'An Incipient way to Learn CISSP'

1. Information Security is an Enterprise wide concern
2. Governance matters, Risk must be managed
3. Everything is Information to conduct operations
4. Not all Information is equal value to enterprise, classification & prioritization must be done
5. Security Policies govern actions by aligning all security operations (Operations Security as well) with Enterprise mission
6. Process driven business with defined procedures
7. C.I.A oriented classification of assets and access controls are the key
8. Business & Information Technology an integrated approach
9. Risk profile on the basis of Criticality & Sensitivity of Inevitable Assets
10. Secure design & architecture leads to assurance
11. Business & Technology should be supple enough
12. Eight Domains provide road map
13. Challenge is to continue operations with minimal impact & How to react
14. Compliance, Standards, Regulations are inevitable contributors
15. Communications language is the real concern

INFOSECTRAIN

Project Management "A CISSP VIEW"

In information technology world the term project is very common. You hardly found people don't have friendship with this buddy at different levels of an organized organization. I am not allowed & can't present as well the full biography of project management but would love to present a elucidating denouement here.

- Information Security Management is all about C.I.A dovetailing among People, Operations & Technology.
- Project Management is all about P.D.C.A of Business, Organization & Technology

The big question of cloud is that how to map them from an information security professional's stand point.
Well the small answer is using the system oriented approach. The term system replaces all jargons & addresses all supportive units of an organization,

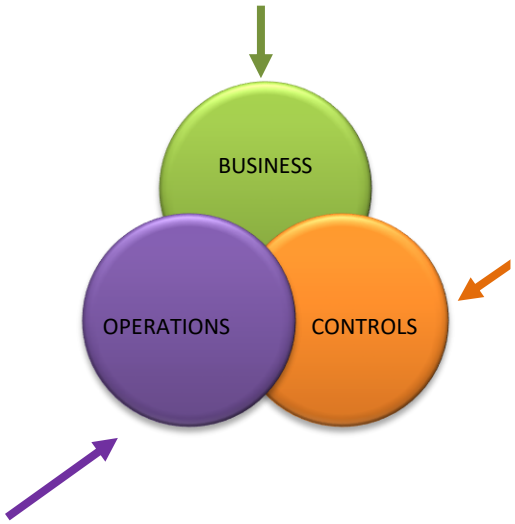
No doubt to say these questions should hit a security professional after the management's approval.

TO FULLFIL A MISSION ONE SHOULD HAVE OBJECTIVES & SCOPE DEFINED BUT THIS CAN BE DONE AFTER UNDERSTANDING THE REQUIREMENTS, THE BETTER YOU KNOW THEM BETTER YOU CAN TRANSLATE IN TERMS OF OBJECTIVE & SCOPE.

INFOSECTRAIN

A THREE SPHERE MODEL OF INFORMATION SECURITY, A PROJECT MANAGEMENT GLANCE THROUGH

1. How expensive the security goanna be to Enterprise, the cost?
2. The cost as per the fund's in hand?
3. The cost of implementation, monitoring & maintenance?
4. The outcome in terms of gains by protecting mission critical assets & managing risk?
5. Is my security plan is aligned with policies, procedure, processes?
6. Do I in compliance according to regulations & type of business?



1. Up to what level the C.I.A is satisfied?
2. Are Physical & Technical controls fulfilling the expectations of Administrative controls?
3. How effective the 3 are to manage the?
4. Do they ameliorate with culture?
5. How effective Training, Awareness & Education o Is?
6. Are those worthy (cost wise) when comparing to the risk mitigated?

1. In what manner applied controls will affect & satisfy the move to mission?
2. Is information associated with critical & sensitive assets are as needed to operate?
3. What areas needs to be focused more to mitigate the risk?
4. Is my risk mitigation technique (A.T.M.A)?
5. Is Residual risk up to the appetite of risk tolerance?
6. How strong my disaster is, the impact & recovery time?

INFOSECTRAIN

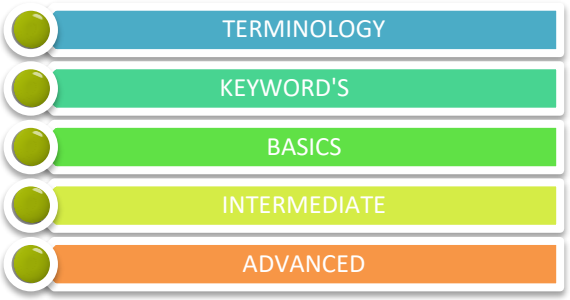
THE 8-D APPROACH OF CISSP: (A CASCADING Methodology)

The very first step to adding more branches to your skills tree is to comprehend the basics in a deep down manner. There can be heaps of approaches to learn a particular topic but the best one is that syncs with your brain in first attempt.

I always put emphasis on understanding the terminology & keywords because our brain is like a file system with inbuilt persistent storage and just requires a high level format of previously installed operating system to form a new file system while have the basics glimpse of old foundations.

As the management of anything requires a methodical and systematic approach, so here there is no exception.

Note: This top down approach is goanna work, if you follow in a step wise step manner.



- Information Security always deployed as a program me.
- In CISSP exam the context is very and really important to grab before you answer a question regardless of the question type.
- You can do this easily if you follow a structured approach as depicted in above figure.
- It's the proven way of studying anything not just only the CISSP.

TERMINOLOGY: (Generic applies holistically on whole domain)

1. SYSTEM
2. SECURITY
3. STRUCTURE
4. SCALABILITY
5. REDUNDANCY
6. RESILIANCE
7. UNIQUE
8. VIRTUAL vs. LOGICAL
9.

Assumptions to have in your knowledge arsenal:

1. It's a team work of all business units, are the part of a system
2. There is a predefined manner to introduce anything in to the system
3. Every component has a life cycle that governs it's journey in the system
4. Every plan goes as a project & of course has a deadline.
5. Prioritize, always when there is a chance.
6. Solution does not matter but the approach does.

SYSTEM

'MANAGEMENT OF ANYTHING REQUIRES MANAGEMENT OF EVERYTHING'

' A SYSTEM IS A GROUP OF DISIMILAR ELEMENTS, CO-ORDINATING WITH EACH OTHER TO ATTAIN A COMMON MISSION/GOAL/OBJECTIVE'.

By considering the above definition if any element fails to coordinate as expected by the system, make the whole system down just if any single gear fails in the above picture.
Its not necessary that always a system leads to Information Technology world, it can be a system of people, processes and in any kind of business.

If any gear requires maintenance one need to ensure that how to continue in that scenario

Visualization and of Business & Information Technology is mandatory because elusive tricks not goanna work here. So a what a system means in Business world and in the world of Information Technology and using both of them you have to develop a Information Security Program oriented system.

System is always hierarchical and organized so one should always start by looking at the basic structure that forms the backbone.

POLICIES: Also called management statement or high level view of mission an organization has. Depicts what should be done in order to keep on moving toward mission.

Policies are objective, scope oriented and system specific as the fact is there is no one size fits all solution.

PROCESS: A well defined flow of activities or tasks intended to attain business goals by utilizing the system in an optimum manner. The mission of an organization usually Service or Product delivery.

PROCEDURE: A collection of step by step instructions to address and satisfy the how part or deployment part of the policy. Basically how something proclaimed in policies should be carried out.
Procedures are as well business specific. For example

Now the deal is to tie all P's for the sake of your information security plan. Well the most difficult questions often have very simple answers.

So I would say Processes are outcome of Policies and Procedures.

Questions should always follow Suggestions if not satisfy the answer as expected.

SECURITY:

Not trying to be sophisticated in simple words just few simple questions:

Q1. Why do we need security?
Q2.What we need to secure?
Q3. How we need to secure?
Q4. What should be level of protection needed?
Q5. Is the cost more that we are trying to protect?

E.g. You are heading for an official conference from your own country, at the airport officials have tussle for your hand baggage and due to excess of weight and request you to carry only either of the items (**Assets**):
Notebook, Smart phone or the slim book of CISSP, now you have to choose:

- Smart phone holds all your personal but some official data & soft copy of your book
- Notebook entails all your smart phone data, official data and a soft copy of your book
- The book itself

If you do the **assessment** to **categorize** the **assets** as per their **priorities**, you will find to carry out your professional & personal activities (**Operations**) you must have your notebook with you.
So here you did the **Assessment**, **Categorization**, and **Prioritization** by considering their worth to keep your professional & professional life functional.
Now protecting assets on the basis of **Assessment**, **Categorization**, and **Prioritization** by curtailing their exposure and curbing their access.
E.g. As your notebook houses your professional & personal data, you want to protect its unauthorized access using a multi layer approach for defeat an ill will intention person.
To ensure this one could go for followings:

1. Ensure proper level of PHYSICAL security of notebook
2. The hotel you are staying in should have ADMINISTRATIVE way's to protect their gust belongings.
3. Technical ways you can use to protect you notebook from unauthorized access or any other misuse.

The above mentioned ways to protect your notebook are called **controls/safeguards** or **countermeasures**.

There is always a threat (possibility that luck will support adversary) & eventually you will lose your notebook and the information within that can be used for malicious purpose.

But if you don't protect your notebook using various layers of defense (assuming it's physically secured) E.g. disabling the usb ports, boot screen password, bios password and not using the DVD or CD ROM drive, login prompt enabled, hard drive is encrypted etc. there is always a possibility (threat) that someone will utilize this weakness (Vulnerability) and in simple words you are at risk of losing your data.

But if you have the full backup of your hard drive you are very much confident that you will be able to continue your **professional & personal activities** by purchasing a new notebook. This act is called 'Mitigation' because you are handling the risk by reducing its ramifications the bad one.

Other options to coupe up with such risk is you can transfer it by buying an insurance but

There is no rocket science applied here, a common sense approach when you protect **something** (**The Access**) & from **someone** (**The person who is not authorized or Unauthorized**).

Ans.1.To protects valuables.
Ans.2.Protection of ineluctable assets, necessary for survivability.
Ans3. Kind of protection
Ans4. Level of protection is high, moderate or low.

Why RISK is there?

What should be done to protect the ASSET'S?

What are the risks with information?

Responsibilities→Accountability→Liability
Putting Controls→ Least Cost
Access Control→ Least Privilege & Need to Know

STANDARDS':

Established mandatory rules, specifications & metrics, used to measure compliance against quality value etc.
Standards are usually intended for compliance purposes.

The Entity has something material & immaterial that could be subject to damage.

That damaged is called " RISK "

This chapter put's focus on how an Information Security Manager will use various methods to ameliorate the loss due to the uncertainty

Using Roles, Policies,

Asset could be anything that has value to the ORGANIZATION. Information, Process, System & eventually the Entity.

RISK: Type of damage & Type of Asset

Information is subject to being lost, tampered with or disclosed.

Impact on entity depends on the nature of their BUSINESS or INDUSTRY.

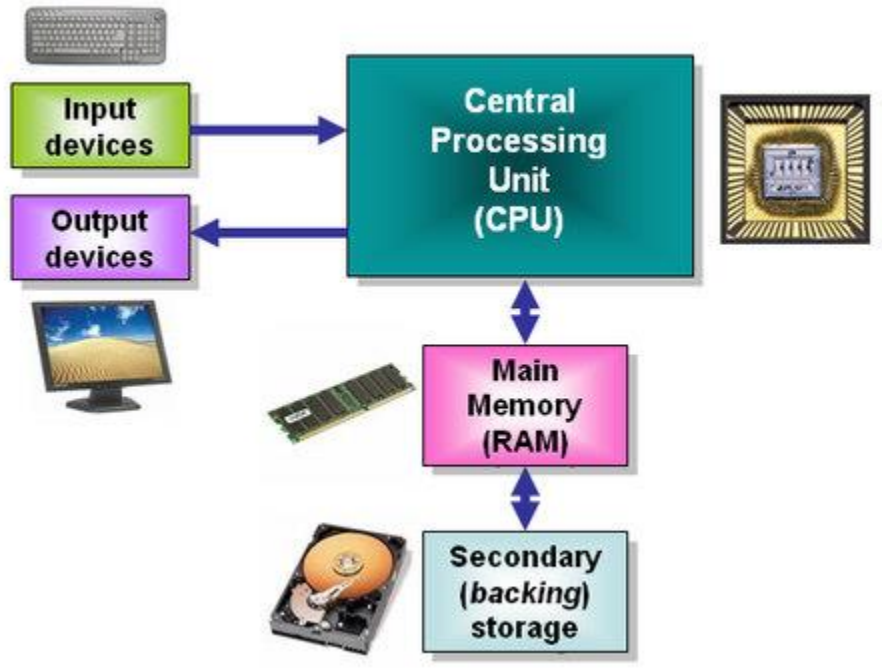
Event is the term used to define the RISK factor.

Cause or Source of RISK Direct or Indeirect

Multi Layer strategy to protect & secure their Mission Critical Assets.

A DISCPLINE TO DESIGN, IMPLEMENT, TEST & SECURE

Memory Chips: ROM, RAM



Computer Architecture:

OS=Memory, Processor, Device, Information Management

THE OS & CPU should be designed to work together.

PROCESSES & PROGRAMS: USER APPLICATION'S

CPU:

Instructions & Data

Registers, ALU (Core of the CPU), Control Unit (Traffic COP)

ALU: THE MOST POWRFUL MATHMATECIAN TO PERFORM THE LOGIC

CLU: To coordinate between the instructions & data to & from CPU or the Interface of CPU for other components.

Register: A Buffer
Cache Memory:

MULTITHREADING: THE APPLICATION CAN MANAGE THE PROCESSING OF VARIOUS THREADS AT A SINGLE PIECE OF TIME.

MULTITASKING: MANAGEMENT OF PROCESSING OF SEVERAL PROGRAMS AT ONE TIME.

USER MODE: Less trusted way of performing OPEARTIONS while doing job for a subject & much more restricted.

KERNEL MODE: Most trusted way of performing OPERATIONS access to any resources.

EXE LAUNCHES THE APPLICATION, IN-TURN PROCESS→THREADS (The smallest unit of execution that A CPU can act upon)

THREAD CAN BE IN STATE OF: RUN, READY (WAITING FOR its TURN) & BLOCKED (WATING FOR USER INPUT OR ANY OTHER.

SINGLE CORE CPU CAN HANDLE A SINGLE THREAD AT A TIME.

IRQ: TO GET CPU ATTENTION REQUIRED, USED BY PROCESS OR DEVICE DRIVER.

MASKABLE (DISABLE CAN BE TURN OFF), UNMASKABLE

MEMORY LOCATIONS ARE MANDATORY TO GET THE ACCESS OF RESOURCES..

ADDRESS BUS & DATA BUS:

A SYSTEM MORE THAN ONE CPU CAN PROCESS MORE THAN ONE THREAD SIMULTANEOUSLY

MULTI PROCESSING: IMPROVE THE PROCESSING CAPACITY

SMP OR ASMP : CAPABILITIES OR LIMITATIONS OF THE OS

THE KERNEL WILL LOAD BALANCE CALLED AFFINITY IN SMP

IN ASMP YOU HAVE THE CHOICE TO DEDICATE THE ASSIGNMENT OF THE DATA & INSTRUCTIONS TO A PARTICULAR CPU. EX: PRIORTIZING MORE & LESS SECURE PROCESS.

NOW WE HAVE MULTI CORE CPU, THE ABOVE MENTIONED APPLIES TO A SINGLE CORE C.P.U

SO WITH A DUAL CORE CPU WE CAN PROCESS TWO THREADS SIMULTENOUSLY.

CRYPTOGRAPHY

THE ART OF HIDING CONFIDENTAIL INFORMATION FROM UNINTENDED RECEPIENT.

CRYPTOSYSTEM:The mechanism of using the Cryptography
Software, Protocol, Algo, Key

XOR operation two input one output (ALGO + KEY)= CIPHER TEXT

Key is long string of Numbers, Size matters

Keysize comes in bit's and defines the key space the combinations of the keys can be created.

Ex: 2 to the power 64 in binary combination
Algo: A combinations of Mathematical equations

CRYPTOANALYSIS: Pen test of Crypto Algorithm

Different Security Services by Cryptography:

Confidentiality
Integrity (Hashing)
Authentication (Private Key) & Authorization
Non-Repudiation (Digital Signature)

Work Factor is so high of an algorithm so the bad guy can't accomplish his/her job.

Plain Text is the readable message, Applying CIPHER'S (An Algorithm)

Different Org. requires various level of C.I.A.N

Ex: Financial Services:

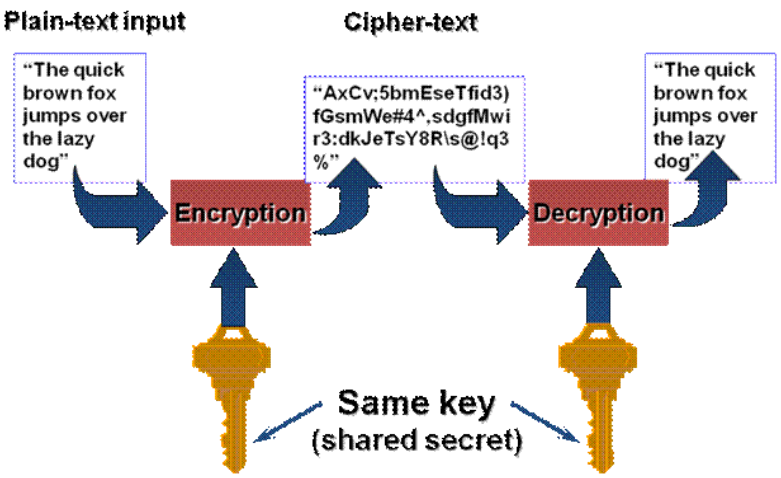
Substitution Cipher:

ABCDEFGHIJKLMNOPQRSTUVWXYZ
ZYXWVUTSRQPONMLKJIHGFEDCBA ⟸ ALGORITHIM

Key: How many spaces we goanna shift:

Transposition Cipher (Symmetric One) The alphabets are not substituted but the order is scrambled

Symmetric Cipher (Sender & Receiver utilize the same KEY) Use substitution and transposition



1. Stream

Encrypts each bit at a time no block mechanism is here. IV is the strength of the stream cipher

Seed Value: IV: Adds randomness in the algorithm to create the various patterns. A pattern is the way to produce the various combinations to make hard for CRYPTOANALYSIS

1. Block
   Each block of message is encrypted separately not the whole message as a single entity , block size may be 64, 128 bits depends on the algo

Key maintenance & scalability is a big issue.
Key Shairng (Out of Band) is the problem

N is the number of users

N(N-1)
---------- = Keys Required

2

Ex: 10 (10-1)/2 = 5*9 = 45 keys are required for 10 users

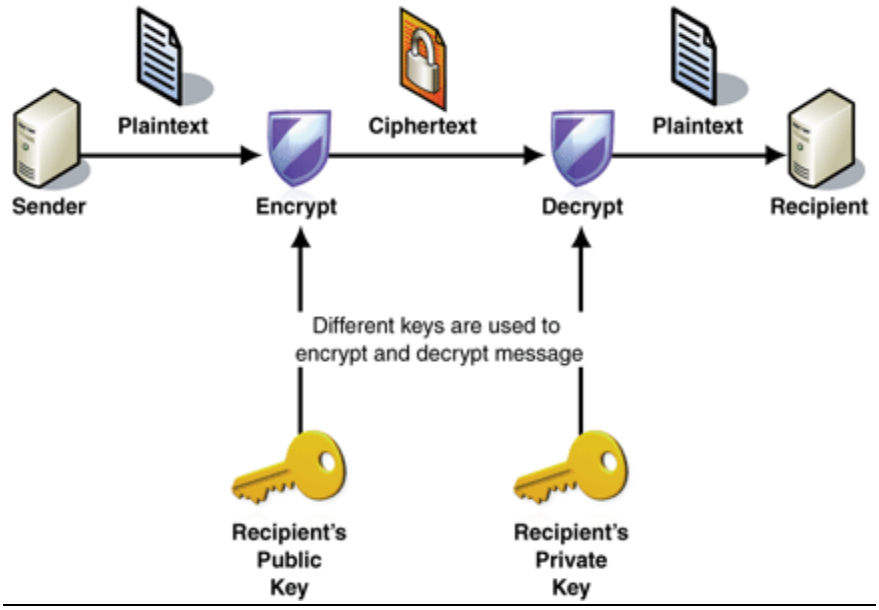
Ex: Symmetric Key Ciphers: (Only C not I or A Or NR)

DES, 3DES, BLOWFISH, IDEA, RC4,5,6, AES, SAFER, SERPENT

The Key Size is the factor to consider them

Fastest way to do the encryption :

Asymmetric Key (Public & Private Key) Cryptography:



A Key Pair:

Public Key is For Public
Private Key is kept private

Associated with each other Mathematically:

No Out of Band management required:

Complex & Slower

RSA
ECC
DH (THE SESSION KEYS, KEEPS ON CHANGING) or KEY AGREEMENT PROTOCOL (UR PUB MY PRI and goanna come up with same SYMMETRIC key)
Elgamal
Knapsack

Private Key encrypts data to ensure the Non-Repudiation….

I want all Confidentiality, Authentication & Non Repudiation
Symmetric Key is Encrypted using the receivers Public Key:
Something is encrypted with the Senders Private Key provides the Authenticity & As well as Non-Repudiation because the sender's public key can only decrypt it.

When Message is Encrypted using the Symmetric key & than on the TOP of that Asymmetric key the Symmetric key should be a session key, only valid for that session.

Mode of Operation:

Factoring
Discrete Logarithm

HASIHNG:

Message digests value appended in message or payload.
Non Cryptographic techniques can be modified by an adversary that's why we employ the MAC as we know that cryptography is resource intensive.

MAC(Message Authentication Code): Symmetric Key used in combination with hashing algorithm, results the MAC

1. MAC: Simply appended to message but MiM with knowledge (the little one) can utilize the same algorithm to generate the same MAC & will exchange on behalf of the sender with receiver.
2. HMAC (Weakest, provides DoA(Data Origin Authentication, System level Authentication) & Integrity): Receiver should have its own (THE SAME ONE) Symmetric key to decrypt an come-up with independent MAC value of HMAC appended packet & perform a comparison

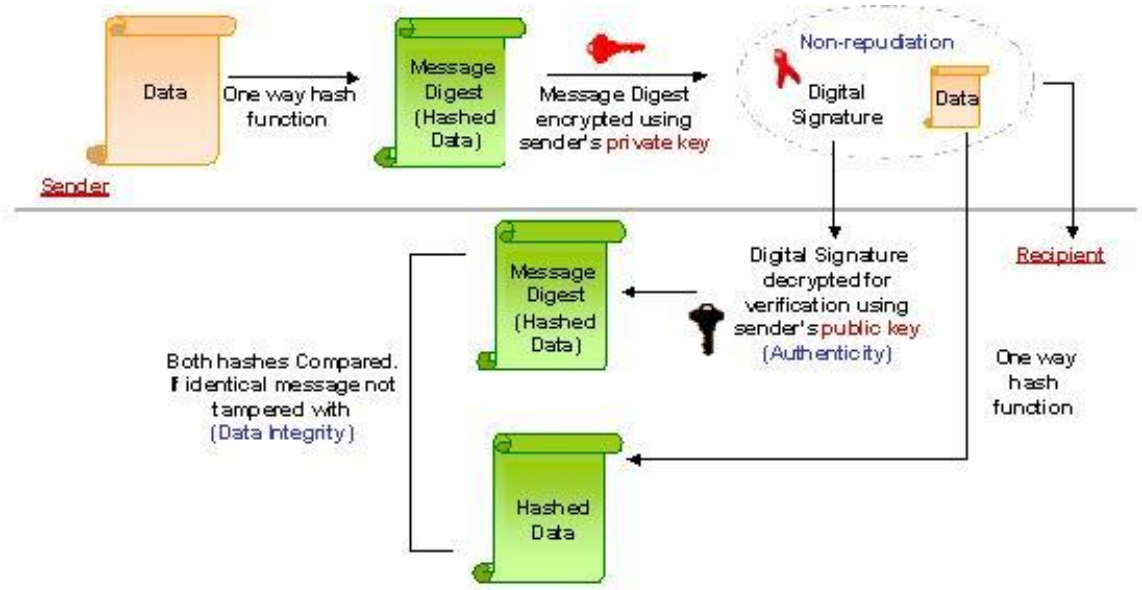
Digital Signatures: Authentication of an Individual & Non-Repudiation:

Steps:

After message is processed via an hashing algorithm the MD value is encrypted using the senders private key.

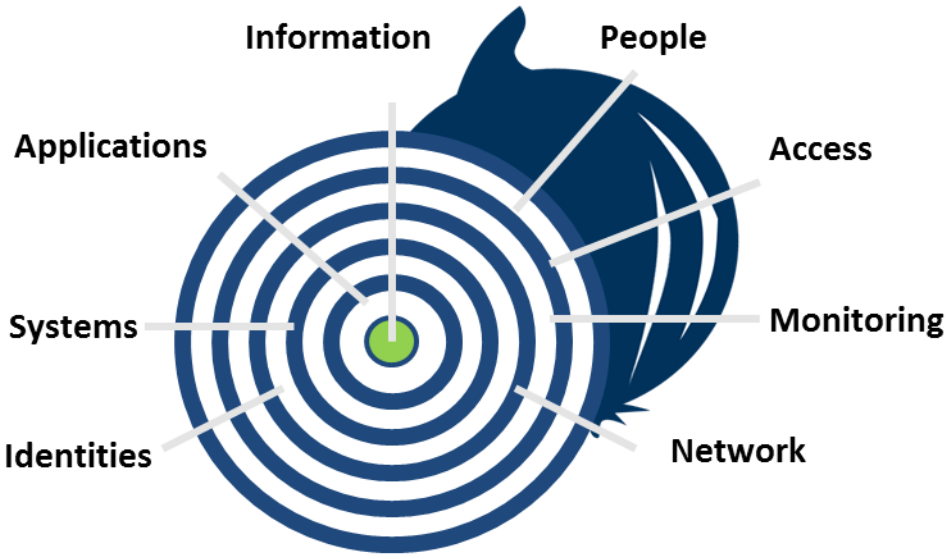
Recipient uses the Senders Public key and it ensures the Integrity, Authentication and Non-repudiation but no confidentiality

DSS:



INFOSECTRAIN

COMMUNICATION'S & NETWORK SECURITY



Defense-in-Depth Model

A Network is a collection of digital devices connected with each other, utilizing some transmission medium (Wired/Wireless) and allows the process running in them to communicate with each other utilizing intermediate network devices.

Networking is the way the devices communicate with each other following various standard's Ethernet, FDD, and Token Ring etc.

Message exchange between two or more digital devices in fact the processes running on them.

Avenues can be used by an attacker can use to enter.

PLEASE EXPECT MORE HERE

INFOSECTRAIN

Identity & Access Management (IAAA)

- A KEY security discipline to make Subject accountable for their actions & secure Objects from the C.I.A perspective.
- Management of User ID's, Authentication and Information Access across multiple systems.
- Your actions should always be C.I.A centric if not all, minimum one should be satisfied
- Everything goes as a project so please keep the basics of Project Management as A Project Manager.
- An Asset is not always an Information Technology based; anything what if destroyed will jeopardize the operations.
- Session (Active communication between two or more entities) is a very important factor.
- Access denied is access maintained? But Why that SO?
- Everyone (Subject & Object) accessing the C.I.A oriented resources should have IAAA well & predefined while following SoD, Job Rotation, and all the policies & good practices you fathom before.
- Information Assets access Business & Information Technology both should be accessible with least privilege & need to know basis.

- Access Control is the way that defines the limitations for authorized users & programs to access, modify and observe and take possession of data, as they are authorized for.

- An authorized subject needing access to authorized object is liable to present the followings:

    1. IDENTIFICATION: YOU ARE WHO YOU SAY YOU ARE E.g. Username

    2. AUTHENTICATION: VERIFICATION OF IDENTIFICATION E.g. Password but can be else or combination. (What You Know (PASSWORD {Weakest}), What You Have (Token, Smart Card {Modest}), What You Are (Physiological or Biometric {Strongest})

    3. AUTHORIZATION: THE LEVEL OF ACCESS (SUBJECT IS AUTHORIZED TO RECEIVE ONCE IDENTIFIED & AUTHENTICATED)

    4. ACCOUNTABILITY: ENSURE THAT THE SUBJECT ACTIONS ON OBJECT'S ARE TRACABLE, VERIFIABLE AND SECURE TO PROVE THE ACTIONS, SUBJECT PERFORMED ON OBJECT.

- The Operational areas of an Organization can be classified in to four broad categories are:

    1. Facility
    2. Support System
    3. Information System
    4. Personnel

- All Physical & Logical access to the various components constituting your information system should be curbed using various access controls as required.

- Access controls following the below mentioned attributes lead to a sound secure access management system.

    1. What Subject's should have access in terms of Physical and Logical entry?
    2. What Object's a Subject can Access?
    3. What Operations the Subject can Perform?
    4. How to make the Subject accountable for their actions?

- Access Control strategy designed using the above four attributes allows the organization to have a better look of its security posture as well as state.

- The assurance of Confidentiality & Integrity also assures the Availability at a certain level of the critical assets. E.g. the area (Physical or Logical) should be available to the Authorized Subjects requiring the access of Objects to perform their tasks towards the mission should not be accessible to unauthorized objects for the sake of Availability.

- Another side of the coin is to ensure only authorized subject should have access to the objects they are authorized for to reduce the attacks surface (intentional & Unintentional) of an asset.

- Again the 4 ways to ensure the IAAA 1). Information 2). System's 3).Device 4).Facilities for the sake of Physical & Logical access of the assets.

- Identification Management lead's to the management of Identification + Authentication and authorization with accountability.

- Identification without authentication is not enough and the vice versa is as well, an additional layer of protection.

LOGICAL ACCESS TO ASSETS

- Here ACCESS = Identification + Authentication + Authorization + Accountability

- Identification is the first step for any access control mechanism intending to support mission critical & sensitive information in a system

- Authorization always is done after the Identification, validates the Identification using various mechanisms by performing comparison or may be a two, three or multiple stage process.

- Authorization is the third layer in the IAAA management that defines the capability of a subject in terms of access to the objects by considering the subjects role and the enterprise goal.

- Structure and Level of the Authorization again are subject to the asset criticality, sensitivity & other controls (if there) are in place in conjunction with sensitivity & clearance level the Subject need to possess before access.

- Accountability reflects the action result of the Subject in a manner that will not pose any liability on enterprise in case of any violation of Legal or Civil law.

- Physical & Logical controls integration is common to defeat the malicious actions and eventually mitigating the adverse impact posed by vulnerability if it exploits a threat and reducing the threat landscape itself.

- Electronic controls can be updated on the fly and administered from a central location.
- During the design & development of such controls one should must deeply analyze the scope (Authorized & Unauthorized Users) and a tiered fashion of implementation. E.g. DiD
- Controls not only intended to prevent & deter the access but also log the access according to the policies and compliance you are under the guidance of.
- Various controls can serve as a different piece of PUZZLE to see the holistic picture of a violation.
- Logical Access Controls (Logic based) as the name suggests always are implemented via system software or the application software or program.
- Logical Access Controls utilize various Access Modes to get their job done to permit & deny access subjects to object.
- Read Only: **VI COP RIN**
- Read & Write: Along with the Read Only rights user is allowed to Add, Modify & Delete but more refined approach of such controls allow the subject to use one field of information read only but the other one with write as well.
- Execute: In terms of application or other programs the subject requires Execution permissions so they are allowed for that but the Read & Write permission goes for Software Developer as an example.
- Administration of logical security controls is an arduous task as it requires Implementation, Monitoring, Modifying, Testing & Terminating the user access from your system (All access not the electronic only) becomes a daunting task if not done in a planned manner.
- The decisions related to grant & provoke the access are taken by data owners and most of the times under the supervision of management.
- Granting access related decisions should follow the organizational policy, role of the subject, job description, need to know, sensitivity of information & many other factors.
- Procedures & Forms for approval are should be in place.
- Access control Administration type:

1. Centralized: As the name suggests but establish procedures should be there. In case of access needs changed, access can be modified after the approval of authority. Centralization

is always suggested method from management perspective of anything monitoring and revoking access is always easy.

2. De-Centralized: The owners or creators are responsible to discern who & what should be given access to, because they better know their data they are responsible for and the can judge better in what relation & regard. But the major drawback of such approach is different data owners advertently can assign access that is not in the benefit of the enterprise and it makes monitoring as well. Especially when the user is transferred or leaves the organization.

3. Hybrid: It utilizes the both approaches to gain the advantage of both mentioned above. The broadest and most basics level is given by a central authority while the specific permissions are given by the Data owner & the creator on file level itself. In case of change of user role will require the owners & creators to ensure it.

- PHYSICAL ACCESS CONTORLS

PHYSICAL SECURITY IS FIRST & MUST

- Physical Access: Access to such areas can be curtailed using the key or tokens but these can always be borrowed or lent to ensure one should have what you know (password), in office hours what you have and after office hours what you know as well. This access can be granular by dividing the office area in to cells or zones.

- Important point to consider here is to ensure that the TAILGATE, PIGYBACKING and ANTI PASSBACK solutions are in place, because your system says employee is with-in the facility but he/she is missing, gone out without utilizing his/her credentials.

- Dual Custody & Dual Key Entry, always good to adopt them as the part of your Physical Security Control Architecture that makes mandatory for two entities to be present while

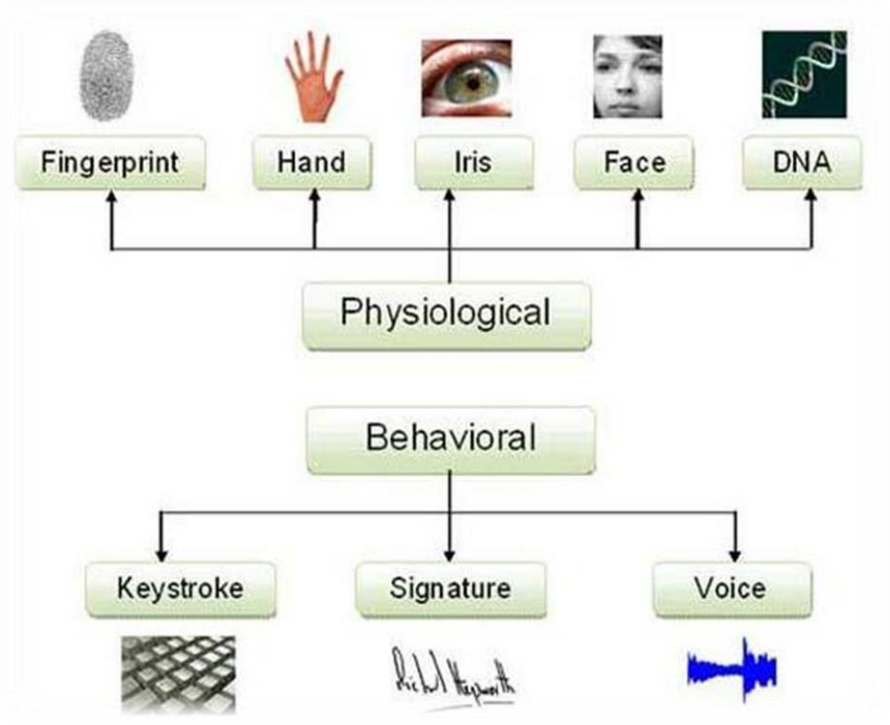
accessing sensitive & critical information asset.

- CCTV, Alarm Arming & disarming, air condition units are as the kind of controls, used for that purpose.

- Tokens aiding the authentication process comes in two flavors:
  1: Soft Token (E.g. Google Authenticator App)
  2: Hard Token (E.g. RSA hard tokens)
  Tokens provide a unique value to system & perform the role of What You Have authentication.
  It generates a secret string used on one time basis & sync's with system.

WHAT YOU ARE?

The physiology or Biometric based authentications are very common now a day.



- User acceptance for such authentication is a challenge.

- Enrolled attribute is used to perform the Authentication.

- Biometric Fingerprint Scanner can be a serious hurdle, can transmit skin diseases.

- Two types: 1) Physiological 2)Behavioral

- THREE STEP PROCESS:

  1) Observation or Collection of Data

  2) Conversion of Collected data in Digital Format (Called TEMPLATE)

  3) Comparison of stored TEMPLATE in database with the received one.

- Adjustable Threshold mechanism is used. Degree of similarity needed to match or fail the verification. The acceptance or rejection of biometric data depends on the below or above of the threshold value.

  - Spoof Attacks are detected using the Aliveness Detection feature.

- Threshold value allows one to make biometric device adjustable, more or less strict.

  Three abstractions are to embrace for access controls are:

  1. Access Control Policy
  2. Access Control Model
  3. Access Control Mechanism

- PACS (PHYSICAL ACCESS CONTROL SYSTEMS) by Department of HOMELAND Security

It's a Security Technology Integration Suite used to control & manage the Physical Access Devices, Intrusion Detection and CCTV etc.

PACS enables an authorized security personnel to simultaneously manage, monitor multiple entry points form a single location.

It also produces event & incidents reports in a documented manner including when & where factors.

PACS major domain is NAC & divided in to 4 areas, is the following:

1. Identification: PIV & PII (nice to remember)
2. Visitors Management
3. Parking Permit Management

4. Alarm Monitoring & Intrusion detection

Either you apply PACS solution or not for your organization but the following questions as a dynamic security professional should hit your brain:

1. The scope, need (in-depth), and solution exactly you are asked for.
2. What will be the security architecture of that solution.
3. Policies to integrate that solution & how that solution serves to management goals.
4. Resources & Metrics to manage & maintain that solution.
5. Training, Awareness & Education of end users to make the solution pragmatic & easily adoptable.

In Access Control the model it will be applied on is very important for a security professional to consider. No doubt that a Centralized model is the mostly preferred one and has its own pros & cons but it may not necessary in every case.

A distributed or de-centralized model may suit best to your enterprise, again there is always a trade-off but don't miss to have a proper look of resources (in all terms) you have in hand.

The Bottom Line is Growth; Complexity & Need to fulfill them are always directly proportional. So better to keep scalability in mind.

- IDENTIFICATION & AUTHENTICATION OF PEOPLE & DEVICES:

There is a planned strategy for any planning & projected view behind every project. Access controls is not an exception.

- Any managed process (series of tasks) has certain components and those are needed to be managed in a structured manner called LIFE CYCLE APPROACH, while the components are communicating with each other with other parts of the main system.

- IAA Identification Authentication Authorization
- ACS Access Control Services
- IM Identity Management
- ACT Access Control Technology

IDENTIFICATION, AUTHENTICATION & AUTHORIZATION

- Access Controls are applied to an Identity (User or Computer) is the starting point
- Every Identity must have a unique Identification
- Accountability of an Identities action is determined by his/her unique Identification
- Secured Audit Trail is the key in making Identity Accountable

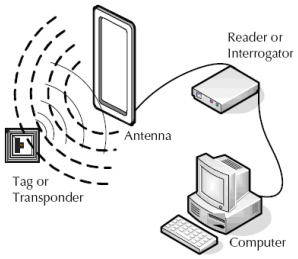
- An Audit Train is a chain of Actions performed by an authorized Identity with C.I.A preserved.
- Identity never comes alone as the TOM can never be there without JERRY, it always comes with Authentication.
- Authentication credentials are assumed to be in the possession of the Identity but can be shared by (So we have multi factor Authentication available)
- Trust is defined by Identification process between authorized user and the Information System.
- Authorization is done on the basis of Identification, that starts the life of an Identity with in an Information System
- Authorization is the process of allocating the access of resources a subject is seeking for as per granted level according to his/her role and requirements
- Authorization must be well defined & monitored to provide the assurance of C.I.A of the information assets.
- Identification is all about the uniqueness
- Authentication is all about the validity of the uniqueness
- Authorization is all about the control to protect the valuables

IDENTIFICATION METHODS:

The most basic one is the username but there are more common as account number, PIN number, one time session identifier or digital certificate in case of a computer system needs authorized access to another one. So it applies to users & digital systems as well.

- **Identification Badges:** Not a fool proof solution, Physically and Logically Identify & Authorize a unique entity.
- Access badges: Stores the information about access (multiple options) and provide authentication & authorization both.
- Most of the time Integrated with Identity badges due to their sharing nature by HUMAN's
- User ID is also one of the methods to uniquely identify (Just Identify) the user within the system.
- Lacking support of any Authentication mechanism User-ID can't (not feasible) have rights to access system.
- **Account Number/PIN** (Personal Identification Number) Associated with financial aspects of users as an authorized entity to access information system.
- **MAC (Media Access Control) (Physical One)** can't be used to identify a unique system over the network, can be changed at software level or can be easily spoofed.
- **IP Address (Logical One)** Must be unique for every computing device in an enterprise but again implemented at software level & can be spoofed can't be used alone as identification mechanism

- **RFID tag** is another method to perform Identification. The major components are 1). An integrated circuit to modulate & demodulate radio signal 2). An antenna to end & receive the radio signal
- Bar Code readers, magnetic readers are common applications of RFID technology with no contact and LINE of SIGHT in place.
- Also called Enhanced Electronic Barcode
- Also known as Chip less RF ID tags or RF Fibers
- AN RFID System entails the following components
  1. An RFID tag or transponder
  2. An RFID reader
  3. A back end database to store the unique information



- RFID tags are 'DUMB' because they can only listen & respond, can't make decisions or verify the authenticity of the signal they are dealing with, it poses a huge risk to compromise by unauthorized access and subject to vulnerabilities like sniffing, eavesdropping, traffic analysis and DoS attacks.
- RFID use at International level: Visa Waver Program (VWP) by USA.
- RFID is also subject to if proper controls are not in place:
  1. Virus 2. Backend SQL database injection 3. RFID reader integrity 4. Personnel Privacy

Email ID: This identification procedure is such that an enterprise can't rely open. Anybody else email ID can be used as an Identification purpose. When designed in a manner that carries their usage as Identification can be used but there are many issues to deal with. Albeit they are unique at root level domain.

USER IDENTIFICATION GUIDELINES

1. UNIQE
2. NON DESCRIPTIVE
3. SECURE ISSUANCE

UNIQUE FACTOR:

This is the first and foremost requirement that user's identification should be unique for various access controls user is the part of in order to gain authorized access with-in the enterprise. Same id for multiple access control can lead to a fundamental risk by user to present his/her wrong password sharing for wrong identification.

NON-DESCRIPTIVE:

Identity should not disclose the user role, position in turn it becomes a boon for ill will person as part of his/her reconnaissance process and can target the user by the identity. It should be pondered that the

system level accounts revealing their privilege strength in their identification name should be renamed or should utilize some way to obfuscate the attacker and SID, RID used by the operating system (Windows) to uniquely identify the user and their privilege also needs to be take care off.

- Use randomize method to create user ID's
- Renaming the user account is really a good practice
- Apply defense in depth wherever possible

SECURE & WELL DOCUMENTED ISSUEANCE:

Well it's the first step of access control to enter so the secure issuance and the proper documentation is the key or no use to follow the above mentioned steps. The user management should be notified about the issuance of their Identification and any system owners the user needs to have access for, as well. The delivery of ID to the user must be done using a secure channel and should be documented either sealed envelope or digital signature protected id, the information should be auditing enabled.

IDENTITY MANAGEMENT IMPLEMENTATION: (Policies, Standards, Processes)

Implementation is the process of, putting all well designed and deeply analyzed individual components together & dovetail them.

Access controls revolve around the subjects and objects. To fasten the policies, procedures & privileges that will all together bind the user across the infrastructure there are couple of plans available.

PASSWORD MANAGEMENT:

The most famous but the weakest form of authentication used from early days to now, it's a PASSWORD.

A PASSWORD validates identities validity by using the mechanism called 'AUHTENTICATION'. As authentication is the process of validating an identity as it says to be with-in a system (can be any system, not just a computer system but most of the times).

Password is a string of combination of characters may be numeric, special one, alphabets only or the combination of all.

It's been observed that when alphanumeric characters are used it's hard for a person with ill will to get it revealed because the work factor is really high.

CHANGE INTERVAL: In modern system the change interval of a password is around 30 – 90 days. The reason behind regular change is that it lessens the effect of the compromise. The lesser one is always good & recommended.

COMPLEXCITY: The more complex a password the harder it's difficult the guess or crack due to the more processing is required but more hard for the user to remember, especially if the user is maintaining couple of them and can become the cause of frustration as well.

LOCKOUT PERIOD: To protect & detection against malicious attempt a LOCKOUT period is set so all attempts will be logged as well as user will not be able to change his/her password without the intervention of an authority as security administrator network administrator.
PASSWORD HISTORY: Same password utilized multiple times is also a sign or weak password management process. This threshold value mitigates the chances of compromising by allowing the end user to come-up with a new password as they change it.
Well it's really important to consider all these factors for good password management across the enterprise and a variety of password manager's integrated with multifactor authentication techniques can be utilized to achieve this goal.
Never underestimate the SOCIAL engineering & habit of users to store password at openly hidden places using sticky notes etc.

ACCOUNT MANAGEMENT:

It deals with creation, modification & decommissioning of accounts. Centralization of administration has always been a key point of doing management Purely specking there are two core models the one is centralized and other one is decentralized.

PROFILE MANAGEMENT:

INCIDENT RESPONSE: Acting against abnormal situation to either restore the normal situation or lessen the impact of the abnormal one is called response.

1. Detection: The first step to ensure that an incident has taken place.
2. Cause of Action: What was the reason behind that can be eliminated or mitigated.
3. Mitigation: Taking actions to lessen the impact.
4. Resolution: Correction of the problems.
5. Documentation: Every step of actions to overcome the situation or mitigation should be documented for future reference.

As attacks are decreasing in their numbers towards the Information System they are becoming sensitive in their nature while utilizing various attack avenues (vectors). There is a prioritizing mechanism the works here as well
There are couples of keywords really mandatory before you immerse yourself in incident management.
Life Cycle
Detection
Root cause analysis
Triage
Investigation

DOMIAN 7

SECURITY OPERATIONS

Understand & Support Investigation's:

In an enterprise the policy governs the actions & ensures the reactions should be used as a counter in case of any compromise in respect to C.I.A.

An investigation is the process of excavating for the reasons (Evidence the Digital One) & series them in a fashion in case of violation. That could divulge the actions performed to take the desired decisions against an accountable entity (An enterprise) or subject (A USER) as per the prescribed law or regulations.

A DIGITAL INVESTIGATION entails the usage of various FIR toolkit (trusted binary) for the purpose of reconstruction of actions performed by and on a digital device while logging the documentation of steps in a verifiable manner.

An Incident causes an investigation. As dealing with digital devices to carry out the investigation requires that one must identify that an incident happened. Digital evidence in form of digital data collection & preservation requires sophisticated techniques to be applied followed by the good practice oriented policies with procedures in place.

Any thing without in support of good documentation is as having a best model of limousine with a fuel tank of five gallons only.

The definition of an Incident in terms of Information security is: Any activity causing the loss of C.I.A of the Information within the system by utilizing physical or logical means is considered as an incident.

The following activities trigger an Investigation: (Performed using the Digital devices & medium)

- Operational: An activity carried out to improve the operational performance related issues named as “ROOT CAUSE ANALYSIS” E.g. a server starts consuming more resources & goes beyond a predefined threshold as the baseline suggests on the regular basis.

- Criminal: An act that presents the felonious (criminal) intention and can become a serious threat & finally poses the risk to national security. E.g. Cyber terrorism.

- Civil: An activity that violates the established ‘CIVIL’ laws not in the societal favor & poses a threat and eventually RISK can destroy communal harmony. E.g. Pornography, Religion specific messages that provokes negatively.

- Regulatory: An activity that violates the established guidelines to comply with. E.g. an employee not complying with the I.T. Security policy of his/her enterprise, an enterprise involved in credit cards related business and not complying with PCI-DSS.

- (Electronic) E-Discovery: Any act that deals with fraud especially in the financial domain. E.g. An enterprise (Public Interest Company) not complying with SoX.

👉 ***GOOD TO KEEP LOCAL JURIDICTION OF PRIVACY IN MIND***

A violation is as it says E.g. not complying with any established law or policy that will make as adverse effect on the society or culture of the operating environment.

The steps involved to mitigate an incident impact or planning for Incident response:

1. Incident response plan should be as per incident response policies & procedures of the enterprise.
2. Scope & objectives as per the policy & procedures.
3. Prepare a CIRT team:
4. Prioritize the Incident as per its impact to the enterprise operations
5. Effective Communication: Who to contact when and in what manner should be documented & provided to all directly (must) & indirectly related to incident response.

Security in Software Development Life Cycle DOMAIN 8

- None of the software 100% perfect in this world
- Most of the attacks take advantage of existing software vulnerability as their entry point
- System & Application both software's are subject to vulnerability & threat
- Security is the point of consideration from development, maintenance to operation
- Web access made the network access more easy
- The 2 or 3 tier architecture can be exploited, lacking proper attention

- Exposure to external system with exchange of data invites security risk of malwares
- Coding is all about logic & syntax seeks for productivity, speed and portability
- The framework is called SDLC
- Security has been a big challenge for developers
- Software is used as a major platform for training & awareness
- Using the client software applications, users interact with network
- Operating System vulnerabilities are more dangerous

Outcome intended:
Understand & Apply security in Software Development Life Cycle
Security controls applicability during the development phases