how to identify Web Applications & Servers security risks, how to prevent them and how security incidents are identified and responded to within the organisation.

### Who is this course for?

The course is intended for Administrators and Security Professionals managing Information, & Communications Technology within businesses whose operation is connected to the cyber space.

### Agenda:

1. **Introduction – Threat Landscape**
   a. The world around us
   b. Examples of incidents
   c. Cost of incidents
   d. Attacker's viewpoint

2. **Privacy regulation made simple**
   a. GDPR & Privacy regulation and its impact on IT & Security Professionals

3. **Pushing the perimeter**
   a. Beyond the traditional defences into the Dark Web and AI

4. **The 10 Commandments to a secure organisation**
   a. 10 most important things to focus on when securing an organisation

5. **Web Application / Server**
   a. Security risks and methods for preventing them

6. **Table top exercise**
   a. Gamification element to visualise different cyber incidents and the ways participants would respond to the incident

**Course 2 – The Certified Information Systems Security Professional (CISSP) certification**[1]

**Duration** – 5 days

**Course Content** – Course is aligned with ISC requirements and will prepare attendees to pass the official exam. It will train attendees to become an information security professional who defines all aspects of IT security, including architecture, design, management, and controls.

## Who is the course for?

The course is intended for professionals who have at least five years of recent full-time security professional work experience in two or more of the eight domains of the CISSP Common Body of Knowledge (CBK). The CISSP CBK is recommended for experienced IT security-related practitioners, auditors, consultants, investigators, or instructors, including network or security analysts and engineers, network administrators, information security specialists, and risk management professionals, who are pursuing CISSP training and certification to acquire the credibility and mobility to advance within their current computer security careers or to migrate to a related career. Through the study of all eight (8) CISSP CBK domains, students will validate their knowledge by meeting the necessary preparation requirements to sit the CISSP certification exam.

## Agenda:

**Day 1**

1. **Security and Risk Management** (Security, Risk, Compliance, Law, Regulations, and Business Continuity)
    a. Confidentiality, integrity, and availability concepts
    b. Security governance principles
    c. Compliance
    d. Legal and regulatory issues
    e. Professional ethic
    f. Security policies, standards, procedures and guidelines

2. **Asset Security** (Protecting Security of Assets)
    a. Information and asset classification
    b. Ownership (e.g. data owners, system owners)
    c. Protect privacy
    d. Appropriate retention
    e. Data security controls
    f. Handling requirements (e.g. markings, labels, storage)

[1] *ISC exam & certificate are not included and can be taken up directly with ISC.*

**Day 2**

3. **Security Engineering** (Engineering and Management of Security)
    a. Engineering processes using secure design principles
    b. Security models fundamental concepts
    c. Security evaluation models
    d. Security capabilities of information systems
    e. Security architectures, designs, and solution elements vulnerabilities
    f. Web-based systems vulnerabilities
    g. Mobile systems vulnerabilities
    h. Embedded devices and cyber-physical systems vulnerabilities
    i. Cryptography
    j. Site and facility design secure principles
    k. Physical security

4. **Communication and Network Security** (Designing and Protecting Network Security)
    a. Secure network architecture design (e.g. IP & non-IP protocols, segmentation)
    b. Secure network components
    c. Secure communication channels
    d. Network attacks

**Day 3**

5. **Identity and Access Management** (Controlling Access and Managing Identity)
    a. Physical and logical assets control
    b. Identification and authentication of people and devices
    c. Identity as a service (e.g. cloud identity)
    d. Third-party identity services (e.g. on- premise)
    e. Access control attacks
    f. Identity and access provisioning lifecycle (e.g. provisioning review)

6. **Security Assessment and Testing** (Designing, Performing, and Analysing Security Testing)
    a. Assessment and test strategies
    b. Security process data (e.g. management and operational controls)
    c. Security control testing
    d. Test outputs (e.g. automated, manual)
    e. Security architectures vulnerabilities

**Day 4**

7. **Security Operations** (Foundational Concepts, Investigations, Incident Management, and Disaster Recovery)
    a. Investigations support and requirements
    b. Logging and monitoring activities
    c. Provisioning of resources
    d. Foundational security operations concepts
    e. Resource protection techniques
    f. Incident management
    g. Preventative measures
    h. Patch and vulnerability management
    i. Change management processes
    j. Recovery strategies
    k. Disaster recovery processes and plans
    l. Business continuity planning and exercises
    m. Physical security
    n. Personnel safety concerns

**Day 5**

8. **Software Development Security** (Understanding, Applying, and Enforcing Software Security)
    a. Security in the software development lifecycle
    b. Development environment security controls
    c. Software security effectiveness
    d. Acquired software security impact

**After completing this course, the student will be able to:**

- Understand and apply fundamental concepts and methods related to the fields of information technology and security
- Align overall organizational operational goals with security functions and implementations
- Understand how to protect assets of the organization as they go through their lifecycle
- Understand the concepts, principles, structures and standards used to design, implement, monitor and secure operating systems, equipment, networks, applications and those controls used to enforce various levels of confidentiality, integrity and availability
- Implement system security through the application of security design principles and application of appropriate security control mitigations for vulnerabilities present in common information system types and architectures

- Understand the importance of cryptography and the security services it can provide in today's digital and information age
- Understand the impact of physical security elements on information system security and apply secure design principles to evaluate or recommend appropriate physical security protections
- Understand the elements that comprise communication and network security coupled with a thorough description of how the communication and network systems function
- List the concepts and architecture that define the associated technology and implementation systems and protocols at Open Systems Interconnection (OSI) model layers 1-7
- Identify standard terms for applying physical and logical access controls to environments related to their security practice
- Appraise various access control models to meet business security requirements
- Name primary methods for designing and validating test and audit strategies that support business requirements
- Enhance and optimize an organization's operational function and capacity by applying and utilizing appropriate security controls and countermeasures
- Recognize risks to an organization's operational endeavours and assess specific threats, vulnerabilities and controls
- Understand the System Lifecycle (SLC) and the Software Development Lifecycle (SDLC) and how to apply security to it; identify which security control(s) are appropriate for the development environment; and assess the effectiveness of software security

### Course 3 – The Certificate of Cloud Security Knowledge (CCSK) certification [2]

**Duration** – 3 days

**Course Content** – Course will prepare attendees with the knowledge to pass the CCSK exam, a widely recognized standard of expertise and the industry's primary benchmark for measuring cloud security skillsets.

### Who is the course for?

The CCSK course is intended to provide understanding of security issues and best practices over a broad range of cloud computing domains. As cloud computing is becoming the dominant IT system, CCSK is applicable to a wide variety of IT and information security jobs in virtually every organization. The CCSK is strongly recommended for IT auditors, system administrators and security professionals with at least 5 years of experience.

### Agenda:

**Day 1**

1. **Cloud Computing Concepts and Architecture**
   a. Definitions of Cloud Computing
      i. Service Models
      ii. Deployment Models
      iii. Reference and Architecture Models
      iv. Logical Model
   b. Cloud Security Scope, Responsibilities, and Models
   c. Areas of Critical Focus in Cloud Security

2. **Governance and Enterprise Risk Management**
   a. Tools of Cloud Governance
   b. Enterprise Risk Management in the Cloud
   c. Effects of various Service and Deployment Models
   d. Cloud Risk Trade-offs and Tools

3. **Legal Issues, Contracts and Electronic Discovery**
   a. Legal Frameworks Governing Data Protection and Privacy
      i. Cross-Border Data Transfer
      ii. Regional Considerations
   b. Contracts and Provider Selection
      i. Contracts

[2] *Cloud Security Alliance exam & certificate are not included and can be taken up directly with Cloud Security Alliance.*

- ii. Due Diligence
- iii. Third-Party Audits and Attestations
- c. Electronic Discovery
  - i. Data Custody
  - ii. Data Preservation
  - iii. Data Collection
  - iv. Response to a Subpoena or Search Warrant

### 4. Compliance and Audit Management

- a. Compliance in the Cloud
  - i. Compliance impact on cloud contracts
  - ii. Compliance scope
  - iii. Compliance analysis requirements
- b. Audit Management in the Cloud
  - i. Right to audit
  - ii. Audit scope
  - iii. Auditor requirements

**Day 2**

### 5. Information Governance

- a. Governance Domains
- b. Six phases of the Data Security Lifecycle and their key elements
- c. Data Security Functions, Actors and Controls

### 6. Management Plan and Business Continuity

- a. Business Continuity and Disaster Recovery in the Cloud
- b. Architect for Failure
- c. Management Plan Security

### 7. Infrastructure Security

- a. Cloud Network Virtualisation
- b. Security Changes with Cloud Networking
- c. Challenges of Virtual Appliances
- d. SDN Security Benefits
- e. Micro-segmentation and the Software Defined Perimeter
- f. Hybrid Cloud Considerations
- g. Cloud Compute and Workload Security

### 8. Virtualisation and Containers

- a. Major Virtualisations Categories
- b. Network
- c. Storage
- d. Containers

**Day 3**

### 9. Information Response

a. Incident Response Lifecycle

b. How the Cloud Impacts IR

### 10. Application Security

a. Opportunities and Challenges

b. Secure Software Development Lifecycle

c. How Cloud Impacts Application Design and Architectures

d. The Rise and Role of DevOps

### 11. Data Security and Encryption

a. Data Security Controls

b. Cloud Data Storage Types

c. Managing Data Migrations to the Cloud

d. Securing Data in the Cloud

### 12. Identity, Entitlement, and Access Management

a. IAM Standards for Cloud Computing

b. Managing Users and Identities

c. Authentication and Credentials

d. Entitlement and Access Management

### 13. Security as a Service

a. Potential Benefits and Concerns of SecaaS

b. Major Categories of Security as a Service Offerings

### 14. Related Technologies

a. Big Data

b. Internet of Things

c. Mobile

d. Serverless Computing

**After completing this course, the student will be able to:**

- Validate the competence gained through experience in cloud security
- Prepare for the CCSK exam

- Demonstrate your technical knowledge, skills, and abilities to effectively develop a holistic cloud security program relative to globally accepted standards
- Differentiate oneself from other candidates for desirable employment in the fast-growing cloud security market
- Gain access to valuable career resources, such as tools, networking and ideas exchange with peers
- Protect against threats with qualified professionals who have the expertise to competently design, build, and maintain a secure cloud business environment

**Course 3 – Web Application Protection (WAP)**

**Duration** – 3 days

**Course Content** – This training course provides the participants with an in-depth understanding of web application vulnerabilities, mitigation strategies, infrastructure, architecture and coding perspective which will enable participants to properly defend their organization's web assets.

### Who is the course for?

This training course provides the participants with an in-depth understanding of web application vulnerabilities, mitigation strategies, infrastructure, architecture and coding perspective which will enable them to properly defend their organization's web assets. The course is intended for IT and security professionals or anyone tasked with implementing, managing, or protecting Web applications.

### Agenda:

**Day 1**

1. **Web Basics and Authentication Security**
2. **Web Application Common Vulnerabilities and Mitigations**

**Day 2**

3. **Proactive Defence and Operation Security**
4. **Web Services Security**
5. **Web Application Technologies**

**Day 3**

6. **Secure Software Development Life cycle**
7. **Demo & Hands on Exercises**

### After completing this course, the student will be able to:

- Understand the OWASP top 10
- Design a secure web protection architecture

- Differentiate oneself from other candidates for desirable employment in the fast-growing web protection security market
- Gain access to valuable career resources, such as tools, networking and ideas exchange with peers