CISSP - Work note

CISSP, What is it ?

CISSP is a certification created by (ISC)² in 1994. The goal is to validate the subjects of all the domains covered in the Common Body of Knowledge (sometime named CBK). The CISSP cover the following domains :

1. Security and Risk Management
2. Asset Security
3. Security Architecture and Engineering
4. Communication and Network Security
5. Identity and Access Management (IAM)
6. Security Assessment and Testing
7. Security Operations
8. Software Development Security

Requirement :

- Work since 5 years in two or more of the of the domains above.
- Accept the CISSP Code of Ethics. Globally, follow these :
  - 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 principles.
  - Advance and protect the profession.
- You may have to answer questions about your background, criminal record, etc.
- Pass the exam (more on this below).
- Once the exam passed, a CISSP holder must endorse your qualification.

In 2018, there is almost 128.000 CISSP worldwide. Member Counts

The Exam

It's more theory and concept, but sometime, you have to know some technical aspect, especially in cryptography and network. It's vendor neutral but sometime vendor or product are mentionned.
Exam is passed through a software, CISSP-CAT (Computerized Adaptive Testing). The number of questions is between 100 and 150 and must be achieved in 3 hours max. Quesions have to be answered as it's not possible to go back to a previously encountered question. The CAT will pick questions in a large base of questions depending of the answers. If the person is bad in a domain, the CAT will send questions about this domain. The questions are made of 4 choices with a single right answer, sometime multiple answer are needed but it's specified.
It's possible to try the exam 3 times per year will at least 30 days between each try. The cost of the exam in 2018 is around 650€, or 699$ or 560£. Multiple langage are available, but as most of the ressource and vocabulary are in english, it's a good

choice to pass it in english.
Bring ID card and voucher.

Advice

- Read the question, then the answers, then reread the question.
- Proceed by elimination. Eliminate the obvious wrong.
- Watch the double negative.
- Be sure to understand the question.

1 - Security and Risk Management

Operation Security Triplets

- **Threat** - an event that could cause harm by violating the security (i.e. Operator abuse of privileges)
- **Vulnerability** - weakness in a system that enables security to be violated (i.e. Weak Segregation of duties)
- **Asset** - anything that is a computer resource (i.e. software data)

Due Care is using reasonable care to protect the interest of an organization. Due care is a legal liability concept that define that define the minimum level of information protection that a business must achieve.
Due Diligence is practicing the activities that maintain the due care effort. Practicing due diligence is a defense againt negligence.

Risk Management

- Risk Avoidance : Change the initial plan to avoid the risk. To avoid the risk of having a server hacked if exposed to internet, do not expose it to internet.
- Risk Mitigation : Install safeguard to limit the risk or thread. To limit the risk of having a server hacked when exposed to internet, install a firewall and an antivirus. The risk is still present, but less than before the installation of the safeguard.
- Risk Assignment : or Risk Transfer, is placing the risk onto another entity or organization. Getting an assurance or outsourcing are a transfer of risk.
- Risk Acceptance : or Risk Tolerance happen when it's a financial non-sens to install safeguard. For example, if the cost of protecting a server is greater than the cost of having this server hacked. Risk Acceptance must be written somewhere.
- Risk Deterrence : involves understanding something about the enemy and letting them know the harm that can come their way if they cause harm to you. Something as simple as a banner indicating any trespassing will be prosecuted is Risk Deterrence.
- Risk Rejection : is ignoring the risk or denying the existence of the risk.
- Residual Risk : is the risk still present after the installation of safeguards or countermeasures.

- Total Risk : is the calcul of the loss for the company without countermease per asset. Calculated by the following formula : Threat x Vulnerability x Asset Value = Total Risk .

  To calculate a risk, a basic formula is :
  Risk = **Threats** (number) x **vulnerabilities** (number) x **Impact** (cost in dollar if the asset is lost) .

Different Planning

- Strategic : Defines the organization's security purpose. Long term 5 years.
- Tactical : Midterm plan developed to provide more details on how to accomplish goals.
- Operational : Short term, highly detailed plan based on the strategic and tactical plan.

Threat Modeling

Threat modeling is the process of identifying, understanding, and categorizing potential threats, including threats from attack sources.

- **DREAD** is part of a system for risk-assessing computer security threats previously used at Microsoft and although currently used by OpenStack and other corporations. It was abandoned by its creators. It provides a mnemonic for risk rating security threats using five categories. A score of 0 to 10 is given to each categories, then the score are additioned and divised by 5 to calculate the final risk score.
  The categories are:
  - **D**amage – how bad would an attack be ?
    - **0** = no damage
    - **10** = complete destruction
  - **R**eproducibility – how easy is it to reproduce the attack ?
    - **0** = impossible
    - **10** = easy and without authentification
  - **E**xploitability – how much work is it to launch the attack ?
    - **0** = advanced knowledge and tools
    - **10** = little knowledge, a web browser
  - **A**ffected users – how many people will be impacted ?
    - **0** = none
    - **10** = all
  - **D**iscoverability – how easy is it to discover the threat ?
    - **0** = nearly impossible, source code or administrator access required
    - **10** = visible easily, from a web browser
- **PASTA** is a risk-centric threat-modeling framework developed in 2012. It contains seven stages, each with multiple activities :
  - **Define Objectives (DO)**, identify Business Objectives, identify Business Compliance Requirement (PCI DSS, HIPAA, etc)

- **Define Technical Scope (DTS)**
- **Application Decomposition and Analysis (ADA)**
- **Threat Analysis (TA)**
- **Vulnerability & Weakness Analysis (WVA)**
- **Attack Modeling & Simulation (AMS)**
- **Risk & Impact Analysis (RIA)**

- **STRIDE** is an acronym for :
  - **S**poofing
  - **T**ampering : modifying data, in transit or stored
  - **R**epudiation
  - **I**nformation disclosure
  - **D**enial of Service
  - **E**levation of privilege
- **VAST** is a threat modeling concept based on Agile project management and programming principles.
- **Trike** is using threat models as a risk-management tool. Within this framework, threat models are used to satisfy the security auditing process. Threat models are based on a "requirements model." The requirements model establishes the stakeholder-defined "acceptable" level of risk assigned to each asset class. Analysis of the requirements model yields a threat model from which threats are enumerated and assigned risk values. The completed threat model is used to construct a risk model based on asset, roles, actions, and calculated risk exposure.

Risk Assessment

- **Quantitative Analysis** aim to calculate the loss in dollar per year of an asset. It then help to calculate how much is reasonable to spend to protect an asset. Some math are involved :
  - **AV** is the cost of an asset in dollar.
  - **EF** is the percentage of lost the realisation of a threat can have on an asset. Noted in percentage or in a decimal. For example 80% or 0.8 .
  - **SLE** is the loss in dollar if a threat is realized. For example, for a 100.000$ warehouse behing hit by a flood estimated to have an EF of 80%, the loss will be 80.000$. It's calculated by the following formula : AV * EF = SLE .
  - **ARO** is an estimate of how often a threat would be successful in exploiting a vulnerability. For example 0.1 for something that have 10% to happen each year.
  - **ALE** is the estimation of loss per asset per year. The formula is ARO * SLE = ALE . For example, our warehouse that have a SLE of 80.000$, with an ARO of 0.1 will give : 80.000 * 0.1 = 8000.
  - **Likelihood Assessment** is the process where the ARO is measured, how many times a risk might materialize in a typical year. It is a measure of risk likelihood. Many agency provide data relative to the likelihood of a threat, for exemple, the NIFC provides daily updates on wildfires occurring in the United States.

- **Controls gap** is the risk reduced by implementing the safeguard. If there is a risk of **10** without the safeguards, and a risk of **3** with the safeguards, the controls gap is **7**.

- **Qualitative assessment** is scenario driven and does not attempt to assign dollar values to components of the risk analysis. Purely quantitative risk assessment is hard to achieve because some items are difficult to tie to fixed dollar amounts. Absolute qualitative risk analysis is possible because it ranks the seriousness of threats and sensitivity of assets into grades or classes, such as low, medium, and high.
  - **Low** : Minor inconvenience that could be tolerated for a short period of time.
  - **Medium** : Could result in damage to the organization or cost a moderate amount of money to repair.
  - **High** : Would result in loss of goodwill between the company and clients or employees. Could result in a legal action or fine, or cause the company to lose revenue or earnings.

  This is a list of qualitative factor that are often forgotten but must be taken in account when assessing the cost of a disaster.

  - Loss of goodwill among client base
  - Loss of employees after prolonged downtime
  - Social/Ethical responsibilities to the community
  - Negative publicity
- **Delphi Method** is a structured communication technique or method, originally developed as a systematic, interactive forecasting method which relies on a panel of experts. The experts answer questionnaires in two or more rounds. After each round, a facilitator or change agent provides an anonymised summary of the experts' forecasts from the previous round as well as the reasons they provided for their judgments. Delphi is a qualitative risk analysis method.
- OCTAVE is a Risk Assessment suite of tools, methods and techniques that provides two alternative models to the original. That one was developed for organizations with at least 300 workers.
  OCTAVE-S is aimed at helping companies that don't have much in the way of security and risk-management resources. OCTAVE-Allegro was created with a more streamlined approach.
- NIST 800-30 is a systematic methodology used by senior management to reduce mission risk.
  Risk mitigation can be achieved through any of the following risk mitigation options:
  - **Risk Assumption.** To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level
  - **Risk Avoidance.** To avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified)
  - **Risk Limitation.** To limit the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability (e.g., use of supporting, preventive, detective controls)

- **Risk Planning.** To manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls
- **Research and Acknowledgement.** To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability
- **Risk Transference.** To transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

MTD is a measurement to indicate how long the company can be without a specific resource. General MTD estimates are:

- Critical = minutes to hours
- Urgent = 24 hours
- Important = 72 hours
- Normal = 7 days
- Non-essential = 30 days

Defense in Depth : The idea behind the defense in depth approach is to defend a system against any particular attack using several independent methods. It is a layering tactic, conceived by the National Security Agency (NSA) as a comprehensive approach to information and electronic security. For example, using a cage, a firewall, an antivirus and IDS for a server is Defense in Depth. Even using different type of control (physical, logical and administrative) is an exemple of defense in depth.

Standard, Baseline, Policies, Procedures

- **Standards** define the technical aspect of a security program. This include hardware and software. As Standards are mandatory, they must be followed by users. For example, if a standard say a company computer must run windows 8 and use outlook for the mail, the users does not have the right to install linux or another version of windows.
- **Policies** are high-level overview of the company's security program. A policy must contain :
  - *Purpose* of the policy.
  - *Scope* and what is covered by the policy.
  - *Responsability* of the entities that must comply with the policy
  - *Compliance* of the policy and how to mesure it. The consequence of the non-respect of the policy should be clear.

  Also, policies should be :

  - *Short* policies are more understandable for employees.
  - *Words* used should be directive, like *must, will*.
- **Procedure** explain in detail how to achieve a task.
- **Baseline** provide a minimum of security that employes and system must meet.
- **Guidelines** are discretionary and provide advice to users.

Access Control

- **Administrative** Access Control.
  - **Procedures and Policy**, that management team write. They must ensure they are enforced and all employees in the company adhere to them. The policy state what are the risk accepted, what actions are acceptable. It should be written by someone who understand the laws of the country in which the company is involved.
  - **Supervisory Structure** make the supervisor accountable for the actions of its team. The supervisors must check the works done by its team should be done accordingly to the company's policy and guideline. It's also true for the supervisor's supervisor.
  - **Personnel controls** are controls put in place to check doesn't break laws or try to steal from the company. For example, the purchase team must make every purchase above 50K validated by the management.
    - **Job Rotation**, Rotation of Duty allow to detect frauds or tasks not done properly.
    - **Separation of duties** should be enforced so that no one individual can carry out a critical task alone that could prove to be detrimental to the company.
    - **Change of Status** controls indicate what security actions should be taken when an employee is hired, terminated, suspended, moved into another department, or promoted.
  - **Testing**
    - This control states that all security controls, mechanisms, and procedures are tested on a periodic basis to ensure that they properly support the security policy, goals, and objectives set for them.
    - The testing can be a drill to test reactions to a physical attack or disruption of the network, a penetration test of the firewalls and perimeter network to uncover vulnerabilities, a query to employees to gauge their knowledge, or a review of the procedures and standards to make sure they still align with business or technology changes that have been implemented.
  - **Security-Awareness** Training control helps users/employees understand how to properly access resources, why access controls are in place and the ramification for not using the access controls properly.
  - **Examples of Administrative Access Control** :
    - Security policy
    - Monitoring and supervising
    - Separation of duties
    - Job rotation
    - Information classification
    - Personnel procedures
    - Investigations
    - Testing
    - Security-awareness and training

- **Technical** Access Control.
  Sometime called Logical Control, are the software, application, OS feature, network appliance, used limit subjects to access the objects.
  - **Network access** firewalls, switches and routers can limit access to the resources.
  - **Network Architecture** This control defines the logical and physical layout of the network, and also the access control mechanisms between different network segments.
  - **System Access** is based on the subject's (often user) rights and permissions, clearance level of users and data classification. It can be as simple as a password, or something more secure like a 2 way authentication with login, password and biometric (retina, finger print, palm, etc). Auth can also be done through a PKI (keys exchange), or TACACS, RADIUS, Kerberos, etc.
  - **Encryption** protect data at rest (stored on a computer, a CD, a tape, etc) or data in transit (while going through the network).
  - **Auditing** These controls track activity within a n/w, on a n/w device or on a specific computer .They help to point out weakness of other technical controls and make the necessary changes.
  - **Examples of Technical Access Controls**
    - ACLs
    - Routers
    - Encryption
    - Audit logs
    - IDS
    - Antivirus software
    - Firewalls
    - Smart cards
    - Alarms and alerts

There is different model of alarm system :

- **Local alarm system** An alarm sounds locally and can be heard up to 400 feet away.
- **Central station system** The alarm is silent locally, but offsite monitoring agents are notified so they can respond to the security breach. Most residential security systems are of this type. Most central station systems arewell-knownor national security companies, such as Brinks and ADT.
- **Proprietary system** This is the same thing as a central station system; however, the host organization has its own onsite security staff waiting to respond to security breaches.
- **Auxiliary station** When the security perimeter is breached, emergency services are notified to respond to the incident and arrive at the location. This could include fire, police, and medical services.

- **Physical** Access Control.
  Are the access control that will physically protect the asset, allowing only authorized personnel to approach it. It can also physically remove or control functionnalities.
  - **Perimeter Security** implementation is a set of multiple physical access control that allow the company to prevent intrusion in its building, factory, datacenter, etc. Perimeter security can be enforced through fences, walls, lighting, security guards, badge, CCTV, motion detector, dogs, etc.
  - **Computer Controls** can be a lock on the cover of the computer to protect the internal parts of the compurer, or the removal of the CD-ROM, USB ports, etc, to prevent the copying of informations. A faraday cage prevent the leaking of electro-magnetic waves.
  - **Work Area Separation** is the fact to separate some employee from others employees. Services working on very sensitive data should not be in the same place as others employee.
  - **Network Segregation** is the physical separation of certain networks. The DMZ should not be on the same switches than the users. The network racks should be accessile only by authorized users.
  - **Data Backups** is a physical control to ensure that information can still be accessed after an emergency or a disruption of the network or a system.
  - **Cabling** should be done in a way that nobody can be hurt, electrocuted, etc. It should also prevent sniffing. There is different type of cable, shielded or not, to avoid electromagnetic crosstalk between cables. Some cables are also more or less protected to mecanical constraint.
  - **Control Zone** is a specific area that surrounds and protects network devices that emit electrical signals. These electrical signals can travel a certain distance and can be contained by a specially made material, which is used to construct the control zone.
  - **Examples of Physical Control**
    - Fences
    - Locks
    - Electronic Lock
    - Badge system
    - Security guard
    - Biometric system
    - Mantrap doors
    - Lighting
    - Motion detectors
    - Closed-circuit TVs
    - Alarms
    - Backups
    - Guards
    - Dogs
    - Laptop locks
    - Mantraps
    - Safe storage area of backups

Each of the access control categorie can be from one of the following type :

- **Preventative** Avoid undesirable events from occurring
  - fences
  - locks
  - biometrics
  - mantraps
  - lighting
  - alarm systems
  - separation of duties
  - job rotation
  - data classification
  - penetration testing
  - access control methods
  - encryption
  - auditing
  - CCTV
  - smart cards
  - security policies
  - security awareness training
  - antivirus software
- **Detective** Identify undesirable events that have occurred
  - Reviewing logs
  - security guards
  - guard dogs
  - motion detectors
  - reviewing CCTV record
  - job rotation
  - mandatory vacations
  - audit trails
  - IDS
  - violation reports
  - honey pots
  - supervision and reviews of usersv
  - incident investigations
  - IPS
- **Corrective** Correct undesirable events that have occurred
  - antivirus solutions
  - business continuity planning
  - security policies
- **Deterrent** Discourage security violations
  - locks
  - fences

- security badges
- security guards
- mantraps
- security cameras
- trespass or intrusion alarms
- separation of duties
- work task procedures
- awareness training
- encryption
- auditing
- firewalls

- **Recovery** Restore resources and capabilities
  - backups and restores
  - fault tolerant drive systems
  - server clustering
  - antivirus software
  - database shadowing
- **Directive** deployed to direct, confine, or control the actions of subject to force or encourage compliance with security policies.
  - Awareness Training
  - Posted Notifications
  - Exit Signs
  - NDA
- **Compensative** Provide alternatives to other controls
  - Logging user's action that don't follow company's policy supplement directive control (policy here).

Employees Data

In European Union, the following principles must be applied in regard to the datas collected by a organization about its employees :

- **Finality**, data must be used for an explicit and legitimate purpose.
- **Necessity**, require that the monitoring method be absolutly necessary. If a less intrusive methods exist, it must be used.
- **Transparency**, require that the users are totally aware of the data collection and the finality.
- **Legitimacy**, require that the data collection is the result of a legal requirement.
- **Proportionality**, require that the employees monitoring to be adapted to the level of threat.
- **Data accuracy** require that private information are kept acurate and up to date.
- **Security** require that the employer take security precaution to protect employees's data.
- **Awarness of the Staff** require that the staff handle that handle the datz to be trained.

GDPR and Privacy Shield

GDPR is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.
This is the main items of the GDPR :

- In case of data breach, the companies must inform the authorities within 24 hours.
- Every EU country must create a central data authority.
- Individuals must have access to their own data.
- Every individual information must be transferable from one service provider to another.
- Individuals have the right to be forgotten. All their informations should be deletable.

EU–US Privacy Shield :
In October 2015 the European Court of Justice declared the previous framework called the International Safe Harbor Privacy Principles invalid. Soon after this decision the European Commission and the U.S. Government started talks about a new framework and on February 2, 2016 they reached a political agreement. The European Commission published the "adequacy decision" draft, declaring principles to be equivalent to the protections offered by EU law.

Intellectual Property

- **Patents** protect inventions. A patent will leave the exclusive rights regarding an invention in the hands of its owner for a period of 20 years, but after the end of that period, the invention becomes part of the public domain. An invention as such should possess three inherent prerequisites:
    1. Must be new
    2. Must be useful
    3. Must not be obvious

  In the technology domain, patents covering hardware devices and manufacturing processes have been issued for many years now. There is still uncertainty, however, on how patents for software inventions would hold up to the scrutiny of most courts.

- **Copyright** protect artistical, literacy, musical or even program through its source code.
- **Trademark** is a recognizable sign, design, or expression which identifies products or services of a particular source from those of others. Trademarks rights must be maintained through actual lawful use of the trademark. These

rights will cease if a mark is not actively used for a period of time, normally 5 years in most jurisdictions.
Trademark Dilution occurs when someone uses a famous mark in a manner that blurs or tarnishes the mark. Using Windows as the name of a toilet cleaner for example can diminish the value of the mark Windows.

- **Trade Secret**

2 - Asset Security

IT asset management (ITAM) is the set of business practices that join financial, contractual and inventory functions to support life cycle management and strategic decision making for the IT environment. Assets include all elements of software and hardware that are found in the business environment.
IT asset management (also called IT inventory management) is an important part of an organization's strategy. It usually involves gathering detailed hardware and software inventory information which is then used to make decisions about hardware and software purchases and redistribution. IT inventory management helps organizations manage their systems more effectively and saves time and money by avoiding unnecessary asset purchases and promoting the harvesting of existing resources. Organizations that develop and maintain an effective IT asset management program further minimize the incremental risks and related costs of advancing IT portfolio infrastructure projects based on old, incomplete and/or less accurate information.
Inventory management deals with what assets are there, where they reside and who owns them.
Configuration management adds a relationship dynamic relating the other items in the inventory. This VM is in this ESX in this rack for example.

The stages of data management process :

1. Capture/Collect
2. Digitalization
3. Storage
4. Analysis
5. Presentation
6. Use

FIPS 199 helps organizations categorize their information systems.

List of criteria to classify data :

- Usefulness
- Timeliness
- Value or cost
- Lifetime or expiration period
- Disclosure damage assessment
- Modification damage assessment
- National or business security implications

- Storage
- ...

The U.S. government/military classification :

- Top secret
- Secret
- Confidential
- Sensitive
- Unclassified

The commonly used commercial or private classification :

- Confidential
- Private
- Sensitive
- Public

List of Breach/vulnerabilities Families

- XSRF is breach that use an already existing session on a sensible site. For example if a user have a running session to its bank site and is browsing another site at the same time. If the other site make a link like http://banksite/sendmoneyto?account=hackeraccount&value=440 , the transaction can be done without the bank requesting anything because the user is already logged.
  The countermease is to have a validation to each critical function exposed. The validation can be a CAPTCHA or an SMS validation for example.
- Side-Channel attack is any attack based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself (e.g. cryptanalysis and software bugs). Timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information, which can be exploited. Side-Channel attack include the following :
  - **Cache attack** — attacks based on attacker's ability to monitor cache accesses made by the victim in a shared physical system as in virtualized environment or a type of cloud service.
  - **Timing attack** — attacks based on measuring how much time various computations (such as, say, comparing an attacker's given password with the victim's unknown one) take to perform.
  - **Power-monitoring attack** — attacks that make use of varying power consumption by the hardware during computation.
  - **Electromagnetic attack** — attacks based on leaked electromagnetic radiation, which can directly provide plaintexts and other information. Such measurements can be used to infer cryptographic keys using techniques equivalent to those in power analysis or can be used in non-cryptographic attacks, e.g. TEMPEST (aka van Eck phreaking or radiation monitoring) attacks.

- **Acoustic cryptanalysis** — attacks that exploit sound produced during a computation (rather like power analysis).
- **Differential fault analysis** — in which secrets are discovered by introducing faults in a computation.
- **Data remanence** — in which sensitive data are read after supposedly having been deleted. (i.e. Cold boot attack)
- **Software-initiated fault attacks** — Currently a rare class of side-channels, Row hammer is an example in which off-limits memory can be changed by accessing adjacent memory too often (causing state retention loss).
- **Optical** — in which secrets and sensitive data can be read by visual recording using a high resolution camera, or other devices that have such capabilities (see examples below).

- Meet In The Middle Attack is a generic space–time tradeoff cryptographic attack against encryption schemes which rely on performing multiple encryption operations in sequence. The MITM attack is the primary reason why Double DES is not used and why a Triple DES key (168-bit) can be bruteforced by an attacker.
- A **skimmer** is a device installed on an ATM or device where user slide its card in it. The skimmer read the card magnetic strip or scan the card number.

Data anonymization

To protect privaty information, it's common to modify data to make it harder, or impossible, to link with the original person.

- **Anonymization** is simply removing the personal data that can be used to identify the original subject. It is not reversible.
- **Pseudonymization** is changing the name of the subject, to a fictiional name or an ID. It is reversible if the relation between the new name and the old name exist.
- **Tokenization** is like pseudonymization, but to retrieve the original data, it's needed to go through a complexe process. It is reversible too.

Security Testing and Evaluation

FISMA require every government agencies to pass a Security Testing and Evaluation, a process that contain 3 categories :

1. **Management Controls** focus on risk assessment, for example doing a risk assessment every year is a management control.
2. **Operational Controls** focus on process executed by human. Checking a policy and how it is enforced is an operational controls.
3. **Technical Controls** focus on process executed or configured on a machine. Configure system to ask for password change every 60 days is a technical control.

3 - Security Architecture and Engineering

Access Control Models

- **MAC** is a model based on data classification and object label. Each data have a label assigned, Top Secret for example, and for example a project, let's say "Mission Pass the CISSP". When a user (after Authentification) try to reach the object "Mission pass the CISSP", the OS check if the user have the clearance to access a Top Secret project. If yes, the OS then check if the users have the "need to know" on the project "Mission pass the CISPP".
  It's important to have an accurate classification of the data to have a functionnal MAC system.
  MAC have different security modes, depending on the type of users, how the system is accessed, etc. This is a table with the different security modes :

	Proper clearance for	Formal access approval for	A valid need to know for	Description
Dedicated security mode	ALL information on the system.	ALL information on the system.	ALL information on the system.	This mode is the equivalent of having only the Top Secret level, for example , on the system.
System high security mode	ALL information on the system	ALL information on the system	SOME information on the system	This mode is the equivalent of having only the Top Secret level, for example, on the system, but there is also multiple project, CISSP and CCIE for example. A user need to have a need-to-know on a project to be able to have access to it.
Compartmented security mode	ALL information on the system	SOME information on the system	SOME information on the system	This mode have multiple level of security (Confidential, Secret, Top-Secret) and multiple project (CISSP and CCIE).
Multilevel security mode	SOME information on the system	SOME information on the system	SOME information on the system	This mode have multiple Compartmented security mode running on parallele.

- **Different type of MAC**
  - **Hierarchical environments** are structured like tree. The top of the tree give access to all the tree. It's possible to read below in the tree but not in another branch.
  - **Compartmentalized environments**, there is no relation between the different security domain hosted in it. To gain access to a object, a subject need to have the exact clearance for the object's security domain.
  - **Hybrid environments** combines hierarchical and compartmentalized. Hybrid MAC environment provide the more granular control over access but become difficult to manage when the environment grow.

- **DAC** is a type of access control defined "as a means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control)". For example, a

user "Rox" in the group "CISSP Student" create a directory "CISSP_Doc", the directory's owner is now "Rox". "Rox" can do decide that he have the read, write and execute right on the Directory and give only the read right to the users in the group "CISSP Student". Linux is DAC system (but it's possible to use other access control).

- **RBAC** is an access control type defined around roles and privileges. The components of RBAC such as role-permissions, user-role and role-role relationships make it simple to perform user assignments.
- **ABAC** Attribute Based Access Control also known as Policy-based access control, defines an access control paradigm whereby access rights are granted to users through the use of policies which combine attributes together. The policies can use any type of attributes (user attributes, resource attributes, object, environment attributes etc.). This model supports Boolean logic, in which rules contain "IF, THEN" statements about who is making the request, the resource, and the action. For example: IF the requestor is a manager, THEN allow read/write access to sensitive data.
    1. The PEP or Policy Enforcement Point: it is responsible for protecting the apps and data you want to apply ABAC to. The PEP inspects the request and generates an authorization request from it which it sends to the **PDP**.
    2. The PDP or Policy Decision Point is the brain of the architecture. This is the piece which evaluates incoming requests against policies it has been configured with. The PDP returns a Permit / Deny decision. The PDP may also use **PIP**s to retrieve missing metadata.
    3. The PIP or Policy Information Point bridges the PDP to external sources of attributes e.g. LDAP or databases.

Security Models

- **Bell-LaPadula Model** is model focused on confidentiality.
  No Read Up is the simple rule for this model.
  No Write Down is the star rule for this model.
  Strong Star rule say no *write up*.
- **Biba Model** is a model focused on integrity.
  No Read Down is the simple rule for this model.
  No Write Up is the star rule for this model.
- **Clark-Wilson Model** is a model focused on integrity. The Clark-Wilson model enforces separation of duties to further protect the integrity of data. This model employs limited interfaces or programs to control and maintain object integrity.
- **Brewer-Nash** is also called Chinese wall model. A subject can write to an object only if it cannot read another object that is in a different dataset. Information flow model, provides access control mechanism that can change dynamically depending on user's authorization and previous actions. Main goal is to protect against conflict of interest by user's access attempts. Chinese Wall model is more context oriented in that it prevents a worker consulting for one firm from accessing data belonging to another, thereby preventing any COI.
- NonInterference also name **Goguen-Meseguer** is a strict multilevel security policy model, first described by Goguen and Meseguer in 1982, and amplified further in 1984.

In simple terms, a computer is modeled as a machine with inputs and outputs. Inputs and outputs are classified as either low (low sensitivity, not highly classified) or high (sensitive, not to be viewed by uncleared individuals). A computer has the non-interference property if and only if any sequence of low inputs will produce the same low outputs, regardless of what the high level inputs are.
That is, if a low (uncleared) user is working on the machine, it will respond in exactly the same manner (on the low outputs) whether or not a high (cleared) user is working with sensitive data. The low user will not be able to acquire any information about the activities (if any) of the high user.

- **Graham-Dennin** is an ACM model that addresses the security issues associated with how to define a set of basic rights on how specific subjects can execute security functions on an object. The model has eight basic protection rules (actions) that outline:
  - How to securely create an object.
  - How to securely create a subject.
  - How to securely delete an object.
  - How to securely delete a subject.
  - How to securely provide the read access right.
  - How to securely provide the grant access right.
  - How to securely provide the delete access right.
  - How to securely provide the transfer access right.

  Moreover, each object has an owner that has special rights on it, and each subject has another subject (controller) that has special rights on it.
  The model is based on the Access Control Matrix model where rows correspond to subjects and columns correspond to objects and subjects, each element contains a set of rights between subject i and object j or between subject i and subject k.
  For example an action A[s,o] contains the rights that subject s has on object o (example: {own, execute}). When executing one of the 8 rules, for example creating an object, the matrix is changed: a new column is added for that object, and the subject that created it becomes its owner.

- **Zachman Framework** is a framework created in 1980 at IBM. It's an ACM based on the view of an architecture from different point of view. The point of view are represented in a table (not finished here yet) :

	DATA, what	FUNCTION, how	NETWORK, where	PEOPLE, who	TIME, when	MOTIVATION, why
Planner :	Important Business	Business process	Business location	Important organizations	Business events	Business Goals
Owner :	Conceptual Data Model					
Designer :	Logical Data Model					
Builder :	Physical Data Model					

Programmer :	Data Definition					
User :	Usable Data					

- **Concentric Circles** An underlying principal for providing good security involves a concept called “Concentric Circles of Protection”, sometimes also called "Security in Depth". This concept involves the use of multiple “rings” or “layers” of security. The first layer is located at the boundary of the site, and additional layers are provided as you move inward through the building toward the high-value assets.
- **Sutherland** model is based on the idea of defining a set of system states, initial states, and state transitions. Through the use of and limitations to only these predetermined secure states, integrity is maintained, and interference is prohibited. The Sutherland model focuses on preventing interference in support of integrity. This model is based on the idea of defining a set of system states, initial states, and state transitions. Through the use of and limitations to only these predetermined secure states, integrity is maintained, and interference is prohibited.
- **Lipner** Model combine the elements of Bell-LaPadula model and Biba model to provide confidentiality and Integrity.

Security Evaluation Methods

- **TCSEC** is a United States Government Department of Defense (DoD) standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system. The TCSEC was used to evaluate, classify, and select computer systems being considered for the processing, storage, and retrieval of sensitive or classified information.

  The TCSEC, frequently referred to as the Orange Book, is the centerpiece of the DoD Rainbow Series publications. Initially issued in 1983 by the National Computer Security Center (NCSC), an arm of the National Security Agency, and then updated in 1985, TCSEC was eventually replaced by the Common Criteria international standard, originally published in 2005.
  The Red Book, also known as the Trusted Network Interpretation, is a supplement to the orange book, that describe security evaluation criteria for networked systems.
  The rating schema of TCSEC :

  - **D** – Minimal protection
    - Reserved for those systems that have been evaluated but that fail to meet the requirements for a higher division.

  - **C** – Discretionary protection (DAC)
    - C1 – Discretionary Security Protection
    - C2 – Controlled Access Protection

- **B** – Mandatory protection (MAC)
  - B1 – Labeled Security Protection
  - B2 – Structured Protection
  - B3 – Security Domains
  - Satisfies reference monitor requirements

- **A** – Verified protection
  - A1 – Verified Design
  - Beyond A1

- **ITSEC**
- **Common Criteria** is a framework to test product, in which computer system users can specify their Security Functional and Assurance Requirements (SFRs and SARs respectively) in a ST. The CC for Information Technology Security Evaluation (referred to as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification. It is currently in version 3.1 revision 5.
  Each TOE have
  - PP a document, which identifies security requirements for a class of security devices (for example, smart cards used to provide digital signatures, or network firewalls) relevant to that user for a particular purpose. Product vendors can choose to implement products that comply with one or more PPs
  - ST a document that identifies the security properties of the target of evaluation. The ST may claim conformance with one or more PPs.
    The TOE is evaluated against the SFRs established in its ST, no more and no less. This allows vendors to tailor the evaluation to accurately match the intended capabilities of their product. This means that a network firewall does not have to meet the same functional requirements as a database management system, and that different firewalls may in fact be evaluated against completely different lists of requirements.
  - SFR specify individual security functions which may be provided by a product. The Common Criteria presents a standard catalogue of such functions. For example, a SFR may state how a user acting a particular role might be authenticated.
  - SAR, is a descriptions of the measures taken during development and evaluation of the product to assure compliance with the claimed security functionality.

    EAL is level of Evaluation that have been tested on a TOE. EAL are separated in 7 level of testing :

5. **EAL1** : Functionally Tested
6. **EAL2** : Structurally Tested
7. **EAL3** : Methodically Tested and Checked
8. **EAL4** : Methodically Designed, Tested and Reviewed
9. **EAL5** : Semiformally Designed and Tested
10. **EAL6** : Semiformally Verified Design and Tested
11. **EAL7** : Formally Verified Design and Tested

ITIL

ITIL is an operational framework created by CCTA, requested by the UK's gov in the 1980s. ITIL provide documentation on IT best practice to improve performance, productivity and reduce cost.
It's divided into the 5 mains following categorie :

1. Service Strategie
2. Service Design
3. Service Transition
4. Service Operation
5. Continual Service Improvement

Misc

ISO 27001 is derived from **BS 7799**. It's focused on Security Governance.

ISO 27002 is derived from **BS 7799**. It's a security standard that recommend security controls based on industry best practices.

It is to be noted that the **CMM**, while originally create to develop software, can be adapted to handle the security management of a company. Each phase correspond to a certain level of maturity in the documentation and the control put in place.
The first phase, **initial**, is where there is no process, no documentation, no control in place. The team reply to each incident by reacting to it.
At the last phase, **optimizing**, the process are sophisticated and the organization is able to adapt to new threats. Every step are covered in Chapter 8.

Covert Timing Channel conveys information by altering the performance of a system component in a controlled manner. It's very difficult to detect this type of covert channel. Covert Storage Channel is writting to a file accessible by another process. To avoid it, the read/write access must be controlled.

A nonce, short for *number used once*, is an arbitrary number that can be used just once in a cryptographic communication. It is often a random or pseudo-random number issued in an authentication protocol to ensure that old communications cannot be reused in replay attacks. They can also be useful as initialization vectors and in cryptographic hash functions.

An initialization vector (IV) is an arbitrary number that can be used along with a secret key for data encryption. This number, also called a nonce, is employed only one time in any session.
The use of an IV prevents repetition in data encryption, making it more difficult for a hacker using a dictionary attack to find patterns and break a cipher.

DRAM use capacitor to store information, unlike SRAM that use flip-flops. DRAM require power to keep information, as it constantly need to be refreshed because the capacitor leak charge over time.
DRAM is cheaper but slower than SRAM.

CVE is the part of SCAP that provide a naming system to describe security vulnerabilities.
CVSS is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat. Scores are calculated based on a formula that depends on several metrics that approximate ease of exploit and the impact of exploit. Scores range from 0 to 10, with 10 being the most severe. CVSS metrics is influnced by three groups of metrics :

1. **Base metrics** indicate the severity of the vulnerability is given by the vendor or the entity that found the vulnerability. It have the largest influence on the CVSS score.
2. **Temporal metrics** indicate the urgency of the vulnerability, it's also given by the vendor or the entity that found the vulnerability.
3. **Environmental metrics** is set by the end-user. It indicate how an environment or end-users organization is impacted. It's optional.

The mase metrics are used to calculate the temporal metrics which are used to calculate the environmental metrics.
XCCDF is the SCAP component that describe security checklist.

SABSA Matrix :

1. Contextual
2. Conceptual
3. Logical
4. Physical
5. Component
6. Operational

Processor Ring

1. Kernel
2. OS components
3. Device drivers
4. Users

Application in Ring 0 can access data in Ring1, Ring2 and Ring3. Application in Ring1 can access data in Ring2 and 3. Application in Ring 2 can access data in Ring3.

Boolean Operator

- **AND** (∧) return true if input 1 and input 2 (colum in1 and in2 in the table) are true. Both need to be true.

in1	in2	res
0	0	0
0	1	0
1	0	0
1	1	1

- **OR** (∨) return true if input 1 or input 2 is true. At least one input must be true, but both can be true to return true.

in1	in2	res
0	0	0
0	1	1
1	0	1
1	1	1

- **NOT** (**~**) take only one input and return the opposite. It return false if the input in true and true if the input is false.

in1	res
0	1
1	0

- **XOR** (⊕) return true if the parameter are different.

in1	in2	res
0	0	0
0	1	1
1	0	1
1	1	0

Cipher, Encryption, Hash, Protocol

Encryption

- **AES** also known by its original name Rijndael is a specification for the encryption of electronic data established by the NIST in 2001. It's a symmetric-key algorithm and it use a block size of 128bits, but three different key length, 128, 192 and 256 bits.

- **CHAP** is an authentication protocol using symmetric key. It's protected against replay attack and reauthenticate the client during the session. CHAP use a 3 ways handshake. It's used in PPPand others protocols.
- **Twofish** is a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits. It was one of the five finalists of the Advanced Encryption Standard contest, but it was not selected for standardization. Twofish is related to the earlier block cipher Blowfish.
  The Twofish algorithm uses an encryption technique not found in other algorithms that XORs the plain text with a separate subkey before the first round of encryption. This method is called prewhitening.
- Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. However, the AES now receives more attention, and Schneier recommends Twofish for modern applications. Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits.
- **RSA** is one of the first public-key cryptosystems and is widely used for secure data transmission. It's a slow algorithm and generally doesn't encrypt users data, but is used during key exchange for faster symmetric key algorithm. Replay attack can't be used against RSA. But brute-force, mathematical and timing attack are possible.
- **DES** is a symmetric-key algorithm for the encryption of electronic data, published as a FIPS in 1977. It use a 56bits key, making it too insecure for modern application. The block length is 64bits.
  DES have multiple mode, ordered below from the best to the worst :
  - **CTR** mode use a 64 bits counter for feedback. As this counter doesn't depend on the previous bits or block for encryption, CTR can encrypt blocks in parallele. CFB, like OFB, doesn't propagate errors.
  - **OFB** mode makes a block cipher into a synchronous stream cipher. It generates keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext. Just as with other stream ciphers, flipping a bit in the ciphertext produces a flipped bit in the plaintext at the same location. This property allows many error correcting codes to function normally even when applied before encryption.
  - **CFB** is a block cipher mode, using a memory buffer to have same size block. It's retired due to the wait in encoding each block. The Cipher Feedback (CFB) mode, a close relative of CBC, makes a block cipher into a self-synchronizing stream cipher.
  - **CBC** mode employs an IV and chaining to destroy cipher text patterns. Because CBC works in block mode, it decrypt message one block at a time. Because it use IV and chaining to prevent leaving text patterns through propagation, if an error happen during reading or transfer, the encrypted file will be unusable.
  - **ECB** It's the weakest DES mode. The disadvantage of this method is a lack of diffusion. Because ECB encrypts identical plaintext blocks into identical ciphertext blocks, it does not hide data patterns well. In some senses, it doesn't provide serious message confidentiality, and it is not recommended for use in cryptographic protocols at all.

- **3DES**
- **S/MIME** is a standard for public key encryption and signing of MIME data (mail). Developed by the RSA company, S/MIME provides the following cryptographic security services for electronic messaging applications:
  - Authentication
  - Message integrity
  - Non-repudiation of origin (using digital signatures)
  - Privacy
  - Data security (using encryption)
- **PGP** is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. Phil Zimmermann developed PGP in 1991. It use a web of trust between users.
- **SEAL** is a stream cipher optimised for machines with a 32-bit word size and plenty of RAM. It use a 160-bit key.
- **Vigenère Cipher** is a cipher that use a square matrix to encrypt text. It's an old cipher first described in 1533.
- **Book Cipher** is a cipher that use a known book to cipher a text. For example for a key 5-5.78-3, the receiver just have to know the book is Moby Dick, for example, then goes to page 5, take word five, and then to page 78 work 3.
- P2PE is a standard created by PCI DSS that encrypt the data from the bank card reader to the payment processor.
- E2EE is like P2PEE but data are decrypted multiple time before reaching the payment processor.

Hash

- **DSA** is a FIPS for digital signature. Messages are signed by the signer's private key and the signatures are verified by the signer's corresponding public key. The digital signature provides message authentication, integrity and non-repudiation. The three algorithms described in the FIPS are **DSA**, **RSA**, and ECDSA
- **SHA-1** is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value known as a message digest – typically rendered as a hexadecimal number, 40 digits long. It's deprecated to due collision.
- **SHA-2** is a set of cryptographic hash functions designed by the NSA. The SHA-2 family consists of six hash functions with digests (hash values) that are 224, 256, 384 or 512 bits: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256.
- **HMAC** is a hash method with a passwork. So only a person that have the password can calculate or check the right hash.
- **ECDSA** is an implementation of DSA that use elliptic curve. For a same sized key, ECDSA is more secure than DSA.

Encryption/Hash Summary

Name	Type	Key Length	Bloc Lenght	Hash Length	Remark
AES	Symmetric Block Cipher	128, 192, 256	128		
Blowfish	Symmetric Block Cipher	32–448	64		
Twofish	Symmetric Block Cipher	128, 192, 256	128		
DES	Symmetric Block Cipher	56 + 8 parity bits	64		DES have multiple mode, ranked from better to worse : CTR OFB is the stream version of DES. CFB CBC ECB is the weakest, leave pattern in the ciphertext.
3DES	Symmetric Block Cipher	56, 112, 168	64		3DES is *just* DES applied 3 times. The key length depend if each DES round use a different key or not. option 1 : DES(key**1**) + DES(key**2**) + DES(key**3**) option 2 : DES(key**1**) + DES(key**2**) + DES(key**1**) option 1 : DES(key**1**) + DES(key**1**) + DES(key**1**) As 3DEs is vulnerable to Meet-in-the-middle attack, the max effective key length is 112 bits
RSA	asymmetric	~			As of 2020, the minimum key should 2048. In 2030, it should be 3072.
SHA-1	Hash			160	Cryptographic weaknesses were discovered and the standard was no longer approved for most cryptographic uses after 2010.
SHA-2	Hash			224, 256, 384, 512	
SHA-3	Hash			224, 256, 384, 512	
MD5	Hash		512	128	Collision can be done in less than a second on a modern computer.

Protocol/Standard

- **X.509** is an ITU standard defining the format of public key certificates. X.509 certificates are used in many Internet protocols, including TLS/SSL
- **CRL** is "a list of digital certificates that have been revoked by the issuing certificate authority (CA) before their scheduled expiration date and should no longer be trusted".
- **OSCP** is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate. It is described in RFC6960 and is on the Internet standards track. It was created as an alternative to CRL, specifically addressing certain problems associated with using CRLs in a public key infrastructure (PKI). Messages communicated via OCSP are encoded in ASN.1 and are usually communicated over HTTP. The "request/response" nature of these messages

leads to OCSP servers being termed OCSP responders. The OSCP server reply by "good", "revoked" or "unknown". Unknown is when the OSCP have no info about a certificat. Some web browsers use OCSP to validate HTTPS certificates. However, the most popular browser, Google Chrome, only uses CRL.

- **PEM** is a de facto file format for storing and sending cryptographic keys, certificates, and other data. Because DER produces binary output, it can be challenging to transmit the resulting files through systems, like electronic mail, that only support ASCII. The PEM format solves this problem by encoding the binary data using base64. PEM also defines a one-line header, consisting of "-----BEGIN ", a label, and "-----", and a one-line footer, consisting of "-----END ", a label, and "-----". The label determines the type of message encoded. Common labels include "CERTIFICATE", "CERTIFICATE REQUEST", and "PRIVATE KEY".
- **IPsec** is a secure network protocol suite that authenticates and encrypts the packets of data sent over an internet protocol network. It's used to create VPN. IPsec use the following protocols :
  - AH provide integrity and authentification of the IP header. It's the IP protocol number 51.
  - ESP is a member of the IPsec protocol suite. It provides origin authenticity through source authentication, data integrity through hash functions and confidentiality through encryption protection for IP packets. In transport mode, ESP doesn't provide authentication and integrity (AH does it then) for the entire packet but it does in tunnel mode because the original packet is encapsulated, ciphered and hashed checked. A new IP packet containing the original packet. ESP is also used to provide integrity for L2TP.
  - IPComp is a low level compression protocol for IP datagrams.
  - IKE is the protocol used to set up a **SA** in the IPsec protocol suite. It use ISAKMP and X.509.
  - ISAKMP is a protocol used for establishing SA and cryptographic keys in an Internet environment. It use IKE or other key exchange protocols.
  - **Oakley** Key Determination Protocol is a key-agreement protocol that allows authenticated parties to exchange keying material across an insecure connection using the Diffie–Hellman key exchange algorithm.
- **S-HTTP** is an obsolete alternative to the HTTPS protocol for encrypting web communications carried over HTTP. HTTPS and S-HTTP were both defined in the mid-1990s to address this need. S-HTTP was used by Spyglass's web server, while Netscape and Microsoft supported HTTPS rather than S-HTTP, leading to HTTPS becoming the de facto standard mechanism for securing web communications. S-HTTP encrypts only the served page data and submitted data like POST fields, leaving the initiation of the protocol unchanged. Because of this, S-HTTP could be used concurrently with HTTP (unsecured) on the same port, as the unencrypted header would determine whether the rest of the transmission is encrypted. Encryption is said to be done at the application layer. In contrast, HTTP over TLS wraps the entire communication within TLS (formerly SSL), so the encryption starts before any protocol data is sent.
- **SET** is a communications protocol standard for securing credit card transactions over networks, specifically, the Internet. SET was not itself a payment system. It

failed to gain attraction in the market. VISA now promotes the 3-D Secure scheme. It use, among others, RSA and DES.

- **DH** key exchange is a method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as originally conceptualized by Ralph Merkle and named after Whitfield Diffie and Martin Hellman. It use discrete logarithm.

Cryptography remark

The symmetrics algorithms have stronger encryption per key bits than asymmetric algorithms.
For exemple : **AES** > **3DES** > **RSA**

Key Clustering in cryptography, is two different keys that generate the same ciphertext from the same plaintext by using the same cipher algorithm. A good cipher algorithm, using different keys on the same plaintext, should generate a different ciphertext irrespective of the key length.

Zero-knowledge Proof is a method by which one party (the prover) can prove to another party (the verifier) that they know a value x, without conveying any information apart from the fact that they know the value x. The essence of zero-knowledge proofs is that it is trivial to prove that one possesses knowledge of certain information by simply revealing it; the challenge is to prove such possession without revealing the information itself or any additional information.

Certification and Accreditation

Trust comes first. Trust is built into a system by crafting the components of security. Then assurance (in other words, reliability) is evaluated using certification and/or accreditation processes.

Fire Extinguisher

There is no official standard in the United States for the color of fire extinguishers, though they are typically red, except for class D extinguishers which are usually yellow, water and Class K wet chemical extinguishers which are usually silver, and water mist extinguishers which are usually white.

Class	Intended use	Mnemotechnic
A	Ordinary Combustible Wood, Paper, etc...	**A**sh
B	Flammable liquids and gases	**B**arrel
C	Energized electrical equipment	**C**urrent
D	Combustible metals	**D**ynamite
K	Oils and fats	**K**itchen

Gas-based fire suppression system

The Montreal Protocols (1989) limit the use of certain type of gas, Halon for example is forbidden. This is list of gas-based fire suppression system :

- **FM-200** is a gas used primarily to protect server romm or data center. It lower the temperature of the room. It is not dangerous to human.
- **CO^2** suppress fire by remove the oxygen. It can kill human so it's not user where human are working.
- **Dry Pipe** are generally configured to start if the gas-based system failed to estinguish the fire.
- **Dry Powders** are mix of CO^2, water and chemical. It generally destroy the equipment.
- **FE-13** is the safest fire suppression system in an electrical environment.It's safe for human and computer.

Pipe system

- **Wet Pipe** system are filled with water. When the sprinkler break due to the temperature increase, it release the water.
- **Dry Pipe** Sprinkler system are filled with compressed air. When the sprinkler break, the pression drop allowing the valve to let the water flow. It is used where temperature are very low, to prevent the water from freezing in the pipe.
- **Deluge System** are almost like dry pipe system. When the fire alarm is triggered, it also open a valve to let the water flow.

NFPA standard 75 require building hosting information technology to be able to withstand at least 60 minutes of fire exposure.

Fence, Lighting

NIST standard pertaining to perimeter protection states that critical areas should be illuminated eight feet high and use two foot-candles (2,4 and 0.6 meter), which is a unit that represents the illumination power of an individual light.

4 - Communication and Network Security

OSI Model

The OSI model is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to its underlying internal structure and technology. Its goal is the interoperability of diverse communication systems with standard protocols. The model partitions a communication system into abstraction layers. The original version of the model defined seven layers.
A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that comprise the contents of that path. Two instances at the same layer are visualized as connected by a horizontal connection in that layer.

1. **Physical**
2. **Data Link** (frame)
   Example of protocols : ATM, Frame-Relay, PPTP, L2TP
3. **Network** (datagram/packet)
   Example of protocols : IPSec
4. **Transport**
   The verification of the packets (segments) delivery occurs a this layer.
   Example of protocols : TCP, UDP, TLS, SSL, SCTP, DCCP
5. **Session**
   The session layer provides the mechanism for opening, closing and managing a session between end-user application processes, i.e., a semi-permanent dialog. Communication sessions consist of requests and responses that occur between applications.
   Example of protocols : SQL, RPC
6. **Presentation**
   It's the first layer after the "packet state". Compression and encryption happen at the presentation layer. Characters encoding too.
7. **Application**
   It manage communication between application. HTTP is used between a web server and a browser for example.
   Example of protocols : HTTP, SMTP, DNS

A mnemotechnic sentence to remember the order of the OSI layers :

A	**A**ll	**A**pplication	
P	**P**eople	**P**resentation	
S	**S**eems	**S**ession	
T	**T**o	**T**ransport	**S**egment (TCP), **D**atagram (UDP)
N	**N**eed	**N**etwork	**P**acket
D	**D**ata	**D**ata Link	**F**rame
P	**P**rocessing	**P**hysical	

A view of the *frame, datagram, segments* :

L2
Data Link, frame
L3
Network, datagram/packet
L4
Transport, segment

TCP/IP Model

TCP/IP is the conceptual model and set of communications protocols used in the Internet and similar computer networks. It is commonly known as TCP/IP because the foundational protocols in the suite are the TCP and the Internet Protocol (IP). It's also modeled in layer :

- **Application layer** is the scope within which applications, or processes, create user data and communicate this data to other applications on another or the same host. The applications make use of the services provided by the underlying lower layers, especially the transport layer which provides reliable or unreliable pipes to other processes. The communications partners are characterized by the application architecture, such as the client-server model and peer-to-peer networking. This is the layer in which all higher-level protocols, such as SMTP, FTP, SSH, HTTP, operate. Processes are addressed via ports which essentially represent services.
- **Transport layer** performs host-to-host communications on either the same or different hosts and on either the local network or remote networks separated by routers. It provides a channel for the communication needs of applications. UDP is the basic transport layer protocol, providing an unreliable datagram service. The Transmission Control Protocol provides flow-control, connection establishment, and reliable transmission of data.
- **Internet layer** exchanges datagrams across network boundaries. It provides a uniform networking interface that hides the actual topology (layout) of the underlying network connections. It is therefore also referred to as the layer that establishes internetworking. Indeed, it defines and establishes the Internet. This layer defines the addressing and routing structures used for the TCP/IP protocol suite. The primary protocol in this scope is the Internet Protocol, which defines IP addresses. Its function in routing is to transport datagrams to the next IP router that has the connectivity to a network closer to the final data destination.
- **Link layer** defines the networking methods within the scope of the local network link on which hosts communicate without intervening routers. This layer includes the protocols used to describe the local network topology and the interfaces needed to effect transmission of Internet layer datagrams to next-neighbor hosts.

TCP useful information

- **<u>Connection opening, three ways hand-shake</u>**

A	===	SYN	==>	B	The active open is performed by the client sending a SYN to the server. The client sets the segment's sequence number to a random value A.
A	<==	SYN/ACK	===	B	In response, the server replies with a SYN-ACK. The acknowledgment number is set to one more than the received sequence number i.e. A+1, and the sequence number that the server chooses for the packet is another random number, B.
A	===	ACK	==>	B	Finally, the client sends an ACK back to the server. The sequence number is set to the received acknowledgement value i.e. A+1, and the acknowledgement number is set to one more than the received sequence number i.e. B+1.

- At this point, both the client and server have received an acknowledgment of the connection. The steps 1, 2 establish the connection parameter (sequence

number) for one direction and it is acknowledged. The steps 2, 3 establish the connection parameter (sequence number) for the other direction and it is acknowledged. With these, a full-duplex communication is established.

- **Connection termination, four ways hand-shake**

A	===	FIN	==>	B	- A is telling B it'll close the connection. As a TCP connection is full duplex (both ways), it's just closing A to B, not B to A.
A	<==	ACK	===	B	- B acknowledge the closing.
A	<==	FIN	===	B	- B send a FIN packet to close the connection B to A.
A	===	ACK	==>	B	- A acknowledge the closing. B to A is now closed too.

- A connection can be "half-open", in which case one side has terminated its end, but the other has not. The side that has terminated can no longer send any data into the connection, but the other side can. The terminating side should continue reading the data until the other side terminates as well.
  A Port scanner is an application designed to probe a server or host for open ports. Such an application may be used by administrators to verify security policies of their networks and by attackers to identify network services running on a host and exploit vulnerabilities.
  A port scan or portscan is a process that sends client requests to a range of server port addresses on a host, with the goal of finding an active port; this is not a nefarious process in and of itself. The majority of uses of a port scan are not attacks, but rather simple probes to determine services available on a remote machine.
  While port scan or portscan is the action to check all (or a defined list) the TCP/UDP ports on a target, portsweep is the action to the one port but on multiple server.
  The result of a port scan fall in one the three following categories :

- **Open, Accepted:** The host sent a reply indicating that a service is listening on the port.
- **Closed, Denied, Not Listening:** The host sent a reply indicating that connections will be denied to the port.
- **Filtered, Dropped, Blocked:** There was no reply from the host.

  A list of SCAN method :

- **TCP Scanning**
  or *connect* scan, check if a port is open by trying to open a complete connection. It's slow but doesn't require root or admin right.
- **SYN Scanning** is a mode that need the root or admin right because the scanner forge its packets, it doesn't use the OS full network stack. The scanner send a SYN packet, the target will reply with a SYN/ACK if the port is opened. The scanner reply directly with a RST packet, closing the connection before the end of the three way handshake. The target reply with a RST is the port is open.
  In short the sequence is :
  Scan send SYN to Target
  Target reply SYN/ACK to Scan
  Scan close with RST
  Target confirm close with RST.

- **UDP Scanning**
  is more complicated because there is no session. A server that receive a packet on a UDP port doesn't need to reply. A syslog port (UDP 514) just receive log, nothing is sent. Some application like TFTP may reply if the server receive a packet.
- **ACK scanning**
  is used to check if there is a firewall between the scanner and the target. A stateful firewall will block this scan while a TCP scan should be accepted if allowed.
- **FIN scanning**
  aim to bypass firewall as they are waiting for a SYN. If the target's port is closed, the target reply with a RST, else it doesn't reply.

  Port from 0 to 1023 are system-ports, or well known ports.
  Port from 1024 to 49151 are registered ports, which are also called user ports. They are assigned by **IANA** but doesn't require escalated system privilege to be used.
  Port from 49152 to 65535 anre dynamic ports.

  FTP use port 21 for authentication/control and 20 for the data.

  In IPv6, FE80::/10 is used to create unicast link-local address.

Network Attack

DDOS attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example, a botnet) flooding the targeted system with traffic. Some DDOS technique below :

- **SYN floods** flood attacks do not require completion of the TCP three way handshake and attempt to exhaust the destination SYN queue or the server bandwidth. Because the source IP addresses can be trivially spoofed, an attack could come from a limited set of sources, or may even originate from a single host.
- **Smurf Attack** spoof the IP of the target and send a large number of ICMP packet to a broadcast address. By default, the network device will reply to the spoofed ICMP packet, the target. It's an obsolete attack.
- **Fraggle Attack** is a variation of a Smurf attack where an attacker sends a large amount of UDP traffic to ports 7 (Echo) and 19 (CHARGEN) to an IP broadcast address, with the intended victim's spoofed source IP address.
- **Teardrop attack** consist of sending a large amount of TCP packets with overlapping payload. It can crash the TCP stack of the remote OS. It's not nescesseraly a distributed attack. It's an old attack and modern OS should not be vulnerable to it.
-
-

Pharming is a DNS attack that consist of try to send a lot of bad entry to a DNS. If a user request the same entry than the attack is trying to spoof, the DNS server may *think* the attacker packet are in fact reply to the users request.

Phreaking boxes are devices used by phone phreaks to perform various functions normally reserved for operators and other telephone company employees.
Most phreaking boxes are named after colors, due to folklore surrounding the earliest boxes which suggested that the first ones of each kind were housed in a box or casing of that color. However, very few physical specimens of phreaking boxes are actually the color for which they are named.
Today, most phreaking boxes are obsolete due to changes in telephone technology.

- Green box - Tone generator, emits 'coin accept', 'coin return' and 'ringback' tones at the remote end of an Automated Coin Toll Service payphone call. Obsolete.
- Blue box - Tone generator, emitted 2600 Hz tone to disconnect a long-distance call while retaining control of a trunk, then generated multi-frequency tones to make another toll call which was not detected properly by billing equipment. Obsolete.
- White box - DTMF tone dial pad.
- Black box - A resistor bypassed with a capacitor and placed in series with the line to limit DC current on received calls. The black box was intended to trip one but not both relays, allowing ringing to stop but not showing the call as answered for billing purposes. Obsolete.
- Red box - Tone generator, emitted an Automated Coin Toll Service tone pair (1700 Hz and 2200 Hz) to signal coins dropping into a payphone. Obsolete.

Bluetooth

Bluetooth use FHSS, the implementation is named AFH.

The cipher used is named E0, it can use a key up to 128bits, but it have weakness, the key length doesn't improve security and some attack have shown that even with a 128bits, it can be cracked like if the key is only 32bits.

Example of Bluetooth attack :

- Bluebugging : It's the process to infect a device and make the attacker able to listen through the device. WP
- Bluejacking : It's the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices. WP
- Bluesnarfing : It's the unauthorized access of information from a wireless device through a Bluetooth connection. WP

The different types of Firewall :

- **1st generation** are just firewall, that just allow the packet without inspecting anything.

- **2nd generation** are stateful filter that read the L4 (TCP/UDP or other) to maintain a session table. So the firewall will allow packets from both directions of the session (until the FIN|ACK).
- **3rd generation** are application layer firewall and are working at the application level. For example if a client try to open a request on a sever on the port 80 but doesn't send a valid HTTP request, the connection is closed and the packets are dropper.
- **4th generation** also name Application Level Gateway or Proxy Firewall act like a proxy.If a user reach a ressource, the firewall open the ressource and check it's nothing forbidden. It can decypher TLS (with the proper cert installed).
- **5th generation** are a type of firewall install on the user computer. It check everything at the OS level.

Intrusion Detection System are device or software that scan the network or behavior of a system to detect a virus/malware or forbeddin action. There is different type of IDS/IPS :

- Network Based
  Network Intrusion Detection Systems (NIDS) are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. It performs an analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of known attacks. Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator. An example of an NIDS would be installing it on the subnet where firewalls are located in order to see if someone is trying to break into the firewall.
- Host Based
  Host intrusion detection systems (HIDS) run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator if suspicious activity is detected.

IDS can use different detection method. They often use both methods :

- Signature-based
  Signature-based IDS refers to the detection of attacks by looking for specific patterns, such as byte sequences in network traffic, or known malicious instruction sequences used by malware. This terminology originates from anti-virus software, which refers to these detected patterns as signatures. Although signature-based IDS can easily detect known attacks, it is difficult to detect new attacks, for which no pattern is available.
- Anomaly-based
  Anomaly-based intrusion detection systems were primarily introduced to detect unknown attacks, in part due to the rapid development of malware. The basic approach is to use machine learning to create a model of trustworthy activity, and then compare new behavior against this model. Although this approach enables the detection of previously unknown attacks, it may suffer from false positives: previously unknown legitimate activity may also be classified as malicious. Most of the existing IDSs suffer from the time-consuming during detection process that degrades the performance of IDSs.

VoIP

Different Attacks :

- **SPIT** is like mail SPAM but with VoIP
- **Caller ID falsification**
- **Vishing** is trying to scam user by using VoIP.
- Remote dialing (aka hoteling) is the vulnerability or feature of a PBX system that allows for an external entity to piggyback onto the PBX system and make long-distance calls without being charged for the tolls.

Cabling

Name	Standard	Cable	Length	Remark
100Base-FX	802.3u-1995	Fiber 1300nm	2km	It's an old standard? 100BASE-FX is a version of Fast Ethernet over optical fiber.

WAN Line Type

Name	Bandwidth	Cable	Remark
T1	1.544Mbps	2 pair of shielded coper wire	
E1	2.084Mbps	2 pair of shielded coper wire	
T3	44.736Mbps		
E3	34.368Mbps		

WIFI

List of **802.11** protocols by frequency :

	900MHz	2.4GHz	5GHz	5.9GHz	60GHz	Modulation
802.11**a**			X			OFDM
802.11**b**		X				DSSS
802.11**g**		X				OFDM
802.11**n**		X	X			OFDM
802.11**ac**			X			
802.11**ad**					X	
802.11**af**						
802.11						

List of security protocol by 802.11 Protocol :

	WEP	WPA	WPA2
RC4		X	

TKIP		X	
AES			X

To avoid collision, 802.11 use CSMA/CA, a mecanism where a device that want to start a transmission send a jam request before sending anything else. CSMA/CA also requiere that the receiving device send an acknoledgement once the data are received. If the sender doesn't receive the acknoledgement, it try to resend the data.

Message Integrity Check is a feature of WPA to prevent MITM attack.

5 - Identity and Access Management (IAM)

In the U.S., two data-classification are mostly used :

- Government or Military classification, classified by the type of damage the involontary divulgation of the data would cause.
  - **Top Secret** is the highest level of classified information. Information is further compartmented so that specific access using a code word after top secret is a legal way to hide collective and important information. Such material would cause "exceptionally grave damage" to national security if made publicly available.
  - **Secret** material would cause "serious damage" to national security if it were publicly available.
  - **Confidential** material would cause damage or be prejudicial to national security if publicly available.
  - **Unclassified** is technically not a classification level, but this is a feature of some classification schemes, used for government documents that do not merit a particular classification or which have been declassified. This is because the information is low-impact, and therefore does not require any special protection, such as vetting of personnel.
- Corporate or Private sector classification.
  - **Confidential** is the highest level in this classification scheme. A considerable amount of damage may occur for an organization given this confidential data is divulged. Proprietary data, among other types of data, falls into this category. This category is reserved for extremely sensitive data and internal data. A “Confidential” level necessitates the utmost care, as this data is extremely sensitive and is intended for use by a limited group of people, such as a department or a workgroup, having a legitimate need-to-know.
  - **Private** are data for internal use only whose significance is great and its disclosure may lead to a significant negative impact on an organization. All data and information which is being processed inside an organization is to be handled by employees only and should not fall into the hands of outsiders.
  - **Sensitive** is data that have been classified and are not public data. If these data where disclosed, a negatif impact for company may happen.

- **Public** are data already published to the outside of the company or with no value. If these data had to be disclosed, no impact for the company would happen.

Subjects are active entity, user or program that manipulate an Object. A user (subject) request a HTTP server (object).

Objects are passive, manipulated by Subject. A database (object) is requested by a reporting program (subject).
It's important to note that an object in a situation can be a subject (and the opposite also) in another situation. If a user request a DB, the user in the subject, the DB is the object. But the DB can request its software version management to check an update. In this case, the DB is the subject and version management is the object.

Need to know is a type of access management to a ressource. For example, a user may have a Top Secret access, he will not be allowed to access all the data at the Top Secret level. He'll be granted to access only the data he is working on. Or the data he *need to know*.

Least Privilege is principle of allowing every module (such as a process, a user, or a program, depending on the subject) to have access only to nothing, except what they are allowed to access. A simple user must not be administrator, a web server should not be started as root.

Access Control are the measures taken to allow only the authorized subject to acess an object. Most of the time, it should allow authorized users and deny non-authorized users (or non-users...). It's one of the most important domain of the CISSP. The Access Control are separated in 3 categories, Administrative, Technical and Physical.

Permission are different from *right* in that permission grant levels of access to a particular object on a file system. Permission to read a file for example.

Right grants users the ability to perform specific actions on a system, such as log in, open the administration panel, etc.

Authentication type

- **Type 1** : Something you know. Password, PIN, birthday, etc.
- **Type 2** : Something you have. Smartcard, ID card, license, etc. Also called transient authentication.
- **Type 3** : Something you are. Fingerprint, retina, face, etc. Also called biometric.

Performance Metrics in Biometrics.

- **Type 1 error** - FRR is in biometrics the probability of type I errors or false non-match rate (FNMR). It's the probability for a valid user to be rejected.

- **Type 2 error** - FAR is in biometrics the probability of type II errors or false match rate (FMR). It's the probability for a non-valid user to be accepted.
- **CER** - CER where the ratio of the FRR and the FAR are equal.

Biometrics Method

- **Retinal scan** - A map of retina's blood vessels.
- **Iris recognition** - A map of the Iris.
- **Fingerprint** - A picture of the fingerprint.
  - Minutiae are the specific plot points on a fingerprint. This includes characteristics such as ridge bifurcation or a ridge ending on a fingerprint.
- **Palm print or structure** - A picture of the palm print of a picture of the structure of the palm.
- **Walk Recognition**
- **Keyboard Typing recognition**
- **Signature recognition**
- **Face recognition**
- **Voice recognition**

Biometric function in two mode :

1. **Verification** (or **Authentication**) mode, the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be.
   For exemple, the user say he is John Doe, the system check he really is John Doe.
2. **Identification** mode, the user didn't say who he is, so the system performs a one-to-many comparison against a biometric database in an attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be".

Throughput, in biometrics term, is the time an authentication took to be completed.

Enrollment, in biometrics term, is the process to register a user in the system, by saving its fingerprint for example.

Cognitive Password is a form of knowledge-based authentication that requires a user to answer a question, presumably something they intrinsically know, to verify their identity. Typical questions are something like "What the name of your first pet", etc.

Oauth 2.0 is an open standard authentication mecanism defined in RFC 6749. Oauth2 is not compatible with OAuth1. It's defined in RFC6749. It's used in the case of site that ask the users to authenticate with gmail or facebook, for example.

Kerberos

Kerberos is an authentication protocol, that function within a realm and use ticket. User authenticate only once, so Kerberos is a SSO system. Kerberos use the UDP port 88 by default. Kerberos also requiere users machines and servers to have a relatively accurate date, because the TGT, the ticket given to an authenticated user by the KDC, are timestamped to avoid replay-attacks.
Kerberos needs to keep the users password in clear.

Each time a client authenticate, a TGT and a session key. The session key is encrypted with the client secret key. When the client needs to access a ressources in the realm, the client decrypt the session key and send it, with the TGT to the TGS. The TGS check in it's base if the users is authorized to access the ressource.

6 - Security Assessment and Testing

Audit

Key elements of an audit report :

- Purpose
- Scope
- Results of the audit

IT staff may perform security assessments to evaluate the security of their systems and applications. Audits must be performed by internal or external auditors who are independent of the IT organization. Criminal investigations must be performed by certified law enforcement personnel.

The frequency of an IT infrastructure security audit or security review is based on risk. The existence of sufficient risk must be establishd to warrant the expense of, and interruption caused by, a security audit on a more or less frequent basis. Asset value and threats are part of risk but are not the whole picture, and assessments are not performed based only on either of these. A high-value asset with a low level of threats doesn’t present a high risk. Similarly, a low-value asset with a high level of threats doesn’t present a high risk. The decision to perform an audit isn’t usually relegated to an administrator, but to the management or security team.

Penetration Testing

1. **Reconnaissance** is collecting all the available data about a target. DNS, IP, address, all published site, etc...

2. **Enumeration** is scanning and trying to have the maximum of informations (web server version, php (for example) version, etc) from everything obtained from the step 1.
3. **Vulnerability Analysis** is searching for a vulnerability from everything obtained on the step 2.
4. **Execution** is using the vulnerability obtained from the step 3.
5. **Reporting** is done by ethical hackers (white hat). After having done the step 1, 2 and 3, they send a report to the target.

- **Blind** testing is giving no information to the pen-tester but inform the company IT team (or other teams) that a test will occur.
- **Double-Blind** testing is giving no information to the pen-tester and don't inform the company's IT team.
- **Targeted** testing give technical information to the pen-tester and inform the company's team about the test.

7 - Security Operations

This is the type of law that must be known to work in the IT Security field :

- **Criminal Law**
  The purpose of these laws is to protect physical integrity of people and the society as a whole. The punishement are Incarceration, Death and Financial, the proof should be "beyond reasonable doubt". Some laws have been designed to protect people and society from crime related to computer :
  - Fourth Amendment protect indivual against unreasonable searches and seizures.
  - **CFAA**, one of the first law (1984) about the computer and network related crimes.
  - **ECPA** of 1986 was enacted by the United States Congress to extend government restrictions on wire taps from telephone calls to include transmissions of electronic data by computer, added new provisions prohibiting access to stored electronic communications. The ECPA has been amended by the CALEA in 1994, the USA PATRIOT Act (2001), the USA PATRIOT reauthorization acts (2006), and the FISA Amendments Act (2008).
  - **USA PATRIOT Act** (2001), In response to the September 11 attacks, Congress swiftly passed legislation to strengthen national security. It expanded the ability of U.S. law enforcementto use electronic monitoring techniques with less judicial oversight. It also amended the **CFAA**.
  - **FISA**, 1977, 2008, regulate the use of electronic surveillance.
  - **FISMA** requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.
  - **ITADA**, (2003) Fraud related to activity in connection with identification documents, authentication features, and information. The statute now makes

the possession of any "means of identification" to "knowingly transfer, possess, or use without lawful authority" a federal crime, alongside unlawful possession of identification documents.

- **DMCA** is a copyright law that criminalizes production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works (commonly known as digital rights management or DRM).
- **GDPR** is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

- **Civil Law**
  These laws are enforced to govern matter between citizens and organizations, ad if the problem is not a crime. Civil can be related to contract, estate, etc. The evidence standard is "Preponderance of the evidence".One of the major difference between criminal and civil law is that criminal law is enforced by the government, but for the civil law, the person or organization must raise the issue.
- **Administrative Law**
  Laws enacted to enforce administrative policies, regulations and procedures.
  - FDA Laws
  - HIPAA was created (1996) primarily to modernize the flow of healthcare information, stipulate how Personally Identifiable Information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and address limitations on healthcare insurance coverage.
  - HITECH (2009) is an act that include new regulation and compliance requirement to the HIPAA act. The HITECH Act requires entities covered by the HIPAA to report data breaches, which affect 500 or more persons, to the United States Department of Health and Human Services (U.S.HHS), to the news media, and to the people affected by the data breaches.
  - FAA Laws
  - FCRA The Fair Credit Reporting Act was one of the first (1968) instances of data protection law passed in the computer age. Purpose of FCRA is that there should be no secret databases that are used to make decisions about a person's life, that individuals should have a right to see and challenge the information held in such databases, and that information in such a database should expire after a reasonable amount of time.
  - GLBA, is a law that protect private data collected by bank and financial institution. It also repealed part of the Glass–Steagall Act of 1933, removing barriers in the market among banking companies, securities companies and insurance companies that prohibited any one institution from acting as any combination of an investment bank, a commercial bank, and an insurance company. With the bipartisan passage of the Gramm–Leach–Bliley Act, commercial banks, investment banks, securities firms, and insurance companies were allowed to consolidate.
  - Privacy Act (1974), a United States federal law, establishes a Code of Fair Information Practice that governs the collection, maintenance, use, and

dissemination of PII about individuals that is maintained in systems of records by federal agencies. It's say that anyone can ask to know the datas every governmental agency have about himself.

- COPPA (1998) applies to the online collection of personal information by persons or entities under U.S. jurisdiction about children under 13 years of age. It details what a website operator must include in a privacy policy, when and how to seek verifiable consent from a parent or guardian, and what responsibilities an operator has to protect children's privacy and safety online including restrictions on the marketing of those under 13.
- FERPA is about the right of the parents to access and amend their child's educational data. It also cover the privacy of the students of 18 years old and more.
- FIPS are publicly announced standards developed by the United States federal government for use in computer systems by non-military government agencies and government contractors.
- SOX Act of 2002 is mandatory. It requiere public traded company to submit to independent audit and to properly disclose financial informations. ALL organizations, large and small, MUST comply. SOX, is a United States federal law that set new or expanded requirements for all U.S. public company boards, management and public accounting firms. The bill, which contains eleven sections, was enacted as a reaction to a number of major corporate and accounting scandals, including Enron and WorldCom. The sections of the bill cover responsibilities of a public corporation's board of directors, adds criminal penalties for certain misconduct, and requires the Securities and Exchange Commission to create regulations to define how public corporations are to comply with the law.
- The Federal Sentencing Guidelines released in 1991 formalized the prudent man rule, which requires senior executives to take personal responsibility for ensuring the due care that ordinary, prudent individuals would exercise in the same situation.
- California Senate Bill 1386 is one of the 1st law about privacy breach notification.

- **Private Regulation**
  These are compliance required by contract.
  - PCI DSS is a standard that company that handle credit card information. The Payment Card Industry Security Standards Council was originally formed by American Express, Discover Financial Services, JCB International, MasterCard and Visa Inc. on 7 September 2006, with the goal of managing the ongoing evolution of the Payment Card Industry Data Security Standard. The council itself claims to be independent of the various card vendors that make up the council.
    PCI DSS allows organizations to choose between performing annual web vulnerability assessment tests or installing a web application firewall.
  - **Downstream liabilities** refers to company's responsibility for damages that result from a security compromise in company's business. For example, if hackers break into company's database and steal the personal information of customers and business partners, company might be held liable for the damage that results.

Evidence

Different type of evidence :

- Real Evidence (also called real evidence or material evidence) are tangible and physical objects, in IT Security: Hard Disks, USB Drives – NOT the data on them. Real evidence must be either uniquely identified by a witness or authenticated through a documented chain of custody.
- Direct Evidence is a testimony from a first hand witness, what they experienced with their 5 senses.
- Circumstantial Evidence Circumstantial evidence is evidence that relies on an inference to connect it to a conclusion of fact—such as a fingerprint at the scene of a crime. By contrast, direct evidence supports the truth of an assertion directly—i.e., without need for any additional evidence or inference.
  On its own, circumstantial evidence allows for more than one explanation.
- Corroborating Evidence is evidence that tends to support a proposition that is already supported by some initial evidence, therefore confirming the proposition.
- Hearsay Evidence is someone saying in court what someone else told him. In certain courts, hearsay evidence is inadmissible unless an exception to the Hearsay Rule applies.
  Computer generated records and with that Log Files were considered hearsay, but case law and updates to the Federal Rule of Evidence have changed that.
- Best Evidence Rule The best evidence rule is a legal principle that holds an original copy of a document as superior evidence. The rule specifies that secondary evidence, such as a copy or facsimile, will be not admissible if an original document exists and can be obtained. The rule has its roots in 18th-century British law.
- Documentary Evidence is any evidence that is, or can be, introduced at a trial in the form of documents, as distinguished from oral testimony. Documentary evidence is most widely understood to refer to writings on paper (such as an invoice, a contract or a will), but the term can also apply to any media by which information can be preserved, such as photographs; a medium that needs a mechanical device to be viewed, such as a tape recording or film; and a printed form of digital evidence, such as emails or spreadsheets.

The five rules of evidence :

- Be Authentic
- Be Accurate
- Be Complete
- Be Convincing
- Be Admissible

To be admissible, evidence must be relevant, material, and competent.

About search warrant :

- To obtain a search warrant, investigators must have probable cause.

- exigent circumstances is a term that describe the seizure of evidence without a warrant. It can happen if there is a probable chance of destruction of evidence.

Electronic Discovery (also e-discovery or ediscovery) refers to discovery in legal proceedings such as litigation, government investigations, or Freedom of Information Act requests, where the information sought is in electronic format (often referred to as electronically stored information or ESI). Electronic discovery is subject to rules of civil procedure and agreed-upon processes, often involving review for privilege and relevance before data are turned over to the requesting party.

Electronic information is considered different from paper information because of its intangible form, volume, transience and persistence. Electronic information is usually accompanied by metadata that is not found in paper documents and that can play an important part as evidence (for example the date and time a document was written could be useful in a copyright case).

The EDRM is a ubiquitous diagram that represents a conceptual view of these stages involved in the e-discovery process.

1. **Identification**
   The identification phase is when potentially responsive documents are identified for further analysis and review. To ensure a complete identification of data sources, data mapping techniques are often employed. Since the scope of data can be overwhelming in this phase, attempts are made to reduce the overall scope during this phase - such as limiting the identification of documents to a certain date range or search term(s) to avoid an overly burdensome request.
2. **Preservation**
   A duty to preserve begins upon the reasonable anticipation of litigation. During preservation, data identified as potentially relevant is placed in a legal hold. This ensures that data cannot be destroyed. Care is taken to ensure this process is defensible, while the end-goal is to reduce the possibility of data spoliation or destruction. Failure to preserve can lead to sanctions. Even if the court ruled the failure to preserve as negligence, they can force the accused to pay fines if the lost data puts the defense "at an undue disadvantage in establishing their defense."
3. **Collection**
   Once documents have been preserved, collection can begin. Collection is the transfer of data from a company to their legal counsel, who will determine relevance and disposition of data. Some companies that deal with frequent litigation have software in place to quickly place legal holds on certain custodians when an event (such as legal notice) is triggered and begin the collection process immediately. Other companies may need to call in a digital forensics expert to prevent the spoliation of data. The size and scale of this collection is determined by the identification phase.
4. **Processing**
   During the processing phase, native files are prepared to be loaded into a document review platform. Often, this phase also involves the extraction of text and metadata from the native files. Various data culling techniques

are employed during this phase, such as deduplication and de-NISTing. Sometimes native files will be converted to a petrified, paper-like format (such as PDF or TIFF) at this stage, to allow for easier redaction and bates-labeling. Modern processing tools can also employ advanced analytic tools to help document review attorneys more accurately identify potentially relevant documents.

5. **Review**
   During the review phase, documents are reviewed for responsiveness to discovery requests and for privilege. Different document review platforms can assist in many tasks related to this process, including the rapid identification of potentially relevant documents, and the culling of documents according to various criteria (such as keyword, date range, etc.). Most review tools also make it easy for large groups of document review attorneys to work on cases, featuring collaborative tools and batches to speed up the review process and eliminate work duplication.
6. **Production**
   Documents are turned over to opposing counsel, based on agreed-upon specifications. Often this production is accompanied by a load file, which is used to load documents into a document review platform. Documents can be produced either as native files, or in a petrified format (such as PDF or TIFF), alongside metadata.

Security Incident Management
The NIST have divided the incident response into the following four steps :

1. Preparation
2. Detection and Analysis
3. Containment, Eradication and Recovery
4. Post-incident Activity

But these steps are usually divided into eight steps to have a better view of the incident management.

1. **Preparation**
   It's what the company or organization have done to train the team and users, to buy the right software, configured the log collector, IDS/IDS, everything that could help to detect and handle the incident. The checklist to handle the incident is also part of the preparation.
2. **Detection**
   Also called identification phase is the most important part of the incident management. The detection phase should include an automated system that check the logs (that should be be centralized in a SIEM). The users's awareness about security is a great point too. Time is an important point.
3. **Response**
   Also called containment is the phase where the team interact with the potential incident. First step is to contain the incident by preventing it to affect others systems.
   Depending of the situation, the response can be to disconnect the network, shutdown the system, isolate the system (by firewalling or just avoiding anyone to work with the affected system). This phase typically

starts with forensically backing up the system involved in the incident. Volatile memory capturing and dumping is also performed in this step before the system is powered off.
Depending of the criticality of the affected systems, the production can be heavily affected or maybe even stopped, it is important to have the management's approval. The response team will have to update the management on the importance of the incident and the estimated time to resolution.

4. **Mitigation**
   During this phase, the incident should be analyzed to find the root cause of the incident. If the root cause is not known, the restoration of the systems may allow the incident to occur again. Once the root cause is known, a way to prevent it to happen again must be applied, the systems can then be restored or rebuild from scratch, to a state where the incident can't occur again. One of the important part of this phase is to prevent this incident to happen on others systems. Changing the firewall rule set or patching the systems are often a solution.
5. **Reporting**
   This phase start at the detection and finish with addition of the incident to the knowledge base of the team. The reporting can take multiple form depending on the public of the communication.
   - For the non-technical people of the organization, a formated mail explaining the problem without very technical problem and most important the estimated time to recovery. If the users have to take action (for example close the mail client), it should be explained (screencapture, etc) so the persons not familiar with computer can do it.
   - For the technical team, the communication should include details, estimated time to recovery and maybe involve the related team in the resolution on the incident. Bridge call may have to be created.

   Depending of the criticality of the incident, the management should be involved in the reporting. If the users have to leave the building quickly for example, the users may not take the request seriously if it come from a not known IT technician.

6. **Recovery**
   During this phase, the system is restored, or reinstalled, rebuild, etc. The business unit responsible of the system only have the ability to decide when the system should go back online or in production. Depending of the actions taken during the mitigation, it's possible an infection persist in the system (if it was not rebuild from scratch or restored but just remove the infection from the system anti-virus for example) so a close monitoring should be applied on the system.
7. **Remediation**
   This phase is done during the mitigation phase. Once the root-cause analysis is over, the vulnerabilities should be mitigated. Remediation start when the mitigation ends. If the vulnerabilities are present in the system's recory image, a recovery image should be generated with the fix applied.

All the system not affected by the incident but vulnerable should be patched, etc. The remediation phase should make the vulnerabilities that have caused the incident to not be able to infect any system in the organization.

8. **Lessons Learned**
   The phase is the most neglected one but it can prevent a lot of incident to happen and accelerate the resolution of similars cases. The incident should be added in a knowledge base, the step taken should be documented, if users or members of the response team needs training, it should be done. The Lessons Learned phase can improve a lot the Preparation phase because if a debriefing is done after each (or each important at least) incident, the team

Configuration Management System

CMS is a systems engineering process for establishing and maintaining consistency of a product's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life.
CMS ca also be used for the following purpose :

- Service Modeling
- Standardization and Compliance
- Incident Resolution
- Change Impact Analysis
- Change Control
- Even Management
- License Management

Configuration Management Process

Configuration Management Process usually involves the three following steps :

1. **Baselining**
2. **Patch Management**
3. **Vulnerability Management**

Change Control / Change Management Process

Change control within information technology (IT) systems is a process—either formal or informal—used to ensure that changes to a product or system are introduced in a controlled and coordinated manner. It reduces the possibility that unnecessary changes will be introduced to a system without forethought, introducing faults into the system or undoing changes made by other users of software.
The goals of a change control procedure usually include :

1. Have all the change reviewed by management
2. Minimal disruption to services

3. Communication for disruption to services
4. Control that the change have a rollback
5. Reduction in back-out activities
6. Cost-effective utilization of resources involved in implementing change

This is the steps included in the Change Management Process.

1. Request the change
2. Review the change
3. Approve/Reject the change
4. Test the change
5. Implement the change
6. Document the change

Request Control process provides an organized framework within which users can request modifications, managers can conduct cost/benefit analysis, and developers can prioritize tasks.

Backup

Difference between following types of backup strategies :

- **Differential** : It copies only those files that have had their data changed since last full backup. This requires more space than incremental backup. Differential backup doesn't clear the archive attribute, so the next differential backup will be larger than the previous one.
- **Incremental** : It takes copies of only those files that have changed since the last full or incremental backup i.e. backup works on incremental basis. This kind of backup strategy takes more time in restoration but is faster at the backup time. Incremental backup clear the archive attribute, so the next incremental backup will not save the same file if they have not change.

Recapitulatif Table :

Backup Strategy	Backup Speed	Restoration Speed	Space taken	Needed for recovery	Clear the backup bit
Full	Slow	Fast	Big	Last Full backup	Yes
Differential	Medium	Medium	Big	Last Full backup + Last differential	No
Incremental	Fast	Slow	Small	Last Full backup + All incremantal since last full backup.	Yes

RAID and is a set of configurations that employ the techniques of striping, mirroring, or parity to create large reliable data stores from multiple general-purpose computer hard disk drives.

- **RAID 0** - Stripping, sending data to two or more disks to increase the write and read speed. For RAID 0, the stripe is done at the block level.

The downside of RAID 0 is if one disk fail in the RAID, the data are lost. The failure rate is multiplied by the number of disks.

- **RAID 1** - Consists of an exact copy (or mirror) of a set of data on two or more disks.
- **RAID 2** - Same as RAID 0, but the stripe is done at the bit level. Rarely implemented because too complex (the disks have to spin at the same speed). As the head and speed need to be synchronized, it can only serve one request at a time.
- **RAID 3** - Same as RAID 2 plus a parity disk. Same as RAID 2, rarely used.
- **RAID 4** - Same as RAID 3 (RAID 2 plus a parity disk) but the striping is done at the block level.
- **RAID 5** - RAID 0 + two parity disk. 2 disk to the data striping + 2 disk for the parity. Minimum number of disk is three.s
  If a striping disk fail, the data can be calculated from the parity disks.
  If a parity disk fail, the data is still present in the striping disks.
- **RAID 6** - RAID 5 + another parity block. Read at the same speed than RAID 5 but write slower.
- **Nested RAID levels**, also known as hybrid RAID, combine two or more of the standard RAID levels.
  RAID 50 is 5+0, combines the straight block-level striping of RAID 0 with the distributed parity of RAID 5

RAID 0 (striping), RAID 1 and its variants (mirroring), RAID 5 (distributed parity), and RAID 6 (dual parity).

Electrical Power is a basic need to operate all the today's business. This is the kind of problem you can encounter with commercial power supply :

- **Blackout** - complete loss of commercial power.
- **Fault** - momentary power outage.
- **Brownout** - an intentional reduction of voltage by a power company.
- **Sag/dip** - a short period of low voltage.
- **Spike** - a sudden rise in voltage in the power supply, during a short period of time.
- **Surge** - a rise in voltage in the power supply, during a long period of time.
- **In-rush current** - the initial surge of current required by a load before it reaches normal operation.
- **Transient** - line noise or disturbance is superimposed on the supply circuit and can cause fluctuations in electrical power.

Noise can occur on a cable :

- **Transverse Mode** happen when there is high charge difference between hot and neutral.
- **EMI** and **RFI** are caused by others electrical device, light source (fluo most of the time), electrical cable, etc.
-

You can mitigate the risk by installing a UPS. UPS have a limited power and can send power to the systems for a short period of time. To be able to have power for days, a diesel generator is needed.

Open Source Intelligence is the gathering of information from any publicly available resource. This includes websites, social networks, discussion forums, file services, public databases, and other online sources. This also includes non-Internet sources, such as libraries and periodicals.

DRP - BCP

DRP is focused on IT and it's part of BCP.
There is 5 methods to test a DRP :

1. Read-through, where all the involved people read the plan. It help find inconsistency, errors, etc.
2. Structure walk-through (also known as table-top exercise) where all the involves person role play their part, by read the DRP, following a scenario.
3. Simulation test is when the team are asked to give a response to a virtual disaster. The response is then tested to check if it's valid.
4. Parallele test is where the DRP is tested for real. If there is a second site, it is activated, etc. The parallele test should never impact production.
5. Full interuption test is when the production is shutdown to test the DRP. It's rarely done due to the heavy impact on production.

Type of DR site :

- **Redundant site** is in the exact same status as the production site and a mecanism will activate a failover to send the traffic to the redundant site. A failure on the production site should be invisible.
- **Hot site** is a mirror site of the current production site. It should be up in 3 hours after an event.
- **Warm site** has everything needed in term of hardware to run the production, but the data are not up to date. Sometime, the telecom line are not ready too. It can take up to 3 days for a warm site to be up.
- **Cold site** is the least expensive. It's just an empty site with no hardware nor data.
- **Reciprocal agreement** is when you agree with another company to host each others if a problem happen. It raise some concern (distance, data confidentiality, etc...)
- **Mobile site** are "datacenters on wheels", trucks with data and hardware ready to leave a site if a disaster is announced.

Business Continuity Planning

BCP is the process of ensuring the continuous operation of your business before, during, and after a disaster event. The focus of BCP is totally on business continuation and it ensures that all services that the business provides or critical functions that the business performs are still carried out in the wake of the disaster.

BCP should be reviewed each year or when significant change occur.
BCP have multiple steps :

1. **Project initiation** is the phase where the scope of the project must be defined.
   - Develop a BCP policy statement.
   - The BCP project manager must be named, he'll be in charge of the business continuity planning and must test it periodically.
   - The BCP team and the CPPT should be constitued too.
   - It is also very important to have the top-management approval and support.
   - **Scope** is the step where which assets and which kind of emergency event are included in the BCP. Each services of the company must be involved in this steps to ensure no critical assets are missed.
2. **BIA** differentiates critical (urgent) and non-essential (non-urgent) organization functions/activities. A function may be considered critical if dictated by law. It also aims to quantify the possible damage that can be done to the system components by disaster.
   The primary goal of BIA is to calculate the MTD for each IT asset.
   Other benefits of BIA include improvements in business processes and procedures, as it will highlight inefficiencies in these areas.
   The main components of BIA are as follows:
   - Identify critical assets
     - At some point, a **vital records program** needs to be create. This document indicate where are located the business criticals records and the procedures to backup and restore them.
   - Conduct risk assessment
   - Determine MTD
   - Failure and recovery metrics
3. **Identify preventive control**
4. **Recovery strategy**
   - Create a high-level recovery strategy.
   - The systems and service identified in the BIA should be prioritized.
   - The recovery strategy must be agreed by executive management.
5. **Designing and development, IT contingency Plan**
   - It's the step where the DRP is designed. A list of detailed procedure to for restoring the IT must be produced at this stage.
6. **Implementation of DRP, training, and testing**
7. **BCP/DRP maintenance**

Or in short :

1. Develop a BCP policy statement
2. Conduct a BIA
3. Identify preventive controls
4. Develop recovery strategies

5. Develop an IT contingency plan
6. Perform DRP training and testinf
7. Perform BCP/DRP maintenance

Misc

Type 1 Hypervisor are VM hypervisor wheere the OS is installed directly on the barebone machine. They perform better.
Type 2 Hypervisor are application installed in an OS, like Linux or Windows. They are called hosted hypervisor, they perform slower than type 1 hypervisor because the OS have to translate each call.

Tripwire is a HIDS.

NIPS is like an IDS, but it's installed inline in the netwwork. It can modify network packets or block attack.

IACIS is a non-profit, all-volunteer organization of digital forensic professionals. The CFCE credential was the first certification demonstrating competency in computer forensics in relation to Windows based computers.

CFTT is a project created by the NIST, to test and certifiate forensics equipements.

Software Escrow Agreement allow the customer to have access to the source code of a software if the vendor is stop the support of an application or is out of business.

8 - Software Development Security

Nonfunctional Requirements define system attributes such as security, reliability, performance, maintainability, scalability, and usability.

Life cycle of a project using a 5 phases SDLC :

1. Initiation
   In this first phase, problems are identified and a plan is created.
2. Acquisition and development
   Once developers reach an understanding of the end user’s requirements, the actual product must be developed.
3. Implementation
   In this phase, physical design of the system takes place. The Implementation phase is broad, encompassing efforts by both designers and end users.
4. Operations and maintenance
   Once a system is delivered and goes live, it requires continual monitoring and updating to ensure it remains relevant and useful.
5. Disposition
   This phase represents the end of the cycle, when the system in question is no longer useful, needed or relevant.

This is a more detailed SDLC, containing 13 phases :

1. **Preliminary analysis**: Begin with a preliminary analysis, propose alternative solutions, describe costs and benefits, and submit a preliminary plan with recommendations.
    1. Conduct the preliminary analysis: Discover the organization's objectives and the nature and scope of the problem under study. Even if a problem refers only to a small segment of the organization itself, find out what the objectives of the organization itself are. Then see how the problem being studied fits in with them.
    2. Propose alternative solutions: After digging into the organization's objectives and specific problems, several solutions may have been discovered. However, alternate proposals may still come from interviewing employees, clients, suppliers, and/or consultants. Insight may also be gained by researching what competitors are doing.
    3. Cost benefit analysis: Analyze and describe the costs and benefits of implementing the proposed changes. In the end, the ultimate decision on whether to leave the system as is, improve it, or develop a new system will be guided by this and the rest of the preliminary analysis data.
2. **Systems analysis**, **requirements** definition: Define project goals into defined functions and operations of the intended application. This involves the process of gathering and interpreting facts, diagnosing problems, and recommending improvements to the system. Project goals will be further aided by analysis of end-user information needs and the removal of any inconsistencies and incompleteness in these requirements. Due Care should be done in this phase.
   A series of steps followed by the developer include:
    1. **Collection of facts**: Obtain end user requirements through documentation, client interviews, observation, and questionnaires.
    2. **Scrutiny of the existing system**: Identify pros and cons of the current system in-place, so as to carry forward the pros and avoid the cons in the new system.
    3. **Analysis of the proposed system**: Find solutions to the shortcomings described in step two and prepare the specifications using any specific user proposals.
3. **Systems design**: At this step desired features and operations are described in detail, including screen layouts, business rules, process diagrams, pseudocode, and other documentation.
4. **Development**: The real code is written here.
5. **Documentation and common program control**:The way data are handled in the system, or the log are generated, etc are documented.
6. **Integration and testing**: All the pieces are brought together into a special testing environment, then checked for errors, bugs, and interoperability.

7. **Acceptance**: The system is tested by a third party. The testing include functionality test and security test.
8. **Testing and evaluation controls**:Create guideline to determine how the system can be tested.
9. **Certification**: The system is compared to a functional security standards to ensure the system complies with those standards.
10. **Accreditation**: The system is approved for implementation. A certified system might not be accredited and an accredited system might not be certified.
11. **installation, deployment, Implementation**: This is the final stage of initial development, where the software is put into production and runs actual business.
12. **Maintenance**: During the maintenance stage of the SDLC, the system is assessed/evaluated to ensure it does not become obsolete. This is also where changes are made to initial software.
13. **Disposal**: In this phase, plans are developed for discontinuing the use of system information, hardware, and software and making the transition to a new system. The purpose here is to properly move, archive, discard, or destroy information, hardware, and software that is being replaced, in a manner that prevents any possibility of unauthorized disclosure of sensitive data. The disposal activities ensure proper migration to a new system. Particular emphasis is given to proper preservation and archiving of data processed by the previous system. All of this should be done in accordance with the organization's security requirements.

Not every project will require that the phases be sequentially executed. However, the phases are interdependent. Depending upon the size and complexity of the project, phases may be combined or may overlap.

The programing language have been classified by generation. WP

1. First-generation language
   It's made of one and zero.
2. Second Generation language
   It's the assembly. The language is specific to a particular processor family and environment.
3. Third Generation language
   These languages includes features like improved support for aggregate data types, and expressing concepts in a way that favors the programmer, not the computer. A third generation language improves over a second generation language by having the computer take care of non-essential details. It's also using a compiler to translate the human readable code to a machine code. Sometime a runtime VM is used, like for C# and java. Fortran, ALGOL, COBOL, C, C++, C#, Java, BASIC and Pascal are 3rd generation language.
4. Fourth Generation language
   This generation is for language that are done for a specific set of problem or task. Mathlab is made to work in the mathematic field. The different

flavor of SQL are done to interact with DataBase. XQuery is made for XML.

5. Fifth Generation language
   While fourth-generation programming languages are designed to build specific programs, fifth-generation languages are designed to make the computer solve a given problem without the programmer. Fifth-generation languages are used mainly in artificial intelligence research.
   OPS5 and Mercury are examples of fifth-generation languages.

In software engineering, coupling is the degree of interdependence between software modules (if a module (or an object) depend heavily on another module/object. Low coupling mean changing something in a class will not affect other class.); a measure of how closely connected two routines or modules are; the strength of the relationships between modules. Coupling is usually contrasted with cohesion (if an object/module implement a lot of unrelated functions. High cohesion mean an object/module implement only related functions) Low coupling often correlates with high cohesion, and vice versa.

Consistency in database systems refers to the requirement that any given database transaction must change affected data only in allowed ways. Any data written to the database must be valid according to all defined rules, including constraints, cascades, triggers, and any combination thereof.
Cardinality refers to the uniqueness of data values contained in a particular column (attribute) of a database table. The lower the cardinality, the more duplicated elements in a column. For example, ID should be unique, so ID have a high cardinality. A column Gender can only accept Male or Female have a low cardinality.
Durability indicate that once a transaction is committed, it's permanently, it'll survive any crash or poweroff of the DB's host. The transaction is written to the disk and in the transaction log. For example, in a garage's DB, if the system indicate to the buyer that he successfully buy a car, the car will remain bought by the owner even if the DB encounter a power outage.
Data Dictionary is a data structure that stores metadata, i.e., (structured) data about information. If a data dictionary system is used only by the designers, users, and administrators and not by the DBMS Software, it is called a passive data dictionary. Otherwise, it is called an active data dictionary or data dictionary.

Test Coverage is a measure used to describe the degree to which the source code of a program is executed when a particular test suite runs. A program with high test coverage, measured as a percentage, has had more of its source code executed during testing, which suggests it has a lower chance of containing undetected software bugs compared to a program with low test coverage. To calculate the test coverage, the formula is *Number of use cases tested / Total number of use cases* . For example, a program with 100 use cases that have 80 use cases tested : 80 / 100 : 0.8 . multiplie it by 100 to obtain the % . 80% in our case.

Negative Testing is a method of testing an application or system that ensures that the plot of the application is according to the requirements and can handle the unwanted input and user behavior. Invalid data is inserted to compare the output against the given input. Negative testing is also known as failure testing or error path testing.

Boundary test are done during negative testing, it consist of send 101 for example to an entry that requiere a number between 0 and 100. When performing negative testing exceptions are expected. This shows that the application is able to handle improper user behavior. Users input values that do not work in the system to test its ability to handle incorrect values or system failure.

CRUD testing Create, Read, Update, and Delete (CRUD) are the four basic functions of persistent storage. CRUD testing is used o validate the CRUD is functioning.

Heap Metadata Prevention is a memory protection that force a process to fail if a pointer is freed incorectly.

Pointer Encoding is a buffer overflow protection recommended by Microsoft during Software Development Lifecycle for Independent Software Vendor, but it's not Required.

Buffer Overflow and pointer protection according for Independent Software Vendor recommendations from Microsoft SDL

Name	Requiement	Priority
Pointer Encoding	No	Moderate
ASLR	Yes	Critical
Heap Metadata Protection	Yes	Moderate
DEP	Yes	Critical

Hardware Segmentation is a memory protection that maps process in different hardware memory location.

Defect Density is a development that determine the average number of defect per line of code.

Risk Density is a secure development metric that determine that rank security issues in order to quantify risk.

Inference is the ability to deduce sensitive information from available non-sensitive informations. For example deducing patient's illness based on that patient's prescription.

Aggregation is combining benign data to reveal potential sensible information.

Software Development Methodologies

- **Agile** Software Development method is an approach to software development under which requirements and solutions evolve through the collaborative effort of self-organizing and cross-functional teams and their customers/end users. Most agile development methods break product development work into small increments that minimize the amount of up-front planning and design.

Iterations, or sprints, are short time frames (timeboxes) that typically last from one to four weeks. Each iteration involves a cross-functional team working in all functions: planning, analysis, design, coding, unit testing, and acceptance testing. At the end of the iteration a working product is demonstrated to stakeholders.
This minimizes overall risk and allows the product to adapt to changes quickly. An iteration might not add enough functionality to warrant a market release, but the goal is to have an available release (with minimal bugs) at the end of each iteration.Multiple iterations might be required to release a product or new features.
Working software is the primary measure of progress.

- **CMM** is a development model created after a study of data collected from organizations that contracted with the U.S. Department of Defense, who funded the research. The term "maturity" relates to the degree of formality and optimization of processes, from ad hoc practices, to formally defined steps, to managed result metrics, to active optimization of the processes.

  The model's aim is to improve existing software development processes, but it can also be applied to other processes.
  There is five maturity levels :

  1. **Initial** : It is characteristic of processes at this level that they are (typically) undocumented and in a state of dynamic change, tending to be driven in an ad hoc, uncontrolled and reactive manner by users or events. This provides a chaotic or unstable environment for the processes. (Example - a surgeon performing a new operation a small number of times - the levels of negative outcome are not known).
  2. **Repeatable** : It is characteristic of this level of maturity that some processes are repeatable, possibly with consistent results. Process discipline is unlikely to be rigorous, but where it exists it may help to ensure that existing processes are maintained during times of stress.
  3. **Defined** : It is characteristic of processes at this level that there are sets of defined and documented standard processes established and subject to some degree of improvement over time. These standard processes are in place. The processes may not have been systematically or repeatedly used - sufficient for the users to become competent or the process to be validated in a range of situations.
  4. **Managed** : It is characteristic of processes at this level that, using process metrics, effective achievement of the process objectives can be evidenced across a range of operational conditions. The suitability of the process in multiple environments has been tested and the process refined and adapted. Process users have experienced the process in multiple and varied conditions, and are able to demonstrate competence. The process maturity enables adaptions to particular projects without measurable losses of quality or deviations from specifications.
  5. **Optimizing** : It is a characteristic of processes at this level that the focus is on continually improving process performance through both incremental and innovative technological changes/improvements.
     At maturity level 5, processes are concerned with addressing

statistical common causes of process variation and changing the process (for example, to shift the mean of the process performance) to improve process performance. This would be done at the same time as maintaining the likelihood of achieving the established quantitative process-improvement objectives. There are only a few companies in the world that have attained this level 5.

In short :

6. **Initial** : It's chaos. Personels is reating to events/requests.
7. **Repeatable** : Personels have already encountered the events/requests and are able to repeat action/unwritten process.
8. **Defined** : Some documentations and Standards are in place.
9. **Managed** : The company/organization have metrics about the process. Personels are trained and experienced.
10. **Optimized** : Company/Organization management is constantly working on improving the process.

- **CPA** or Critical Path Method (CPM) is an algorithm for scheduling a set of project activities. It is commonly used in conjunction with the program evaluation and review technique (PERT). A critical path is determined by identifying the longest stretch of dependent activities and measuring the time required to complete them from start to finish.
  Critical Path Analysis is commonly used with all forms of projects, including construction, aerospace and defense, software development, research projects, product development, engineering, and plant maintenance, among others. Any project with interdependent activities can apply this method of mathematical analysis. The first time CPM was used for major skyscraper development was in 1966 while constructing the former World Trade Center Twin Towers in New York City. Although the original CPM program and approach is no longer used, the term is generally applied to any approach used to analyze a project network logic diagram.
- **Waterfall Model** is the oldest and most common model used for SDLC methodology. It works on the principal of finishing one phase and then moving on to the next one. Every stage builds up on information collected from the previous phase and has a separate project plan. Though it is easy to manage, delays in one phase can affect the whole project timeline. Moreover, once a phase is completed, there is little room for amendments until the project reaches the maintenance phase.
  The phases :
  1. Requirement
  2. Design
  3. Implementation
  4. Verification
  5. Maintenance
- Spiral Model The spiral model is a risk-driven software development process model. Based on the unique risk patterns of a given project, the spiral model guides a team to adopt elements of one or more process models, such as incremental, waterfall, or evolutionary prototyping.

- **IDEAL**
    1. **I**NITIATION phase in which management support is obtained for process improvement, the objectives and constraints of the process improvement effort are defined, and the resources and plans for the next phase are obtained.
    2. **D**IAGNOSIS, identifies the appropriate appraisal method (such as CMM-based), identifies the project(s) to be appraised, trains the appraisal team, conducts the appraisal, and briefs management and the organization on the appraisal results.
    3. **E**STABLISHMENT, an action plan is developed based on the results of Phase 2, management is briefed on the action plan, and the resources and group(s) are coordinated to implement the action plan.
    4. **A**CTION phase, in which resources are recruited for implementation of the action plan, the action plan is implemented, the improvement effort is measured, and the plan and implementation are modified based on measurements and feedback.
    5. **L**EVERAGE phase, which ensures that all success criteria have been achieved, all feedback is evaluated, the lessons learned are analyzed, the business plan and process improvement are compared for the desired outcome, and the next stage of the process improvement effort is planned.
-

Processor Mode

Processor have different mode of execution.

- **Ring 0** : Kernel/Supervisor/Priviliged is the mode used to execute code that have complete access to the hardware. It's normally reserved to the OS functions.
- **Ring 3** : Users/Applications mode, is used to run applications.

Misc

Data Warehouse is the process of collecting large volume of data on a high performance storage.
Data Mining is the process of searching large volume of data for patterns.

Index

Write a JS function that will point to the place where the string match

- **AAA** : Authentication, Authorization, Accounting is used to refer to a family of protocols that mediate network access. Two network protocols providing this functionality are particularly popular: RADIUS protocol and Diameter. WP
- **ABAC** : Attribute Based Access Control also known as Policy-based access control, defines an access control paradigm whereby access rights are granted to users through the use of policies which combine attributes together. WP

- **Accountability** : In ethics and governance, accountability is answerability, blameworthiness, liability, and the expectation of account-giving. In IT, it can be achieved by a strong identification and authentication system, a non-modifiable log system to obtain non-repudiation. WP
- **ACM** : Access Control Matrix is a way of representing the right a set of subjects have on a set of objects. It's represented in an table.WP
- **AES** : Advanced Encryption Standard, is a specification for the encryption of electronic data established by the NIST in 2001. Discussed in domain 3. WP
- **AFH** : Adaptating Frequence Hoping is the FHSS method used in Bluetooth.
- **ALE** : Annualized Loss Excpectancy is third and final step of the quantitative assessment seeks to combine the potential loss and rate per year to determine the magnitude of the risk.WP
- **AV** : Asset Value, is the cost in dollar of an asset. Discussed in Chapter 1.
- **AH** : Authentication Header is a member of the IPsec protocol suite. WP
- **APIPA** : Automatic Private IP Addressing is protocol to get an IP when there is no DHCP. It automatically choose an IP in the range 169.254.1.0 to 169.254.254.255. WP
- **ARO** : Anualized Rate of Occurance is an estimate of how often a threat would be successful in exploiting a vulnerability.
- **ARP** : Address Resolution Protocol is used to resolve IP addresses to MAC addresses.
- **ASLR** : Adress Space Layout Randomization increase security of an OS or a software by randomizing the address space positions of key data areas of a process. WP
- **ATM** : Asynchronous Transfer Mode is a standard for carriage of traffic. It use fixed-size packets. WP
- **BCP** : Business Continuity Planning is the process of creating systems of prevention and recovery to deal with potential threats to a company. WP
- **BIA** : Business Impact Analysis differentiates critical (urgent) and non-critical (non-urgent) organization functions/activities. WP
- **BRP** : Business Recovery Planning, a subset of DRP, focus on returning to normal business after recovering from a disaster.
- **BYOD** : Bring Your Own Device is a policy that allow users to connect their own device to the company's network. WP
- **CALEA** : Communications Assistance for Law Enforcement Act, under B.Clinton, 1994. CALEA's purpose is to enhance the ability of law enforcement agencies to conduct lawful interception of communication by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have built-in capabilities for targeted surveillance . WP
- **CAPTCHA** : Completely Automated Turing test to tell Computer and Human Appart. WP
- **CBC** : Cipher Block Chaining mode employs an IV and chaining to destroy cipher text patterns. Because CBC works in block mode, it decrypt message one block at a time. WP
- **CCTA** : Central Computer and Telecommunication Agency, the UK's agency that created ITIL. WP

- **CC** : Common Criteria is an international standard (ISO/IEC 15408) for computer security certification. WP
- **CCMP** : Counter Mode Cipher Block Chaining Message Authentication Code Protocol is an encryption protocol designed for Wireless LAN products that implements the standards of the IEEE 802.11i amendment to the original IEEE 802.11 standard. CCMP is a cryptographic encapsulation mechanism based upon the Counter Mode with CBC-MAC of the Advanced Encryption Standard (AES) standard. It was created to address the vulnerabilities presented by Wired Equivalent Privacy (WEP), a dated, insecure protocol. WP
- **CCTV** : Closed Circuit Television. WP
- **CER** : Crossover Error Rate is where the ratio of the FRR and the FAR are equal. WP
- **CFAA** : Computer Fraud and Abuse Act is a bill enacted in 1984. The CFAA prohibits the access to a system without authorization. Before this law, the computer or network related crime was prosecuted as mails and wire fraud.WP
- **CFCE** : Certified Forensic Computer Examiner is a certification in computer forensic. WP
- **CFB** : Cipher FeedBack, is a block cipher mode, using a memory buffer to have same size block. It's retired due to the wait in encoding each block. The Cipher Feedback (CFB) mode, a close relative of CBC, makes a block cipher into a self-synchronizing stream cipher. WP
- **CFTT** : Computer Forensics Tool Testing is a project at the NIST is to establish a methodology for testing computer forensic software tools by development of general tool specifications, test procedures, test criteria, test sets, and test hardware. NIST
- **CHAP** : Challenge Handshake Authentication Protocol is used to authenticate a user or network host to an authenticating entity. That entity may be, for example, an Internet service provider. WP
- **CISSP** : Certified Information System Security Professional. WP
- **CMDB** : Configuration Management DataBase
- **CMM** : Capability Maturity Model WP
- **CMS** : Configuration Management System is a systems engineering process for establishing and maintaining consistency of a product's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life. WP
- **Cognitive Password** : is a form of knowledge-based authentication that requires a user to answer a question, presumably something they intrinsically know, to verify their identity. Typical questions are something like "What the name of your first pet", etc.WP
- **COOP** : Continuity Of Operation Plan focus on maintenaning the business during a disaster.
- **COPPA** : Children's Online Privacy Protection Act of 1998 is a law about the privacy of children under the age of 13. WP
- **COBIT** : Control Objectives for Intormation and Related Technologies is a good-practice framework created by international professional association ISACA for information technology management and IT governance. WP

- **Covert Channel** : In computer security, a covert channel is a type of attack that creates a capability to transfer information objects between processes that are not supposed to be allowed to communicate by the computer security policy.
- **CPA** : Critical Path Analysis (or sometime Critica Path Method (CPM)) is an algorithm for scheduling a set of project activities. It is commonly used in conjunction with the program evaluation and review technique (PERT).WP
- **CPPT** : Continuity Planning Project Team should represent all the stakeholders in the organization, such as HR, the IT department, the physical security department, public relations, and all other personnel responsible for effective business.
- **CRL** : Certificate Revocation List is "a list of digital certificates that have been revoked by the issuing certificate authority (CA) before their scheduled expiration date and should no longer be trusted". WP
- **CSMA/CA** : Carrier Sense Multiple Access with Collision Avoidance is used by WiFi 802.11.WP
- **CSMA/CD** : Carrier Sense Multiple Access with Collision Detection is used by Ethernet. WP
- **CTR** : Counter is a DES stream cipher mode, where it use a 64bits counter for feedback. It doesn't propagate error. WP
- **CVE** : Common vulnerabilities and Exposures system provides a reference-method for publicly known information-security vulnerabilities and exposures. The Mitre Corporation, maintains the system, with funding from the National Cyber Security Division of the United States Department of Homeland Security. WP
- **CVSS** : Common Vulnerabilities Scoring System is a free and open industry standard for assessing the severity of computer system security vulnerabilities. WP
- **CYOD** : Choose Your Own Device is a business trend and phenomenon designed to give an organization more control of devices that employees use to handle company data. With CYOD, an organization allows employees to select from specified devices for business usage. External
- **DAC** : Discretionary Access Control is an Access Control system that rely on the fact that object can be access regardbing subject/group to which they belong.WP
- **DCCP** : Datagram Congestion Control Protocol
- **DCE** : Data Circuit-terminating Equipment is a device that sits between the data terminal equipment (DTE) and a data transmission circuit. It is also called data communication(s) equipment and data carrier equipment. Usually, the DTE device is the terminal (or computer), and the DCE is a modem. WP
- **DDOS** : Distributed Deny Of Service attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. WP
- **DES** : Data Encryption Standard is a symmetric-key algorithm for the encryption of electronic data. WP
- **Diffie Hellman** : is a method of securely exchanging cryptographic keys over a public channel. WP

- **DMCA** : Digital Millennium Copyright Act, is a 1998 United States copyright law that implements two 1996 treaties of the World Intellectual Property Organization (WIPO). It criminalizes production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works (commonly known as digital rights management or DRM).WP
- **DREAD** : Damage, Reproductibility, Exploitability, Affected used, Discoverability, is part of a system for risk-assessing computer security threats previously used at Microsoft and although currently used by OpenStack and other corporations. It was abandoned by its creators.WP
- **DRM** : Digital Right ManagementWP
- **DRP** : Disaster Recovery Plan is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster. WP
- **DSA** : Digital Signature Algorithm, is a FIPS for digital signatures. WP
- **DSS** : Digital Signature Standard is a FIPS specifying a suite of algorithms that can be used to generate digital signatures established by the NIST. WP
- **DTE** : Data Terminal Equipment is an end instrument that converts user information into signals or reconverts received signals. These can also be called tail circuits. Usually, the DTE device is the terminal (or computer), and the DCE is a modem. WP
- **EAL** : Evaluation Assurance Level in the CC, is the rating level assign to the Target Of Evaluation. WP
- **ECB** : Electronic Code Book, is an encryption mode, use by DES for exemple. The disadvantage of this method is a lack of diffusion. Because ECB encrypts identical plaintext blocks into identical ciphertext blocks, it does not hide data patterns well. In some senses, it doesn't provide serious message confidentiality, and it is not recommended for use in cryptographic protocols at all. WP
- **ECDSA** : Elliptic Curve Digital Signature Algorithm is an implementation of DSA that use elliptic curve. WP
- : Electronic Communications Privacy Act is law enacted in 1986 to extend restriction to wiretape.WP
- **EDRM** : Electronic Discovery Reference Model is a ubiquitous diagram that represents a conceptual view of these stages involved in the e-discovery process. Electronic discovery (also e-discovery or ediscovery) refers to discovery in legal proceedings such as litigation, government investigations, or Freedom of Information Act requests, where the information sought is in electronic format (often referred to as electronically stored information or ESI). WP
- **EF** : Exposure Factor, is the subjective, potential percentage (some time noted as 0.8 for 80%) of loss to a specific asset if a specific threat is realized. Discussed in Chapter 1.WP
- **EMI** : Electromagnetic Interference also called RFI when in the radio frequency spectrum, is a disturbance generated by an external source that affects an electrical circuit by electromagnetic induction, electrostatic coupling, or conduction. WP
- **ESP** : Encapsulating Security Payload is a member of the IPsec protocol suite. WP

- **E0** is a stream cipher used in the Bluetooth protocol. It generates a sequence of pseudorandom numbers and combines it with the data using the XOR operator. The key length may vary, but is generally 128 bits. It's a weak cipher.WP
- **E2EE** : End to End Encryption is a system of communication where only the communicating users can read the messages. WP
- **FAR** : False Accept Rate is in biometrics the probability of type II errors or false match rate (FMR).WP
- **FCRA** : Fair Credit Reporting Act was one of the first instances of data protection law passed in the computer age. Key among these innovations was the determination that there should be no secret databases that are used to make decisions about a person's life. WP
- **FEMA** : Federal Emergency Management Agency have for purpose to coordinate the response to a disaster that has occurred in the United States and that overwhelms the resources of local and state authorities. The governor of the state in which the disaster occurs must declare a state of emergency and formally request from the president that FEMA and the federal government respond to the disaster. WP
- **FERPA** : Family Educational Right and Privacy Act cover the right for parents to have access to their child's education data.WP
- **FHSS** : Frequency Hopping Spread Spectrum is a method of changing frequency during a communication, using a sequence known only from the authorized device/person. Bluetooth do it through AFH. WP
- **FIPS** : Federal Information Processing Standards are publicly announced standards developed by the United States federal government for use in computer systems by non-military government agencies and government contractors. FIPS publications do not apply to national security systems (as defined in FISMA). FIPS publications may be adopted and used by non-federal government organizations and private sector organizations. WP
- **FISA** : Foreign Intelligence Surveillance Act, regulate the use of electronic surveillance.WP
- **FISMA** : Federal Information Security Management Act. A 2002 Act. The act recognized the importance of information security to the economic and national security interests of the United States. WP
- **FM200** is a gas used in datacenter to to remove fire without destroying the equipment. WP
- **Fraggle Attack** : is a DDOS based on UDP and target's IP spoofing.WP
- **Frame Relay** : is a standardized technology that specifies the physical and data link layers of digital telecommunications channels using a packet switching methodology. WP
- **FRR** : False Reject Rate is in biometrics the probability of type I errors or false non-match rate (FNMR)WP
- **GDPR** : General Data Protection Regulation is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). WP
- **GLBA** : Gramm–Leach–Bliley Act repealed part of the Glass–Steagall Act of 1933, removing barriers in the market among banking companies, securities companies and insurance companies that prohibited any one institution from acting as any combination of an investment bank, a commercial bank, and an

insurance company. With the bipartisan passage of the Gramm–Leach–Bliley Act, commercial banks, investment banks, securities firms, and insurance companies were allowed to consolidate. WP

- **HIDS** : Host-based Intrusion Detection System is an IDS installed on a host. WP
- **HIPAA** : Health Insurance Portability and Accountability Act was created primarily to modernize the flow of healthcare information, stipulate how Personally Identifiable Information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and address limitations on healthcare insurance coverage. WP
- **HITECH** : Health Information Technology for Economic and Technical Health is an act that include new regulation and compliance requirement to the HIPAA act. WP
- **HMAC** : Hash-based Message Authentication Code is a hashing method with a password. WP
- **HTTP** : HyperText Transfer Protocol, OSI layer 7 protocol
- **IACIS** : International Association of Computer Investigative Specialists has been providing computer Forensic Training for over 27 years. WP
- **HVAC** : Heating, Ventilation and Air Conditioning. WP
- **IaaS** : Infrastructure as a Service, is when a provider allow customer to install VM, manage network, etc. WP
- **IANA** : Internet Assigned Number Authority is a function of ICANN, a nonprofit private American corporation that oversees global IP address allocation, autonomous system number allocation, root zone management in the Domain Name System (DNS), media types, and other Internet Protocol-related symbols and Internet numbers. WP
- **IDEAL** : Initial Diagnose Establish Action Leverage
- **IDS** : Intrusion Detection System. WP
- **IEEE** : Institute of Electrical and Electronic Engineers. WP
- **IEEE 802** : Institute of Electrical and Electronic Engineers 802 is a family of IEEE standards dealing with local area networks and metropolitan area networks. WP
- **IEEE 802.11** : **IEEE802**.11 is part of the IEEE 802 set of LAN protocols, and specifies the set of media access control (MAC) and physical layer (PHY) protocols for implementing WLAN, Wi-Fi. WP
- **IEEE 802.15** : Bluetooth. WP
- **IKE** : Internet Key Exchange is the protocol used to set up a security association (SA) in the IPsec protocol suite. WP
- **IPComp** : IP Payload Compression Protocolis is a low level compression protocol for IP datagrams. WP
- **IPS** : Intrusion Prevention System. WP
- **IPsec** : IP Security is a secure network protocol suite that authenticates and encrypts the packets of data sent over an internet protocol network. WP
- **ISA** : Interconnect Security Agreement. WP
- **ITADA** : Fraud related to activity in connection with identification documents, authentication features, and information"). The statute now makes the possession of any "means of identification" to "knowingly transfer, possess, or use without lawful authority" a federal crime, alongside unlawful possession of identification documents.

- **ITIL** : Information Technology Infrastructure Library is a set of detailed practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business. It was created in the 1980s by CCTA from a request from the UK gov.WP
- **ITSEC** : Information Technology Security Evaluation Criteria, is a structured set of criteria for evaluating computer security within products and systems. The ITSEC was first published in May 1990 in France, Germany, the Netherlands, and the United Kingdom based on existing work in their respective countries.WP
- **ITU** : International Telecommunication Union is a specialized agency of the United Nations (UN) that is responsible for issues that concern information and communication technologies.WP
- **ISACA** : Information System Audit and Control Association is an international professional association focused on IT governance. It created COBIT. WP
- **ISAKMP** : Internet Security Association and Key Management Protocol is a protocol defined by RFC 2408 for establishing Security Associations (SA) and cryptographic keys in an Internet environment. WP
- **(ISC)²** : International Information Systems Security Certification Consortium, a non-profit group with the primary goal to provide training and certifications in the IT Security field. www.isc2.orgWP
- **ITAM** : IT Asset Management introduces financial aspects of the asset – cost, value and contractual status. ITAM also refers to full lifecycle management of the asset. ITAM is designed to manage the physical, contractual and financial aspects of the asset. WP
- **IV** : Initialization vector. WP
- **KDC** : Key Distrition Cented are authentication server in a Kerberos network. WP
- **L2TP** : Layer 2 Tunneling Protocol is a Layer 2 tunneling protocol used to support VPNs or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy. WP
- **LCP** : Link Control Protocol, forms part of the PPP, within the family of Internet protocols. In setting up PPP communications, both the sending and receiving devices send out LCP packets to determine the standards of the ensuing data transmission. WP
- **LLC** : Logical Link Control is a layer 2 protocol that allow multiple protocols on the same network medium. It's 802.2. WP
- **MAC** : Mandatory Access Control is an Access Control system based on data classification and labels. The famous Top Secret come from here.WP
- **MD5** : Message Digest 5, a hashing algorithm producing 128 bits output. WP
- **MIC** : Message Integrity Check is an integrity control used in WPA.
- **MTD** : Maximum Tolerable Downtime is the longest period of time a resource can be unavailable without causing irreparable harm to the business. WP
- **NAC** : Network Access Control is a technology that allow access to the network only if the device fill the requierement (OS version, AV up to date, etc). If a device fail these requierement, a page displaying a allowing to resolve the issue may be displayed.WP

- **NAT-PT** : Network Address Translation/Protocol Translation (NAT-PT) is defined in RFC 2766 but due to numerous problems, it has been obsoleted by RFC 4966 and deprecated to historic status. WP
- **NDA** : Non-Disclosure Agreement. WP
- **NFPA** : National Fire Protection Association is a United States trade association, albeit with some international members, that creates and maintains private, copyrighted standards and codes for usage and adoption by local governments. The association was formed in 1896 by a group of insurance firms. WP
- **NIDS** : Network Intrusion Detection System is an IDS installed on a the network, generally on a promiscous port, to avoid issue. WP
- **NIFC** : National Interagency Fire Center in Boise, Idaho is the physical facility which is the home to the National Interagency Coordination Center (NICC), and the National Multi-Agency Coordination group (NMAC or MAC). WP
- **NIPS** : Network Intrusion Prevention System is an IPS installed on the network. Generally inline, to be able to modify the traffic accordingly to its policy. WP
- **NIST** : National Institute of Standard and Technology WP
- **NSA** : National Security Agency, WP
- **OASIS** : Organization for the Advancement of Structured Information Standard is a global nonprofit consortium that works on the development, convergence, and adoption of open standards for security, Internet of Things, energy, content technologies, emergency management, and other areas. WP
- **OCTAVE** : Operationaly Critical Threat, Asset and Vulnerability Evaluation approach defines a risk-based strategic assessment and planning technique for security.WP
- **OSI** : Open Systems Interconnection model
- **OFB** : Output Feedback mode makes a block cipher into a synchronous stream cipher. It generates keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext. Just as with other stream ciphers, flipping a bit in the ciphertext produces a flipped bit in the plaintext at the same location. This property allows many error correcting codes to function normally even when applied before encryption. . WP
- **OFDM** : Orthogonal Frequency Division Multiplexing, in telecommunications, orthogonal frequency-division multiplexing (OFDM) is a method of encoding digital data on multiple carrier frequencies. OFDM has developed into a popular scheme for wideband digital communication, used in applications such as digital television and audio broadcasting, DSL internet access, wireless networks, power line networks, and 4G mobile communications. WP
- **OSCP** : Online Certificate Status Protocol is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate. It is described in RFC 6960 and is on the Internet standards track. WP
- **OWASP** : Open Web Application Security Project is an online community, produces freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security. WP
- **PaaS** : Platform as a Service, is when a provider allow customer to develop, run and manage application without having to manage the infrastructure like the OS, Network, etc. WP
- **PAN** : Personal Area Network WP

- **PASTA** : Process for Attack Simulation and Threat Analysis is a seven-step, risk-centric methodology. Discussed in domain 1. WP
- **PCI DSS** : Payment Card Industry Data Security StandardWP
- **PEAP** : Protected Extensible Authentication Protocol also known as Protected EAP or simply PEAP, is a protocol that encapsulates the Extensible Authentication Protocol (EAP) within an encrypted and authenticated TLS tunnel. The purpose was to correct deficiencies in EAP; EAP assumed a protected communication channel, such as that provided by physical security, so facilities for protection of the EAP conversation were not provided. WP
- **PEM** : Privacy-Enhanced Mail is a de facto file format for storing and sending cryptographic keys, certificates, and other data. WP
- **PGP** : Pretty Good Privacy is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. It use a web of trust. WP
- **PHI** : Protected Health Information, under the US law is any information about health status, provision of health care, or payment for health care. WP
- **PII** : Personally Identifiable Information, is information that allow to identify or give personal information on an individual. WP
- **PKI** : Public Key Infrastructure.WP
- **PP** : Protection Profile in the CC, is a set of security requierement that describe the TOE. WP
- **PPP** : Point to Point Protocol is a layer 2 protocol used to establish a direct connection between two devices. PPP is a successor for SLIP.WP
- **PPTP** : Point to Point Tunneling Protocol is an obsolete method for implementing virtual private networks. PPTP has many well known security issues. WP
- **P2PE** : Point to Point Encryption is a standard created by the PCI. WP
- **RADIUS** : Remote Authentification Dial-In User Service is a networking protocol, operating on port 1812 that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service.WP
- **RAID** : Redundant Array of Independent Disks. WP
- **RARP** : Reverse Address Resolution Protocol, translate MAC into IP address. WP
- **RBAC** : Role-Based Access Control is a security model defined around roles and privileges. Sometime RBAC can be "Rule Based Access Control". A firewall is a rule based acess control.WP
- **Repudiation** : is the ability to deny something. In IT, i's the ability to deny a user have done an action. The goal is to obtain non-repudiation, to be abme to prove a user have done an action.WP
- **RFI** : Radio-Frequency Interference, is a disturbance generated by an external source that affects an electrical circuit by electromagnetic induction, electrostatic coupling, or conduction. WP
- **RPC** : Remove Procedure Call is when a computer program causes a procedure (subroutine) to execute in a different address space (commonly on another computer on a shared network). WP

- **RPO** : Recovery Point Objective is the amount of data loss or system uavailability, mesured in time, a system or a company can endure. Recovery Point Objective is also the maximum sustainable data loss based on backup schedules and recovery.
- **RSA** : Rivest–Shamir–Adleman is one of the first public-key cryptosystems and is widely used for secure data transmission. WP
- **RSN** : Robust Security Network is another name for WPA2
- **RTO** : Recovery Time Objective is the acceptable amount of time to restore the function.
- **SA** : Security Association is the sharing of the parameters in a VPN between the two side to create the connection. WP
- **SaaS** : Software as a Service, is when a provider allow customer to use a software through web or other, but the customer manage nothing, he just use the application. WP
- **SABSA** : Sherwood Applied Business Security Architecture. SABSA is a framework and methodology for enterprise security architecture and service management. WP
- **SAML** : Security Assertion Markup Language is an open standard for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. WP
- **SCAP** : Security Content Automation Protocol is a NIST naming convention to describe security vulnerabilities. WP
- **SCTP** : Stream Control Transmission Protocol
- **SDLC** : System Development Life Cycle or Software Development Life Cycle. It's stated in the Sybex book that there is no distinction made about it for CISSP. ciscopress WP
- **SET** : Secure Electronic Transaction is a communications protocol standard for securing credit card transactions over networks, specifically, the Internet. WP
- **SEAL** : Software-optimized Encryption ALgorithm is a stream cipher optimised for machines with a 32-bit word size and plenty of RAM. WP
- **SHA-1** : Secure Hash Algorithm 1 is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value known as a message digest. Deprecated. Discussed in chapter 3. WP
- **SHA-2** : Secure Hash Algorithm is a set of cryptographic hash functions designed by the United States National Security Agency (NSA).Secure Hash Algorithm 2 WP
- **S-HTTP** : Secure HyperText Transfer Protocol is an obsolete alternative to the HTTPS protocol for encrypting web communications carried over HTTP. Discussed in chapter 3. WP
- : Security Information and Even Management, are a family of tools that does monitoring, reporting, notifications, correlation of events, etc. WP
- **SLA** : Service Level Agreement is a commitment between a service provider and a client. Particular aspects of the service – quality, availability, responsibilities – are agreed between the service provider and the service user. WP
- **SLE** : Single Loss Expectency is the monetary value expected from the occurrence of a risk on an asset. It's calculate by : AV*EF=SLE . WP

- **S/MIME** : Secure/Multipurpose Internet Mail Extension is a standard for public key encryption and signing of MIME data. WP
- **SMTP** : Simple Mail Transfer Protocol, OSI layer 7 protocol
- **Smurf Attack** : is a distributed denial-of-service attack based on ICMP and target's IP spoofing.WP
- **SNMA** : Sollicited Node Multicast Address, the protocol used to replace ARP in IPv6. WP
- **SOC** : System Organization Control are report of audit of a company, in the standard defined in SSAE 16. WP
- SOX : Sarbane - Oxley Act of 2002 is mandatory. ALL organizations, large and small, MUST comply. SOX, is a United States federal law that set new or expanded requirements for all U.S. public company boards, management and public accounting firms. SOX site
- **SPIT** : SPam over Internet Telephony is unsollicited call using VOIP. WP
- **SQL** : Structured Query Language, OSI layer 5 protocol WP
- **SSL** : Secure Sockets Layer. Developed in the early 90's by Netscape, it's now replaced by TLS. The last version, SSL3 is deprecated due some security breachs. While using TCP, it's still an OSI's layer 4 protocol.WP
- **ST** : Security Target is the documentation the TOE and others security requierement in the CC testing process. WP
- **TACACS** : Terminal Access Controller Access-Control System refers to a family of related protocols handling remote authentication and related services for networked access control through a centralized server. WP
- **TOE** : Target of Evaluation, in the CC, is the tested product.
- **TCP** : Transmission Control Protocol
- **TGS** : Ticket-Granting Service issue ticket and session keys to the client. WP
- **TGT** : Ticket-Grant Ticket is in Kerberos, a timestamped and encrypted. This ticket is granted by the KDC. The TGT will be sent to the TGS each time the user want to reach a new ressource. WP
- **TLS** : Transport Layer Security WP
- **TPM** : Trusted Platform Module (also known as ISO/IEC 11889) is an international standard for a secure cryptoprocessor, a dedicated microcontroller designed to secure hardware through integrated cryptographic keys. WP
- **TCB** : Trusted Computing Base is the set of all hardware, firmware, and/or software components that are critical to the system security, in the sense that bugs or vulnerabilities occurring inside the TCB might jeopardize the security properties of the entire system. WP
- **TCSEC** : Trusted Computing System Evaluation Criteria, is a United States Government Department of Defense (DoD) standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system. Not used anymore but it's the model for others security evaluation method, such as ITSEC. WP
- **UDP** : User Datagram Protocol
- **UPS** : Uninterruptible Power Supply is an electrical apparatus that provides emergency power to a load when the input power source or mains power fails. WP

- **USA PATRIOT** : Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, In response to the September 11 attacks, Congress swiftly passed legislation to strengthen national security. WP
- **USPTO** : United States Patent and Trademark Office. USPTO
- **VAST** : Visual, Agile and Simple Threat modeling. WP
- **VPN** : Virtual Private Network WP
- **WAN** : World Area Network is a telecommunications network or computer network that extends over a large geographical distance/place. WP
- **WPA2** : Wi-Fi Protected Access 2 security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. WP
- **XACML** : eXtensible Access Control Markup Language defines a declarative fine-grained, attribute-based access control policy language, an architecture, and a processing model describing how to evaluate access requests according to the rules defined in policies. It's used mainly in SDN.WP
- **XCCDF** : Extensible Configuration Checklist Description Format is an XML format specifying security checklists, benchmarks and configuration documentation. It's part of the SCAP. XCCDF development is being pursued by NIST, the NSA, The MITRE Corporation, and the US Department of Homeland Security. WP
- **XSRF** : Cross-Site Request Forgery also known as one-click attack or session riding and abbreviated as **CSRF**. It works by having a users click on a forged link pointing to a site where the users already have a session opened. WP
- **XOR** : Exculisive OR, or boolean operator that return true only when the input differ. WP
- **X.400** : X.400 is a suite of ITU-T Recommendations that define standards for Data Communication Networks for Message Handling Systems (MHS) — more commonly known as email. It's replaced by SMTP. WP
- **X.500** is a series of computer networking standards covering electronic directory services. The X.500 series was developed by ITU-T, formerly known as CCITT, and first approved in 1988. The directory services were developed in order to support the requirements of X.400 electronic mail exchange and name lookup. It's kind of replaced by LDAP. WP
- **X.509** : X.509 is a standard defining the format of public key certificates. X.509 certificates are used in many Internet protocols, including TLS/SSL. WP

Resources

- The current Sybex book can be found at https://www.wiley.com/go/cissp8e. The book grant access to a large set of question online. It must be read from cover to cover. It's a little bit redundant sometime, but it's said to cover 100% of the exam.
- The GRC podcast, with text transcript : Link
- Test and audio lecture : Link
- Wikibooks have a article with a great explanation to a lot a word and technologies that it's needed to know to pass the exam : Link

- The infosec documentation is very great, a lot of this page content is based on it. Link.
- MindCert have some great map : MindCert
- IT Dojo have a great youtube channel with around 100 videos (as of July 2019), in video is about 2 questions and great explaination. Youtube Playlist.
- MF Prod have maybe the more deep, long and detailed videos about the CISSP on Internet. Youtube Channel

Every force you create has an echo. Your own bad energy will be your undoing.