ISC2 CC - Certified in Cybersecurity

Exam Preparation Guide (Part-1)

Instructor: **Haris Chughtai** (**Linkedin**)

dc.expert123@gmail.com

Dated: 2024

PART-1: INTRODUCTION, EXAM & COURSE REGISTRATION, REFERENCE STUDY

INTRODUCTION

Setting the stage

About Instructor

- Instructor: **Haris Chughtai**
  - Offering this course for free course to help community to learn & grow
  - Designed the course for those who want to embark a career path in Cybersecurity by writing ISC2 CC exam but not sure where to start and how to prepare.
  - Course is designed in two parts (This deck is Part 1)
    - Part 1: ISC2 CC exam information, registration using free voucher & reference study to start preparing for exam
    - Part 2: ISC2 CC study of each domain to prepare for exam

https://www.linkedin.com/in/haris-chughtai-0054415/

dc.expert123@gmail.com

Class Format

- Online - All to join the Google meet link on/before scheduled time
- Course content - slide deck, study guides, videos, discussion, whiteboarding etc
- Turn ON your camera if you like so (not mandatory but encouraged)
- Take your own notes
- Raise your hand (in Gmeet) if need to ask questions/ clarification/ comment
- Assessment/Quiz/Reading assignment/Presentation etc (whatever works :-)

Housekeeping

- Class time & Punctuality
- Collaboration Tools
  - Google Meet - Preferred to be attended over PC/Laptop
  - Whatsapp Group
  - Google Drive for relevant course material
- Class will be recorded
- Attendance will be taken at the end of each class class
- Feel free to excuse yourself from the course if you think course is not meant for you (just message me directly)

Set the expectations right …

- Expectation is students have basic understanding about Computer Network and Cybersecurity foundation concepts
  - If not, stop here and first go through these Networking & Cybersecurity fundamental course

- Make use of ISC2 free training material and exam voucher (at least for now!)

- One of the best entry level certification to embark on Cybersecurity professional career

- **Although it's termed entry level but still not very easy exam unless you prepare well !**

CC COURSE & EXAM

Course outline and exam information

Course developed & delivered by ***Haris Chughtai***

CC Exam Information

Length of exam	2 hours
Number of items	100
Item format	Multiple choice
Passing grade	700 out of 1000 points
Exam language availability	English
Testing center	Pearson VUE Testing Center

https://www.isc2.org/certifications/cc/cc-certification-exam-outline

CC Exam Study Domains

Domain 1: Security Principles

Domain 2: Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts

Domain 3: Access Controls Concepts

Domain 4: Network Security

Domain 5: Security Operations

https://www.isc2.org/certifications/cc/cc-certification-exam-outline

CC Exam Domains Weights

Domains	Average Weight	Approx # Qs
1. Security Principles	26%	20
2. Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts	10%	7
3. Access Controls Concepts	22%	17
4. Network Security	24%	18
5. Security Operations	18%	13
Total	**100%**	75*

** You may pass just in 75 Qs*

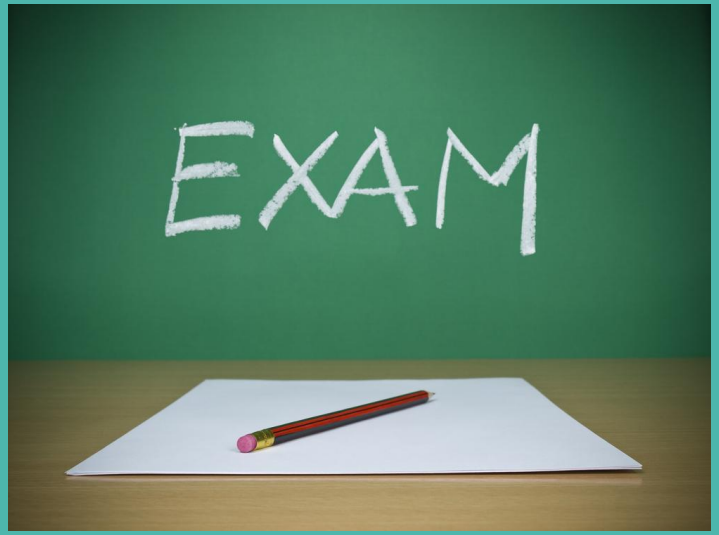
https://www.isc2.org/certifications/cc/cc-certification-exam-outline

What you need to pass the exam?

- Quieter area to focus on studies - set few hours a day for a month at least
- Mental presence - avoid social media during the class
- Attention, dedication & passion to learn and clear exam in first attempt
- Personal commitment & efforts - self motivation to review the reference study material

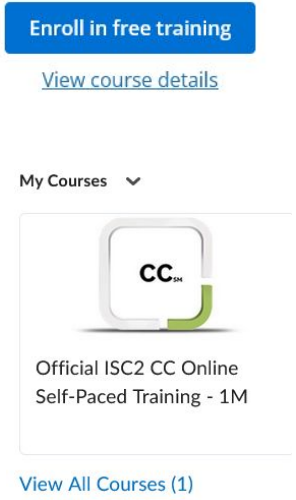
Steps to Register and Book the exam

Get it done asap meanwhile you prepare!



Register to access ISC2 CC Course

1. Create your account on ISC2 (if you don't already have one)
   - https://my.isc2.org/s/login/SelfRegister
   - Fill necessary forms with your demographic & other information
     - Fill "**Student**" if you are not clear in Employer/Position fields
     - Fill "**ISC2 Direct**" in Educational Training Program
     - You will have to read "**Account Policy**" to have enable accept option
2. Enrol your free ($0.00) access to training material
   - https://my.isc2.org/s/Candidate-Benefits/1MCC-Online-Self-Paced
3. One enrolled, click on "MY COURSES" to ensure you can access CC self paced training
4. Bookmark this link for direct access to the official study
   - https://learn.isc2.org/d2l/home/9541



*Course developed & delivered by **Haris Chughtai** (dc.expert123@gmail.com)*

Register for CC exam at Pearson VUE

1. Follow the following steps to register exam at Pearson VUE via ISC2
   - https://www.isc2.org/register-for-exam *(Alternatively you can visit Pearson VUE and type ISC2 (it will take you to ISC2 page)*
   - Fill necessary forms with your demographic & other information
     - Fill "**Student**" if you are not clear in Employer/Position fields
     - Fill "**ISC2 Direct**" in Educational Training Program
     - You will have to read "**Account Policy**" to have enable accept option

2. Select the test center near to your location (it is an **in-person exam**)

3. Select the exam time

1. Click on "Check Out"
   - It will show you the Exam fee of USD 199 + Tax (~USD 225)
   - Click on Exam Voucher and use "**CC1M12312024"** (valid for 2024) to waive the fee to $0.00

Make sure

- *Take two pieces of IDs on exam day e.g. Driving Licence, Passport, National ID card, Student ID etc*
- *Your name on ISC2 is exactly same as your ID, if not get in touch with ISC2 to have your name corrected as your ID*

WHAT SHOULD I STUDY TO PREPARE FOR THE EXAM?

Reference Study

Following **first four** should be sufficient to pass the exam but Mike Chapple course provides additional valuable knowledge.

1. ISC2 - Certified in Cybersecurity Official Study Material
   https://learn.isc2.org/d2l/home/9541
2. Fundamentals of **Networking** & **Cybersecurity** course by Haris Chughtai
3. Register as "Public" on Fortinet Training site & complete following two self paced trainings
   i. Fortinet Cybersecurity Fundamentals (FCF)
   ii. Fortinet Cybersecurity Associate (FCA)
4. Practice well each domain Flashcards
   https://quizlet.com/carla_jenkins3/folders/isc2-certified-incybersecurity/sets
5. Sample Practice Qs to revise concepts of each domain
   https://www.youtube.com/watch?v=hQz5UCR_uc0&list=PLsfuhEym5Akw3nWaix18OGE1GAO3l31rz&index=1
6. Linkedin Learning by Mike Chapple
   https://www.linkedin.com/learning/isc-2-certified-incybersecurity-cc-cert-prep/

Do your own Google/Youtube research to get exam input from those who recently passed!

On the day of your exam

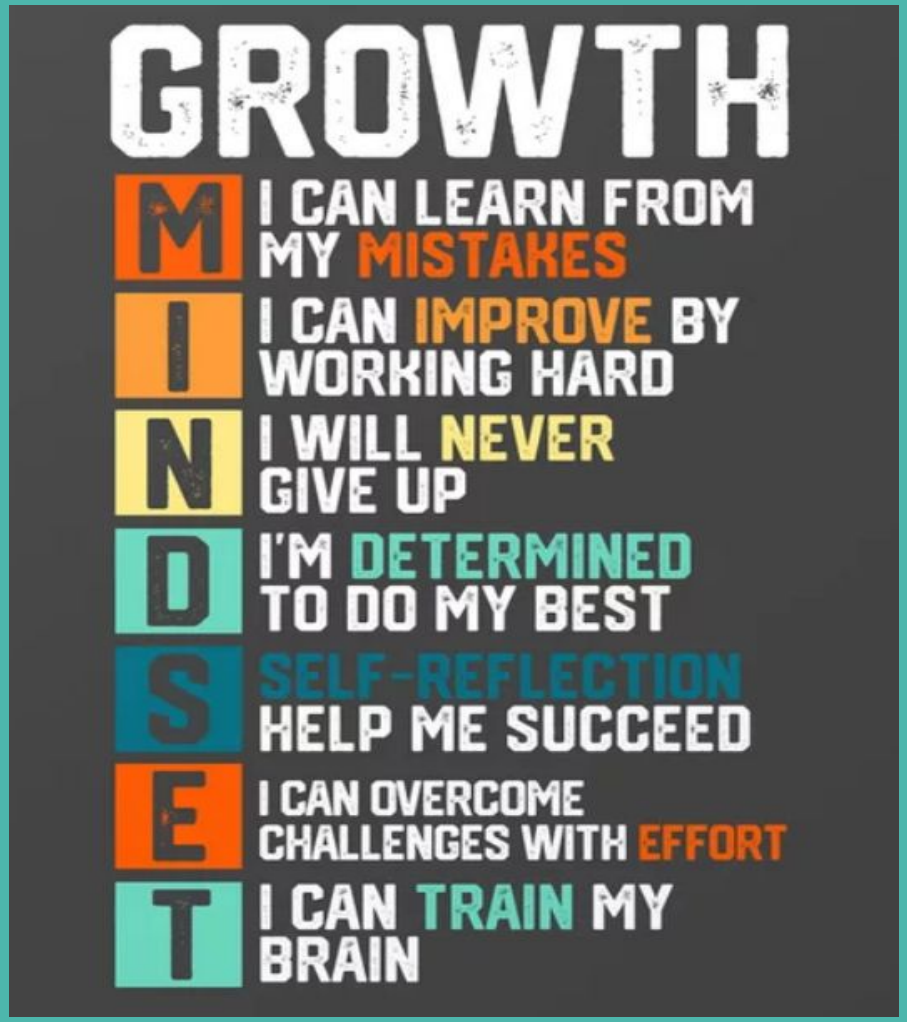
1. Reach to the VUE Pearson test center 30 min before your scheduled exam time.
   a. Give yourself enough time to overcome traffic and transportation issues
   b. Make sure you have two photo IDs with you, at least one of them must be government issued
   c. Your name on the government ID should match your name registered to ISC2

2. Keep an eye on the watch - You must attempt all the questions so time it well !
   a. Keep in mind It is not an easy exam! - Time flies when stuck !
   b. Not having time to attempt all questions reduces your chances of passing the exam !
   c. Not all questions are straight forward, some will require more time
   d. Many questions will appear unfamiliar - Don't panic it normal for most professional exams
   e. If stuck on a question, read it twice, use common sense & method of elimination to select what appears to be the best answer.

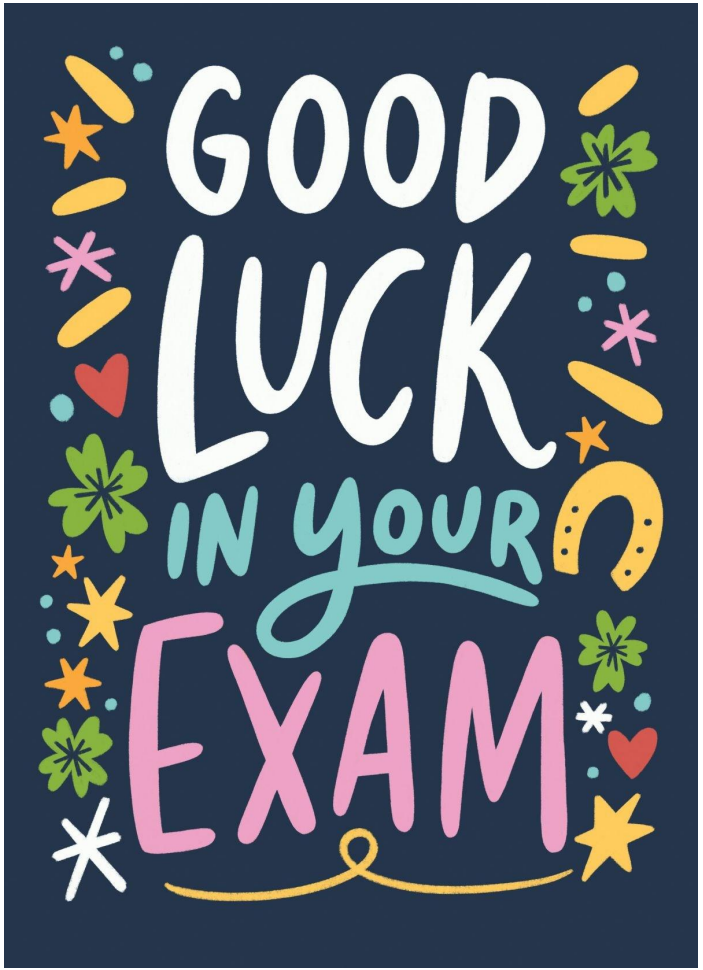
Not all the questions will be from ISC2 study material, you will need to use your logic and your base technology understanding to answer many question.

Train your brain to be a growth mindset!

Keep learning, keep growing



Course developed & delivered by ***Haris Chughtai***



*Course developed & delivered by **Haris Chughtai** (dc.expert123@gmail.com)*

ISC2 CC - Certified in Cybersecurity

Exam Preparation Guide (Part-2)

Instructor: **Haris Chughtai** (**Linkedin**)

dc.expert123@gmail.com

Dated: 2024

PART-2: KEY CONCEPTS OF ISC2 CC DOMAINS, REFERENCE STUDY

*Course developed & delivered by **Haris Chughtai** (dc.expert123@gmail.com)*

Introduction

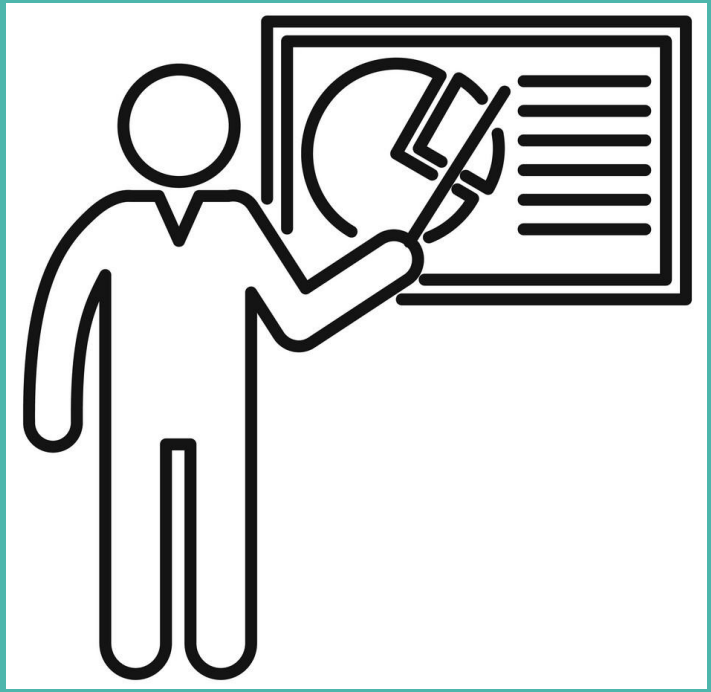
- This is Part-2 of the ISC2 CC exam preparation course
  - You can review Part-1 here
- Instructor: **Haris Chughtai**
  - Offered this course for free course to help community to learn & grow
  - Designed the course for those who want to embark a career path in Cybersecurity by writing ISC2 CC exam but not sure where to start and how to prepare.

https://www.linkedin.com/in/haris-chughtai-0054415/

dc.expert123@gmail.com

COURSE CONTENT

Study material to prepare for exam?



Course developed & delivered by ***Haris Chughtai***

CC Exam Domains

Domain 1: Security Principles

Domain 2: Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts

Domain 3: Access Controls Concepts

Domain 4: Network Security

Domain 5: Security Operations

https://www.isc2.org/certifications/cc/cc-certification-exam-outline

Domain 1: Security Principles

Domain 1:
Security Principles

1.1 Understand the security concepts of information assurance

- Confidentiality
- Integrity
- Availability
- Authentication (e.g., methods of authentication, multi-factor authentication (MFA))
- Non-repudiation
- Privacy

1.2 Understand the risk management process

- Risk management (e.g., risk priorities, risk tolerance)
- Risk identification, assessment and treatment

1.3 Understand security controls

- Technical controls
- Administrative controls
- Physical controls

1.4 Understand (ISC)² Code of Ethics

- Professional code of conduct

1.5 Understand governance processes

- Policies
- Procedures
- Standards
- Regulations and laws

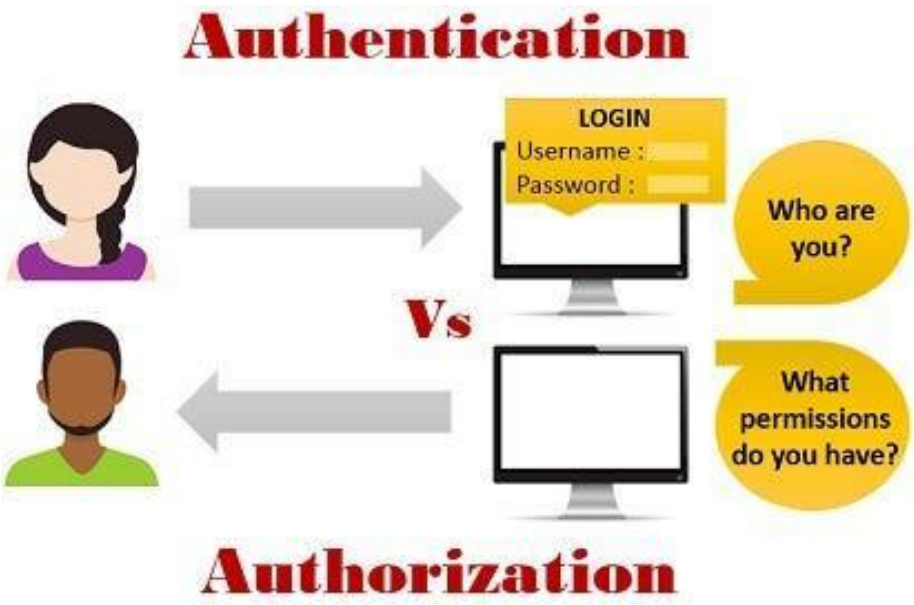
https://www.isc2.org/certifications/cc/cc-certification-exam-outline

Domain 1: Security Principles

- **CIA Triad** - Confidentiality, Integrity, Availability
  - **Confidentiality**: We must protect the data that needs protection and prevent access to unauthorized individuals.
  - **Integrity**: We must ensure the data has not been altered in an unauthorized manner
  - **Availability**: we must make sure data is accessible to authorized users when and where it is needed, and in the form and format that is required

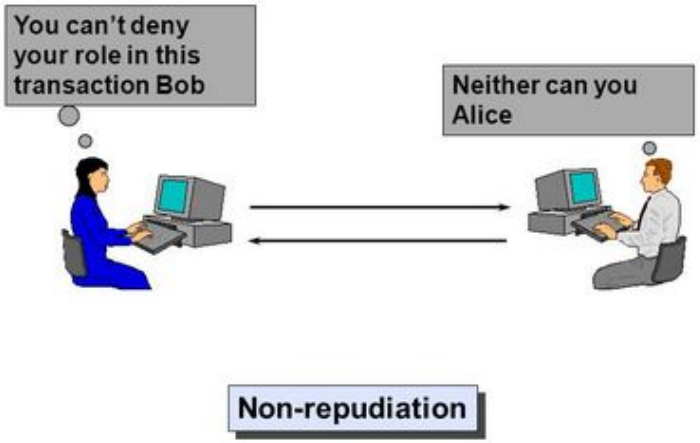
Domain 1: Security Principles

- Authentication vs Authorization
  - **Authentication** - The act of identifying or verifying the eligibility of a station, originator, or individual to access specific categories of information.
  - **Authorization** - The right or a permission that is granted to a system entity to access a system resource

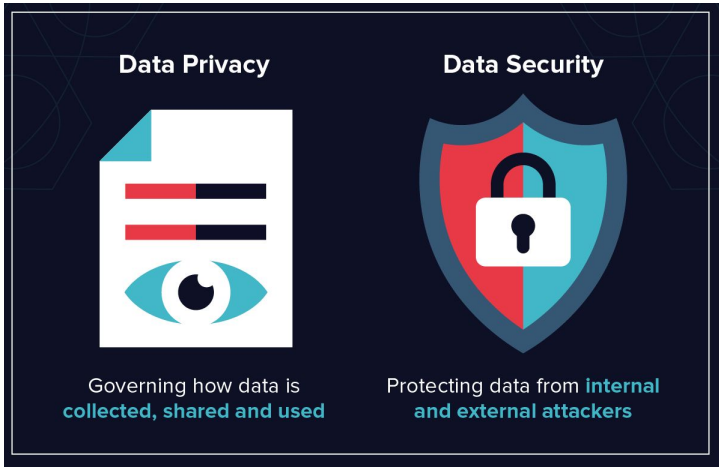


Domain 1: Security Principles

- **Non-repudiation** - The inability to deny taking an action such as creating information, approving information and sending or receiving a message. In simple terms non-repudiation in information security is the *ability to* ***prevent a denial*** *in an electronic message or transaction.*



- **Data Privacy** - Defines how data is collected, stored & distributed.
- **Data Security:** Tools, processes & controls used to safeguard data



Domain 1: Security Principles

- **Information security risk** reflects the potential adverse impacts that result from the possibility of unauthorized access, use, disclosure, disruption, modification or destruction of information and/or information systems.

- **Risk Management** - Identification, Assessment, Treatment etc. By applying risk management, we were able to assess and prioritize the risks to an organization (e.g. asset vulnerabilities that can be exploited by threats). An organization can decide whether to:

  - **Accept** the risk (ignoring the risks and continuing risky activities)

  - **Avoid** the risk (ceasing the risky activity to remove the likelihood that an event will occur)

  - **Mitigate** the risk (taking action to prevent

  - **Reduce** the impact of an event), or transfer the risk (passing risk to a third party)

Domain 1: Security Principles

Probability			
Very Likely	Acceptable Risk (medium – 2)	Unacceptable Risk (high – 3)	Unacceptable Risk (extreme – 5)
Likely	Acceptable Risk (low – 1)	Acceptable Risk (medium – 2)	Unacceptable Risk (high – 3)
Unlikely	Acceptable Risk (low – 1)	Acceptable Risk (low – 1)	Acceptable Risk (medium – 2)
Ocurrence / Impact	Low	Moderate	High

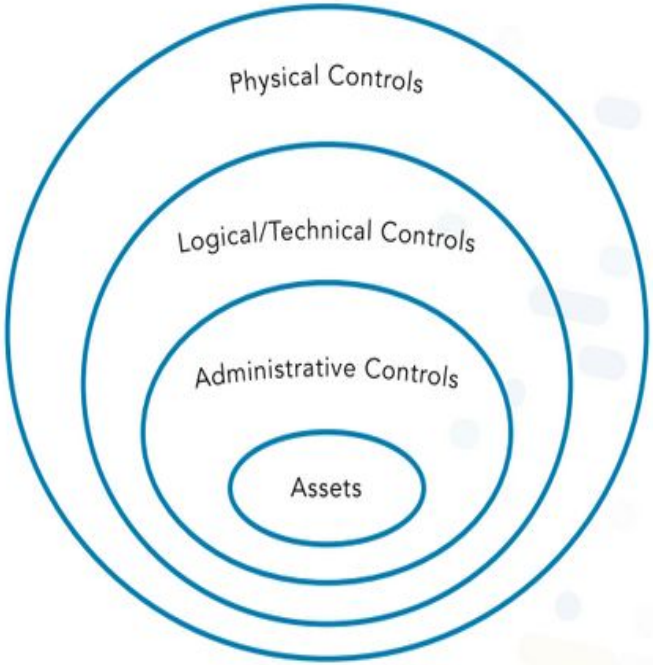
Probability x Impact = Risk

Impact (how serious is the risk?)

Domain 1: Security Principles

- **Security Controls** act as safeguards or countermeasures prescribed for an information system (or assets) to protect the confidentiality, integrity and availability of the system and its information. Implementation of security controls is expected to reduce risk to an acceptable level

- Three types of security controls
  - **Administrative controls** (also known as managerial controls) are directives, guidelines or advisories aimed at the people within the organization.
  - **Physical controls** address process-based security needs using physical hardware devices, such as a badge reader, architectural features of buildings and facilities, and specific security actions taken by people.
  - **Technical controls** (also called logical controls) are security controls that computer systems and networks directly implement through configuration.

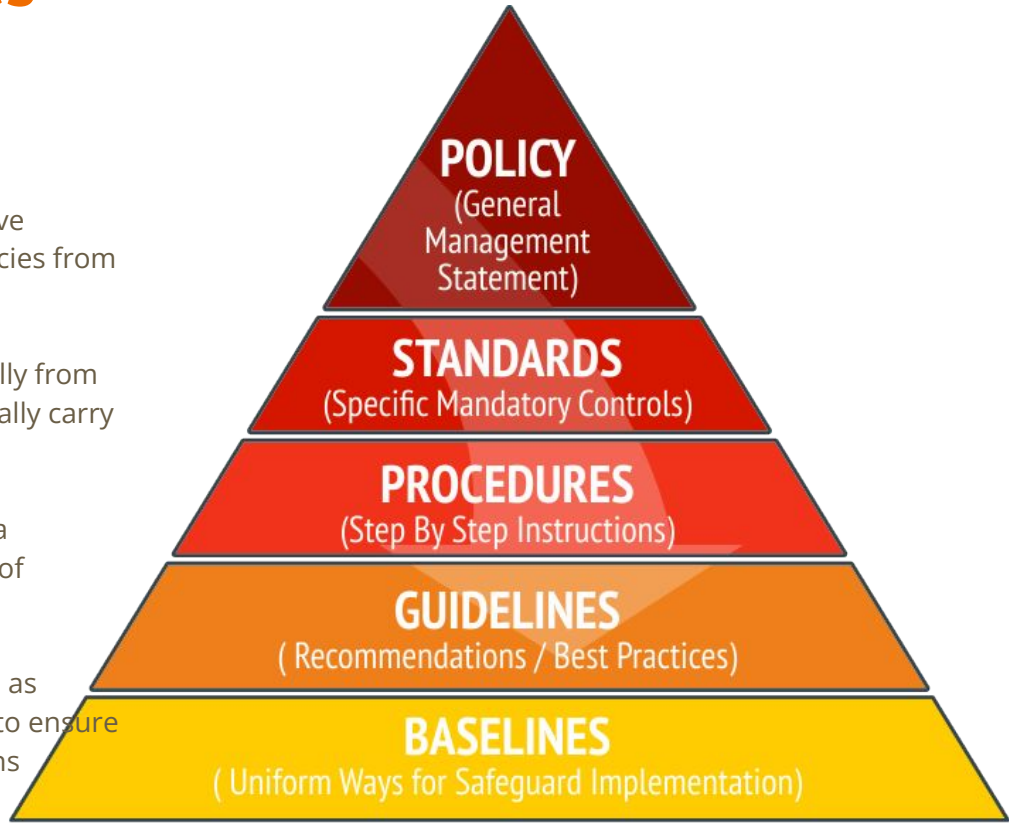


Domain 1: Security Principles

Security Governance & Processes - Policies, Standards, Procedure, Regulations & Law

Policies and Procedures shape organizational management and drive decision-making. Typically procedures are driven from policies, policies from standards, standards from regulations

- **Regulations** are commonly issued in the form of laws, usually from government (not to be confused with governance) and typically carry financial penalties for noncompliance
- **Standards** are often used by governance teams to provide a framework to introduce policies and procedures in support of regulations.
- **Policies** are put in place by organizational governance, such as executive management, to provide guidance in all activities to ensure the organization supports industry standards and regulations
- **Procedures** are the detailed steps to complete a task that will support departmental or organizational policies.



ISC2 Code of Ethics

- We must act legally and ethically in the field of cybersecurity.
- All members of (ISC)2 commit to adhere to its code of ethics

Code of Ethics Preamble

- The safety and welfare of society and the common good, duty to our principals, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
- Therefore, strict adherence to this Code is a condition of certification.

Code of Ethics Canons:

- Protect society, the common good, necessary public trust and confidence, and the infrastructure.
- Act honorably, honestly, justly, responsibly, and legally.
- Provide diligent and competent service to principals.
- Advance and protect the profession.

Domain 2: BC, DR & IR

Maintaining business operations during or after an incident, event, breach, intrusion, exploit or zero day is accomplished through the implementation of Incident Response, Business Continuity (BC), and/or Disaster Recovery (DR) plans.

Domain 2:
Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts

2.1 Understand business continuity (BC)

- Purpose
- Importance
- Components

2.2 Understand disaster recovery (DR)

- Purpose
- Importance
- Components

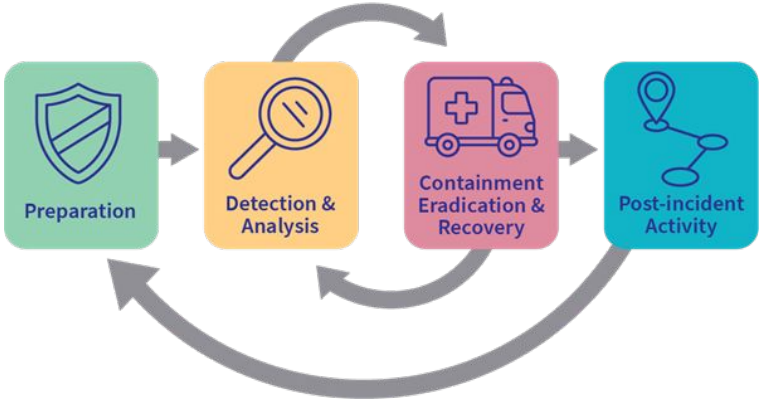
2.3 Understand incident response

- Purpose
- Importance
- Components

https://www.isc2.org/certifications/cc/cc-certification-exam-outline

Domain 2: Incident Response (IR)

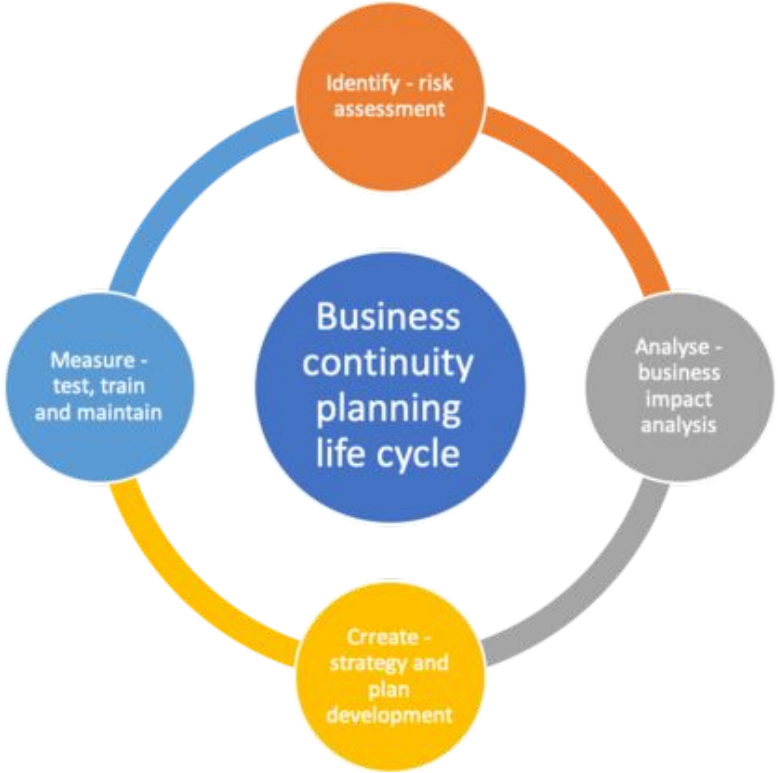
- IR is an organizational process that enables timely & effective response to cyber attacks
- Incident Response plan responds to abnormal operating conditions to keep the business operating
- The four main components of Incident Response are:
  - Preparation
  - Detection and Analysis
  - Containment, Eradication and Recovery
  - Post-Incident Activity



- Incident Response teams are typically a cross-functional group of individuals who represent the management, technical and functional areas of responsibility most directly impacted by a security incident.

Domain 2: Business Continuity Plan (BCP)

- The main focus of business continuity is to keep the operations running during crisis
- Components of the Business Continuity Plan (BCP) include details about how and when to enact the plan and notification systems and call trees for alerting the team members and organizational associates that the plan has been enacted
- The plan provides the team with immediate response procedures and checklists and guidance for management
- Business Impact Assessment (BIA) - Identify and prioritize the risks



Domain 2: Disaster Recovery (DR)

- When both the Incident Response (IR) and Business Continuity (BC) plans fail, the Disaster Recovery (DR) plan is activated to return operations to normal as quickly as possible

- The Disaster Recovery (DR) plan may include the following components:
  - executive summary providing a high-level overview of the plan
  - department-specific plans
  - technical guides for IT personnel responsible for implementing and maintaining critical backup systems
  - full copies of the plan for critical disaster recovery team members, and checklists for certain individuals

*Understand the terminologies: High Availability (**HA**), Fault Tolerance (**FT**), Single Point of Failure (**SPOF**)*

Disaster Recovery Plan and Business Continuity Plan

This slide represents the similarities and differences between a disaster recovery plan and a business continuity plan. It explains how a disaster recovery plan is a part of the business continuity plan.

- Disaster Recovery Plan: Concerned about recovering from business disruptions and obstacles
- Business Continuity Plan: Mainly concerned with keeping operations operating in the face of disruptions
- Business continuity plans are typically more resource-intensive than disaster recovery plans
- Add text here
- Add text here

Domain 3: Access Control

Administrative	• Policies and procedures • Awareness and training
Physical	• Perimeter security • Work area separation
Technical	• Idenity and access management • Loging and monitoring

Domain 3:
Access Controls Concepts

3.1 Understand physical access controls

- Physical security controls (e.g., badge systems, gate entry, environmental design)
- Monitoring (e.g., security guards, closed-circuit television (CCTV), alarm systems, logs)
- Authorized versus unauthorized personnel

3.2 Understand logical access controls

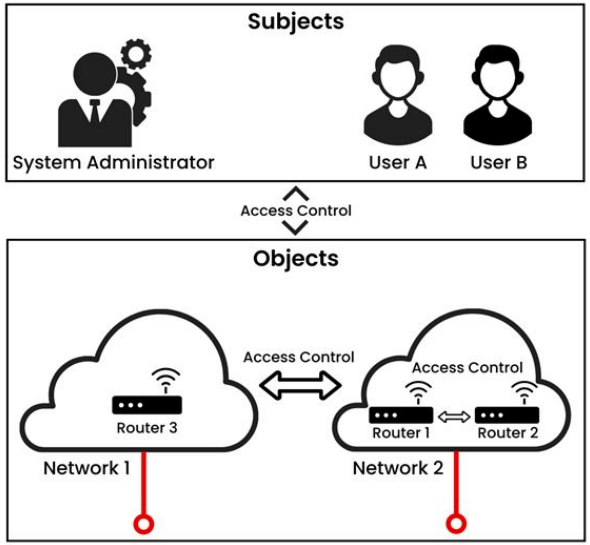
- Principle of least privilege
- Segregation of duties
- Discretionary access control (DAC)
- Mandatory access control (MAC)
- Role-based access control (RBAC)

https://www.isc2.org/certifications/cc/cc-certification-exam-outline

Domain 2: Access Control

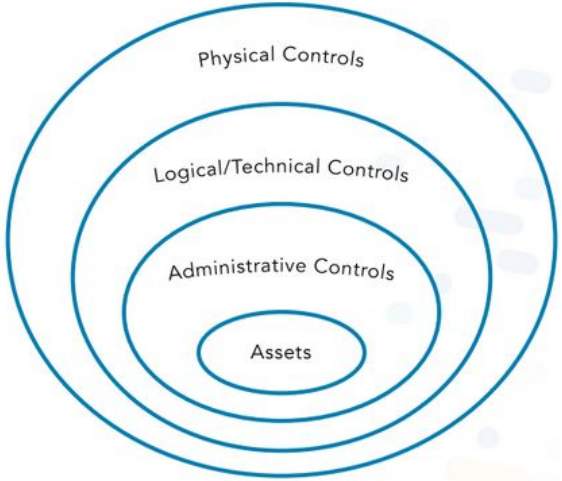
- Access is based on three elements:
  - **Subjects** (who)
  - **Objects** (what)
  - **Rules** (how and when)

- Trustworthiness and the need for access also determine access



Elements of Access Control

- **Defence in Depth (DiD):**
  - An information security strategy integrating people, technology, and operations capabilities to establish variable barriers across *multiple layers* and missions of the organization



Domain 2: Access Control

Mainly two types of Access Controls enforcement i.e. Physical & Logical/Technical

- **Physical Controls**
  - Physical access controls include security guards, fences, motion detectors, locked doors/gates, sealed windows, environmental design, lights, cable protection, laptop locks, badges, swipe cards, guard dogs, cameras, mantraps/turnstiles and alarms
  - Physical security controls (e.g., badge systems, gate entry,fences, locked doors, Mantrap/Transtiles, swipe cards, saled windows, Motion detectors, lights, guard dogs, laptop locks, security guards etc)
  - Monitoring (e.g. security guards, closed-circuit television (CCTV), alarm systems, logs)
  - Authorized versus unauthorized personnel

Domain 2: Access Control

Mainly two types of Access Controls enforcement

- Physical & Logical/Technical

- **Logical or Technical Controls**

  - Configuration or settings related controls - can be configuration settings or parameters stored as data, managed through a software graphical user interface (GUI), or they can be hardware settings done with switches, jumper plugs or other means

  - Principle of least privilege

  - Segregation of duties, Segregation of duties, two-person integrity

  - Examples of logical access control
    - Configuration settings or parameters stored as data, managed through a software
    - graphical user interface (GUI)
    - Hardware settings done with switches, jumper plugs or other means

Domain 2: Access Control

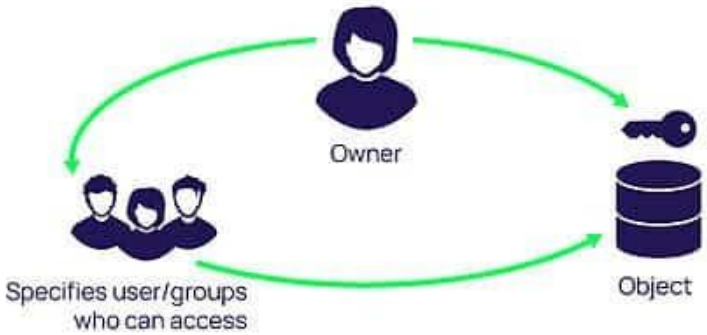
Logical or Technical Controls - MAC, DAC, RBAC

- **Mandatory access control (MAC):**
  - Mandatory access control is the principle of restricting access to objects based on the sensitivity of the information that the object contains and the authorization of the subject to access information with that level of sensitivity. **This type of access control is mandatory in the sense that subjects cannot control or bypass it.**
  - MAC model gives only the owner and custodian management of the access controls. This means the subjects/**end-user has no control over any settings** that provide any privileges to anyone
  - MAC is the highest access control (most restrictive)

Domain 2: Access Control

Logical or Technical Controls - MAC, DAC, RBAC

- **Discretionary access control (DAC):**
  - DAC allows an individual complete control over any objects they own along with the programs associated with those objects.
  - Discretionary access control is the principle of restricting access to objects based on the identity of the subject (the user or the group to which the user belongs)
  - DAC is the least restrictive access control compared to MAC model



Domain 2: Access Control

Logical or Technical Controls - MAC, DAC, RBAC

- **Role-based access control (RBAC):**
  - An access control, as the name suggests, sets up user permissions based on roles.
  - RBAC model provides access control based on the position an individual fills in an organization
  - Understand that there is a difference between Regular User Account and a Privileged User Account
    - Privileged Access Management and how it relates to risk and the CIA Triad: it reduces risk by allowing admin privileges to be used only when needed, provides confidentiality by limiting the need for administrative access that is used during routine business, ensures integrity by only allowing authorized administrative access during approved activities, and confirms availability by providing administrative access when needed

Domain 2: Access Control

Logical or Technical Controls

- **User Management (Identity Governance)**
  - New employee – account created
  - “Onboarding” – creating an account (or cloning a baseline account) for a new employee
  - Changed position – account modified
  - Temporary leave of absence – account disabled
  - Separation of employment – account deleted
  - “Offboarding” – deleting an account (or disabling then deleting an account) for a terminated employee

Domain 4: Network Security

Domain 4:
Network Security

4.1 Understand computer networking

- Networks (e.g., Open Systems Interconnection (OSI) model, Transmission Control Protocol/Internet Protocol (TCP/IP) model, Internet Protocol version 4 (IPv4), Internet Protocol version 6 (IPv6), WiFi)
- Ports
- Applications

4.2 Understand network threats and attacks

- Types of threats (e.g., distributed denial-of-service (DDoS), virus, worm, Trojan, man-in-the-middle (MITM), side-channel)
- Identification (e.g., intrusion detection system (IDS), host-based intrusion detection system (HIDS), network intrusion detection system (NIDS))
- Prevention (e.g., antivirus, scans, firewalls, intrusion prevention system (IPS))

4.3 Understand network security infrastructure

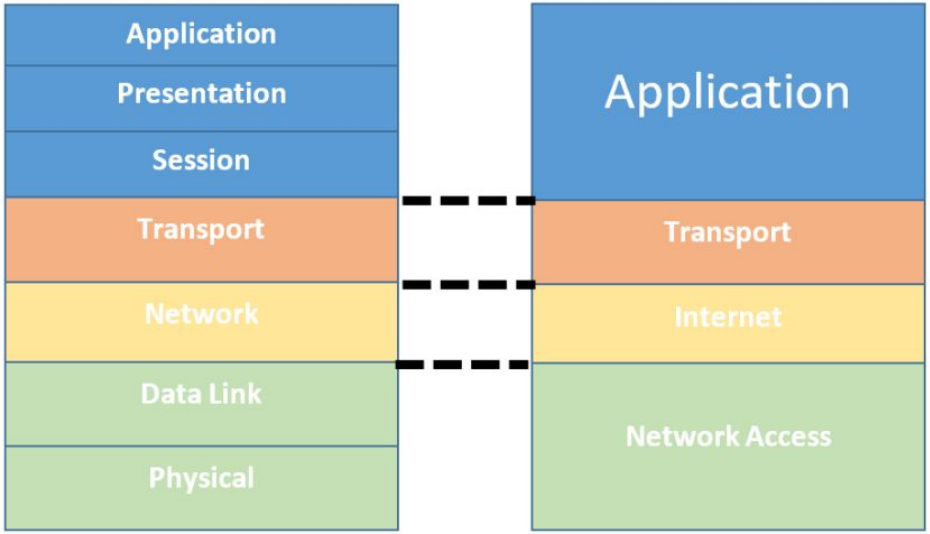
- On-premises (e.g., power, data center/closets, Heating, Ventilation, and Air Conditioning (HVAC), environmental, fire suppression, redundancy, memorandum of understanding (MOU)/memorandum of agreement (MOA))
- Design (e.g., network segmentation (demilitarized zone (DMZ), virtual local area network (VLAN), virtual private network (VPN), micro-segmentation), defense in depth, Network Access Control (NAC) (segmentation for embedded systems, Internet of Things (IoT))
- Cloud (e.g., service-level agreement (SLA), managed service provider (MSP), Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), hybrid)

https://www.isc2.org/certifications/cc/cc-certification-exam-outline

Domain 4: Network Security

Remember 7-layer OSI & 4-layer TCP/IP reference Model

- OSI - 7 Layer Model
  - The open systems interconnection (OSI) model is a conceptual framework used to describe the **flow of information from one computing device to another** operating in a networking environment. It is protocol independent.
- TCP/IP - 4 Layer Model
  - Simplified version of OSI model.
  - Provides a communication protocols suite using which **network devices can be connected <u>to the Internet.</u>** It relies on standardized protocols



OSI Model

TCP/IP Model

What's the difference between two models?

TCP/IP is a practical model that addresses specific communication challenges and relies on <u>standardized protocols</u>. In contrast, OSI serves as a conceptual comprehensive, <u>protocol-independent</u> framework designed to encompass various network communication methods.

TCP/IP model can be thought as the practical interpretation of the conceptual OSI model

Domain 4: Network Security

Types of Networks

- LAN – Local Area Network
- WLAN – Wireless Local Area Network
- WAN – Wide Area Network
- VPN – Virtual Private Network
- EPN – Enterprise Private Network
- PAN – Personal Area Network
- CAN – Campus Area Network
- MAN – Metropolitan Area Network
- SAN – Storage Area Network
- SAN – System-Area Network
- POLAN – Passive Optical Local Area Network

Network Devices

- Switches
- Access Points
- Routers
- Firewalls
- Endpoints
- Servers
- Hubs
- Printers
- Fax Machines
- Gateways
- Repeaters
- Bridges
- Modems

Network Attack Types

- DoS/DDoS
- Fragment
- Oversized Packet
- Spoofing
- Privilege Escalation
- Insider Threat
- Man-in-the-Middle
- Code/SQL Injection
- XSS (Cross Site Scripting)

Network Threat Types

- Spoofing
- DoS/DDoS
- Virus
- Worm
- Trojan
- On-Path (Man-in-the-Middle)
- Side-channel
- Phishing
- Rootkit
- Adware/Spyware
- Malware

Technologies used to Identify Threats

- IDS
- NIDS
- HIDS
- SIEM

Technologies used to Prevent Threats

- Antivirus/Antimalware
- Scans
- Firewalls
- IPS
- NIPS
- HIPS

Domain 4: Network Security

Requirements of a Data Center

- Power
- HVAC
- Fire Suppression
- Redundancy
- MOU/MOA

Cloud Service Models

- SaaS
- IaaS
- PaaS

Cloud Deployment Models

- Public
- Private
- Community
- Hybrid

Network Design Terminology

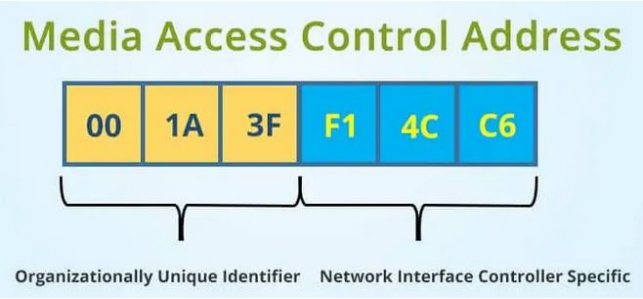
- Virtual Local Area Network (VLAN)
- Virtual Private Network (VPN)
- Network Access Control
- Defense in Depth
- Zero Trust
- Network Segmentation, e.g., microsegmentation and demilitarized zone (DMZ)

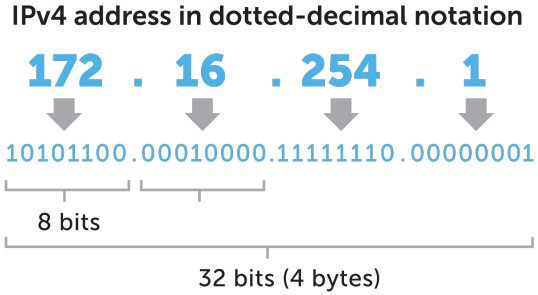
Domain 4: Network Security

- The **MAC address - Media Access Control address** is a unique identifier assigned to a NIC (Network interface controller/Card). MAC Address is also known as the Physical Address of a network device. MAC address is a unique identifier assigned to a NIC (Network interface controller/Card). MAC Address is also known as the Physical Address of a network device

- An **IP address** is a unique logical address that identifies a device on the network. IP Addresses are of two types IPv4 & IPv6. IPv4 vs IPv6: IPv4 is commonly used however IPv6 is a modernization of IPv4:is advanced which bring many new advantages including following:
  - A much larger address field (support more devices)
  - Improved security
  - Improved quality of service (QoS)

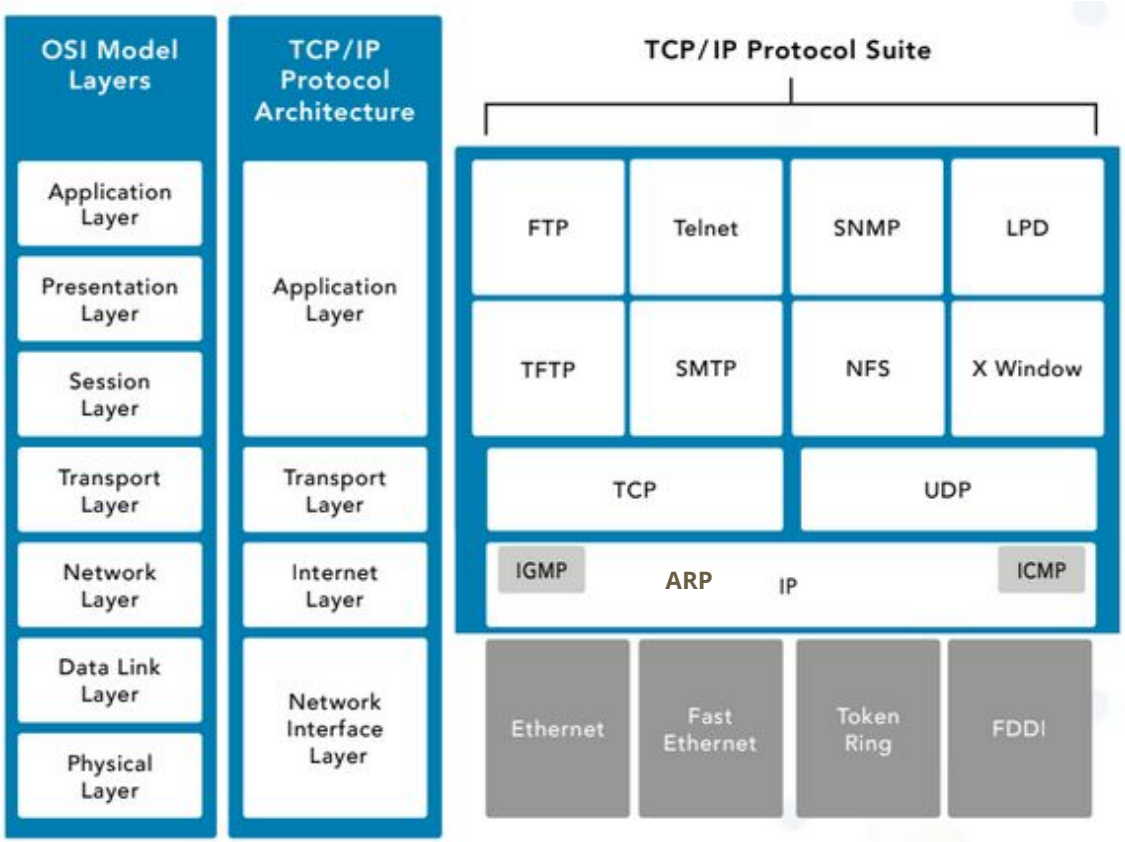
- The primary distinction between MAC and IP addresses is that MAC addresses are used to verify the computer's physical address. It uniquely identifies the network's devices. While IP addresses are logical & used to uniquely identify a device's network connection.





Domain 4: Network Security

- Common network applications & protocols in each layer of TCP/IP model



Domain 4: Network Security

- Remember these commonly used applications port numbers

Insecure Port	Protocol	Secure Alternative Port	Protocol
21 - FTP	File Transfer Protocol	22* - SFTP	Secure File Transfer Protocol
23 – Telnet	Telnet	22* - SSH	Secure Shell
25 – SMTP	Simple Mail Transfer Protocol	587 – SMTP	SMTP with TLS
37 – Time	Time Protocol	123 – NTP	Network Time Protocol
53 – DNS	Domain Name Service	853 - DoT	DNS over TLS (DoT)
80 – HTTP	HyperText Transfer Protocol	443 – HTTPS	HyperText Transfer Protocol (SSL/TLS)
143 - IMAP	Internet Message Access Protocol	993 – IMAP	IMAP for SSL/TLS
161/162 - SNMP	Simple Network Management Protocol	161/162 - SNMP	SNMPv3
445 – SMB	Server Message Block	2049 - NFS	Network File System
389 – LDAP	Lightweight Directory Access Protocol	636 - LDAPS	Lightweight Directory Access Protocol Secure

Domain 5: Security Operations

Domain 5:
Security Operations

5.1 Understand data security

- Encryption (e.g., symmetric, asymmetric, hashing)
- Data handling (e.g., destruction, retention, classification, labeling)
- Logging and monitoring security events

5.2 Understand system hardening

- Configuration management (e.g., baselines, updates, patches)

5.3 Understand best practice security policies

- Data handling policy
- Password policy
- Acceptable Use Policy (AUP)
- Bring your own device (BYOD) policy
- Change management policy (e.g., documentation, approval, rollback)
- Privacy policy

5.4 Understand security awareness training

- Purpose/concepts (e.g., social engineering, password protection)
- Importance

https://www.isc2.org/certifications/cc/cc-certification-exam-outline

Domain 5: Security Operations

Data Handling Lifecycle

Data Sensitivity Levels

- **Highly restricted**: Compromise of data with this sensitivity label could possibly put the organization's future existence at risk. Compromise could lead to substantial loss of life, injury or property damage, and the litigation and claims that would follow.
- **Moderately restricted**: Compromise of data with this sensitivity label could lead to loss of temporary competitive advantage, loss of revenue, or disruption of planned investments or activities.
- **Low sensitivity** (sometimes called "internal use only"): Compromise of data with this sensitivity label could cause minor disruptions, delays or impacts.
- **Unrestricted public data:** As this data is already published, no harm can come from further dissemination or disclosure.

Domain 5: Security Operations

- **Data privacy** is a guideline for how data should be collected or handled, based on its sensitivity and importance. Data privacy is typically applied to personal health information (PHI) and personally identifiable information (PII). This includes financial information, medical records, social security or ID numbers, names, birthdates, and contact information.
- Example of data privacy regulations/laws are GDPR/EU, PIPEDA/Canada

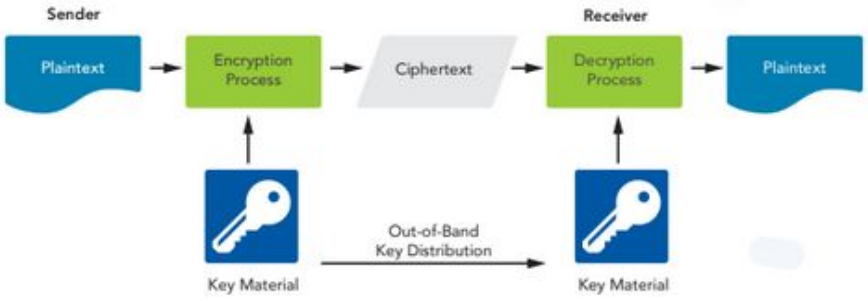
- **Data protection** signifies the strategic and procedural steps undertaken to safeguard the privacy, availability, and integrity of sensitive data, and is often interchangeably used with the term 'data security.'

Domain 5: Security Operations

- **Cryptography/Encryption** is a data security mechanism to conceal information by altering it so that it appears to be random data.
- There are two encryption mechanisms - Symmetric & Asymmetric
- Five functions of cryptographic hash - Useful, Nonreversible, Content integrity assurance, Unique, Deterministic

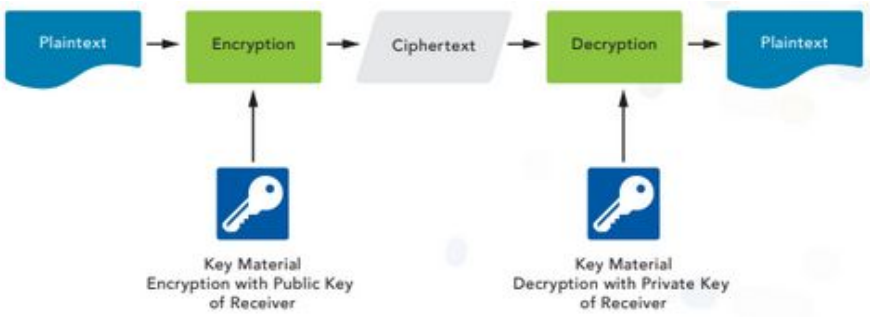
Symmetric - only one key used by sender & receiver for both encryption and decryption

Symmetric Encryption
(same Key)



Asymmetric - different keys (Public & Private) are used for encryption and decryption.

Symmetric Encryption
(different Keys)



Domain 5: Security Operations

Logging & Monitoring

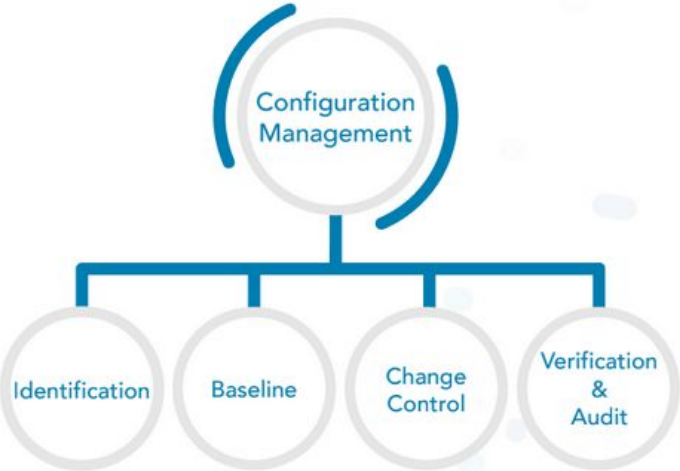
INGRESS

- Firewalls
- Gateways
- Remote authentication servers
- IDS/IPS tools
- SIEM solutions
- Anti-malware solutions

EGRESS

- Email (content and attachments)
- Copy to portable media
- File Transfer Protocol (FTP)
- Posting to web pages/websites
- Applications/application programming interfaces (APIs)

System Hardening

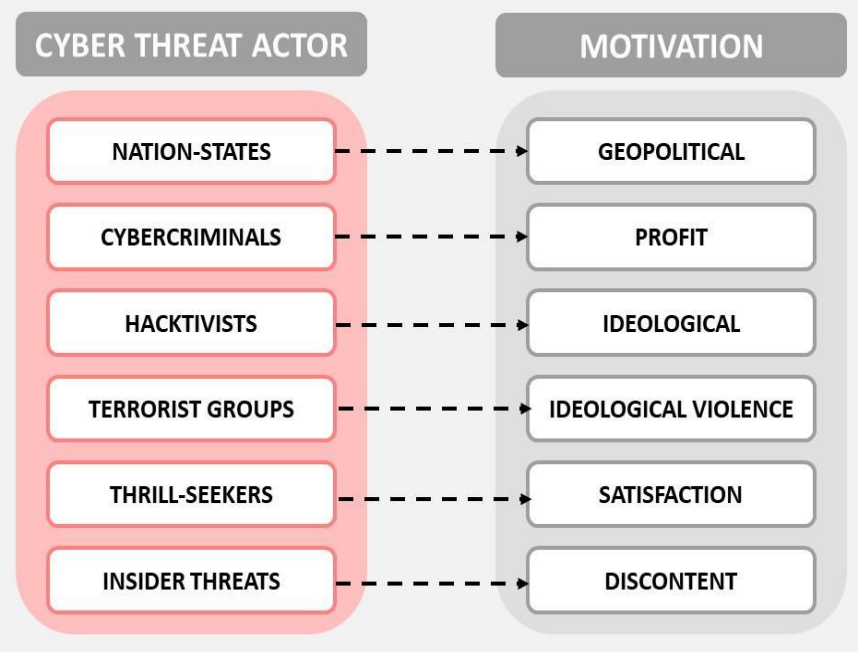


Elements of configuration management

- Inventory
- Baseline
- Updates
- Patches

Domain 5: Security Operations

Threat Actors & their motivations



Common types of Cybersecurity Attacks

- Eavesdropping, IP-Spoofing, MiTM (Man in the Middle)
- Phishing, Whale-phishing, Spear-Phishing, Drive-by Download, Trojan Horse, Botnets
- Denial of Service (DoS)
- Brute force, Password/Dictionary
- URL interpretation, DNS-Spoofing
- SQL Injection, Cross-Site-Scripting/XSS
- Trojan Horse, Cryptojacking, Ransomware

Common types of Social engineering techniques

- Baiting
- Phone phishing or vishing
- Pretexting
- Quid pro quo
- Tailgating
- False flag or false front operations

Domain 5: Security Operations

Threat Actors & Risks

- **Threat Actors:** APT, Botnet/Zombies, Malware/Virus, Social Engineering (Phishing, Vishing, Smishing), Ransomware, DDoS etc
- **Cyber Risk:** Cyber risk is based on the probability of a bad event happening to your business's information systems, leading to the loss of confidentiality, integrity, and availability of information

Malware Attacks

Viruses
Worms
Trojans
Ransomware
Cryptojacking

Spyware
Adware
Fileless malware
Rootkits

Social Engineering

Baiting
Pretexting
Phishing
Vishing (voice phishing)

Smishing
Piggybacking
Tailgating

Man-in-the-Middle

Wi-Fi eavesdropping
Email hijacking

DNS spoofing
IP spoofing
HTTPS spoofing

Denial-of-Service

HTTP flood DDoS
SYN flood DDoS
UDP flood DDoS
ICMP flood
NTP amplification

Injection

SQL injection
Code injection
OS command injection
LDAP injection

XML eXternal Entities (XXE)
Injection Cross-Site Scripting (XSS)

Domain 5: Security Operations

- **Best practices Security Policies:** Password, Acceptable Use Policy (AUP), Bring your Own Device (BYOD), Privacy policy etc

- **Security Awareness Trainings**

Reference study to prepare for the exam

Reference Study

Following **first four** should be sufficient to pass the exam but Mike Chapple course provides additional valuable knowledge.

1. ISC2 - Certified in Cybersecurity Official Study Material
   https://learn.isc2.org/d2l/home/9541

2. Fundamentals of **Networking** & **Cybersecurity** course by Haris Chughtai

3. Register as "Public" on Fortinet Training site & complete following two self paced trainings
   i. Fortinet Cybersecurity Fundamentals (FCF)
   ii. Fortinet Cybersecurity Associate (FCA)

4. Practice well each domain Flashcards
   https://quizlet.com/carla_jenkins3/folders/isc2-certified-incybersecurity/sets

5. Sample Practice Qs to revise concepts of each domain
   https://www.youtube.com/watch?v=hQz5UCR_uc0&list=PLsfuhEym5Akw3nWaix18OGE1GAO3l31rz&index=1

6. Linkedin Learning by Mike Chapple
   https://www.linkedin.com/learning/isc-2-certified-incybersecurity-cc-cert-prep/

Do your own Google/Youtube research to get exam input from those who recently passed!

On the day of your exam

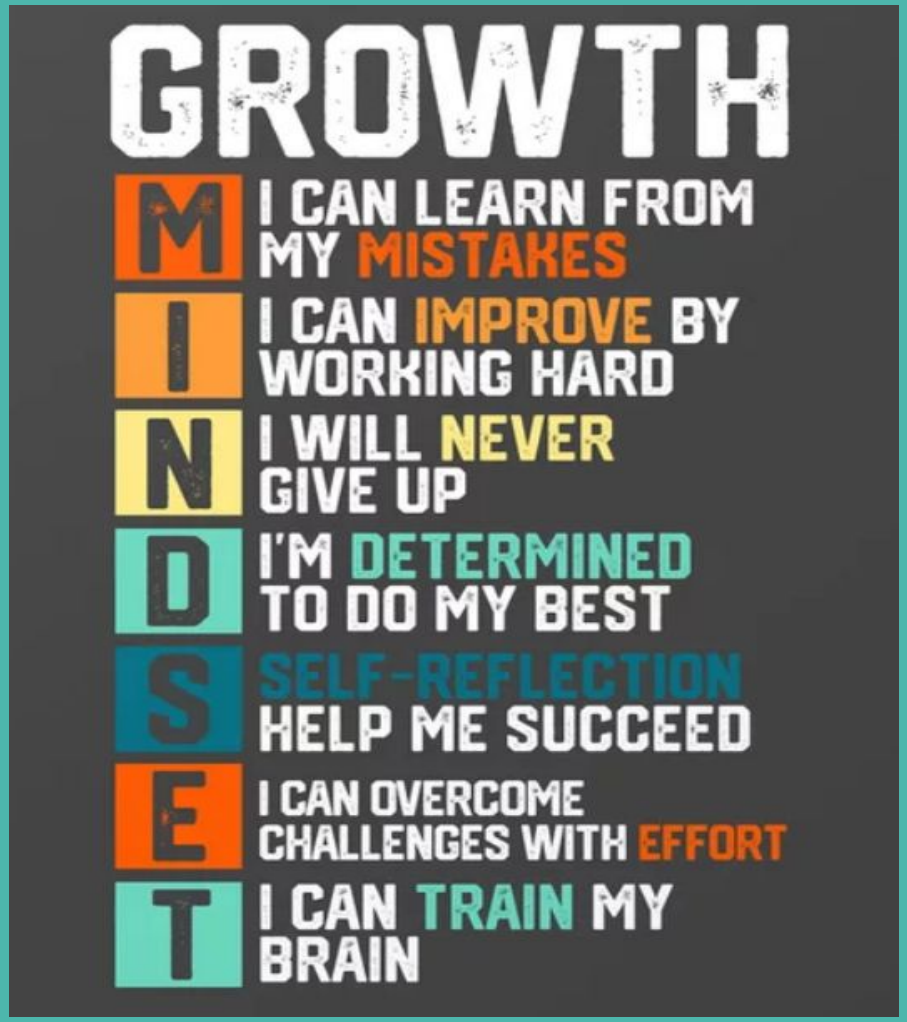
1. Reach to the VUE Pearson test center 30 min before your scheduled exam time.
   a. Give yourself enough time to overcome traffic and transportation issues
   b. Make sure you have two photo IDs with you, at least one of them must be government issued
   c. Your name on the government ID should match your name registered to ISC2

2. Keep an eye on the watch - You must attempt all the questions so time it well !
   a. Keep in mind It is not an easy exam!! - Time flies when stuck !
   b. Not having time to attempt all questions is the worst time management!
   c. Not all questions are straight forward, some will require more time
   d. Many questions will appear unfamiliar - Don't panic it normal for any professional exam
   e. If stuck on a question, read it twice, use common sense & method of elimination to select what appears to be the best answer.

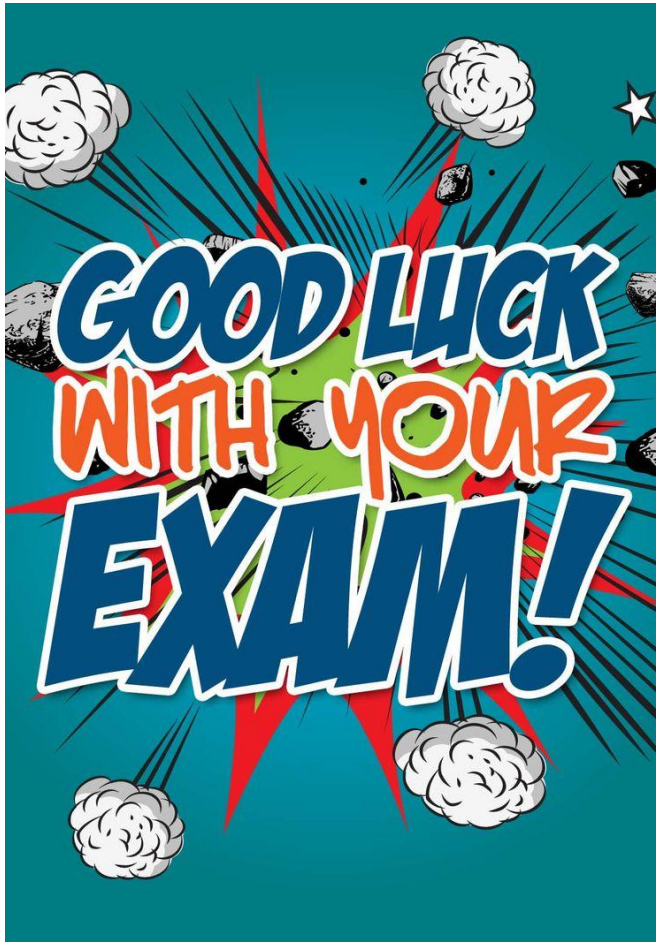
Not all the questions will be from ISC2 study material, you will need to use your logic and your base technology understanding to answer many question.

Train your brain to be a growth mindset!

Keep learning, keep growing



Course developed & delivered by ***Haris Chughtai***


GOOD LUCK
WITH YOUR
EXAM!