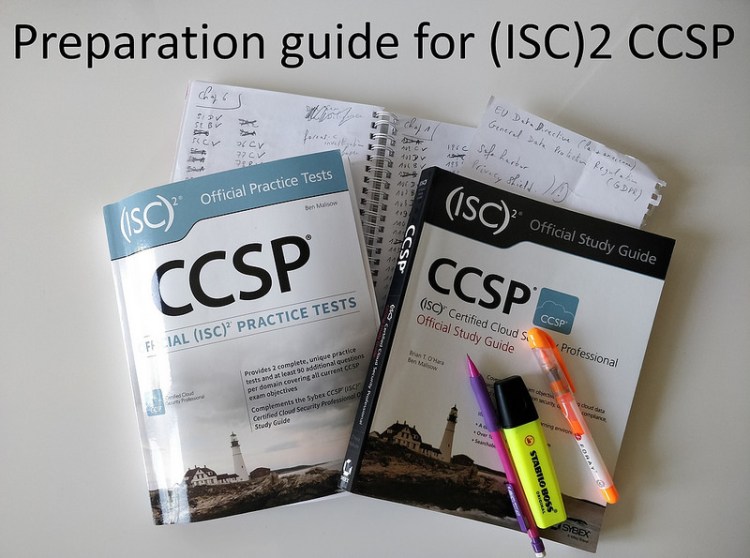
**Preparation Guide for ISC2 Certified Cloud Security Professional (CCSP) Certification**

Posted by [squastana](https://stanislas.io/author/squastana/)

I just get my Certified Cloud Security Professional (CCSP) Certification and it is time now to share my preparation notes for those who are interested to pass this exam and get certified too. This article is just one another **preparation guide to CCSP** but I hope it will be useful



Before starting studying, you must know very well what this certification is about and what are the prerequisite

The topics included in the CCSP Common Body of Knowledge (CBK) ensure its relevancy across all disciplines  
in the field of cloud security. Successful candidates are competent in the following 6 domains:  
– Architectural Concepts & Design Requirements (19%)  
– Cloud Data Security (20%)  
– Cloud Platform & Infrastructure Security (19%)  
– Cloud Application Security (15%)  
– Operations (15%)  
– Legal & Compliance (12%)

It is a **4 hours exam** in front of a computer (and under video camera :))

There are **125 questions**

**The passing score is 700/1000**

Mandatory to read before preparing and passing CCSP Exam : CCSP Exam Outline  
Source : <https://www.isc2.org/-/media/ISC2/Certifications/Exam-Outlines/CCSP-Exam-Outline.ashx>

You will need between 40 to 60 hours to prepare correctly this exam (depending on your experience, knowledge…). Don’t underestimate the time necessary to study books, read white papers, search information and practice blank tests.

So if you spend 2 hours a day preparing, you can pass exam in one month.

I also strongly encourage to schedule your exam day before starting to study (because it will be easier to make a reverse planning)

There are 2 Official books that I think are mandatory to read :

* CCSP (ISC)2 Certified Cloud Security Professional Official Study Guide : <https://amzn.to/2uqQrQ5>
* CCSP Official (ISC) 2 Practice Tests : <https://amzn.to/2Jg7t8E>

The second book must be used **only after reading the first one** (that contains also some practice questions but more easier than the practice tests book)

Next you will find all my preparation notes, there are a lot of URL with a lot of additional content to read because everything is not in the official books ! I put also a package of documents in my Onedrive ([https://G1drv.ms/f/s!ApyDK\_-MHwLvisVDZH1fx4OSWNItFw](https://1drv.ms/f/s!ApyDK_-MHwLvisVDZH1fx4OSWNItFw)) if you want to download quicker a “package of good papers to read”

**======—– Domain 1 – Architectural Concepts & Design Requirements (19%)——-======**

Cloud Computing Definitions (ISO/IEC 17788)  
ISO/IEC 17788 Overview and vocabulary on Cloud computing  
NIST 800-145 Cloud computing definition : <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

NIST 500-292 : Cloud Computing Reference Architecture  
<https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=909505>

Reduction in Capital Expenditure (Capex)  
Cloud = metered service model  
Cloud bursting

Elasticity  
Simplicity  
Scalability

Cloud Customer  
Cloud User

Cloud = Elasticity, Simplicity, Scalability

Cloud Service models : IaaS, Paas, SaaS  
Cloud deployment models : Public, Private, Community, Hybrid

CSP : Cloud Service Provider  
Ex: Azure, AWS

CSB : Cloud Service Broker

CASB : Cloud Access Service Broker. 3d party offering IAM (Identity & Access Management) to CSP and Cloud customer  
Offers services like : SSO, certificate management, cryptographic key escrow (=key recovery) cf. <https://www.schneier.com/academic/archives/1997/04/the_risks_of_key_rec.html>

Regulators : entities that ensure organization are in compliance with the regulatory framework for which they are responsible  
ex: HIPAA, GLBA, PCI-DSS, ISO, SOX  
Example of regulators : FTC (Federal Trade Commission), SEC (Security and Exchange Commission)

NaaS : Network as a Service <https://en.wikipedia.org/wiki/Network_as_a_service>  
CompaaS : Compliance as a Service  
DSaaS : Data Science as a service

Cloud portability : ability to move applications & associated data between 2 clouds or between cloud and on-premises

Pat-down : A pat-down is not standard procedure

FIPS 140-2 : NIST document that lists accredited and outmoded cryptosystems

— FIPS 140-2 Levels

FIPS-140-2 : The Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2) is a U.S. government computer security standard used to approve cryptographic modules.  
The title is Security Requirements for Cryptographic Modules.  
FIPS 140-2 defines four levels of security, simply named “Level 1” to “Level 4”  
– Security Level 1 provides the lowest level of security : No specific physical security mechanisms are required in a Security Level 1 cryptographic module beyond the basic requirement for production-grade components  
– Security Level 2 improves upon the physical security mechanisms of a Security Level 1 cryptographic module by requiring features that show evidence of tampering  
– Security Level 3 attempts to prevent the intruder from gaining access to CSPs (Critical Security Parameter) held within the cryptographic module.  
– Security Level 4 provides the highest level of security. At this security level, the physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access. Penetration of the cryptographic module enclosure from any direction has a very high probability of being detected, resulting in the immediate deletion of all plaintext CSPs  
Source : <https://en.wikipedia.org/wiki/FIPS_140-2>

Due care versus Due diligence :

– Due diligence is the act of gathering the necessary information so the best decision-making activities can take place.  
due diligence requires that an organization continually scrutinize their own practices to ensure that they are always meeting or exceeding the requirements for protection of assets and stakeholders  
This is something a company does prior to buying a service i.e. check the service provider is compliant in the areas they claim to be i.e. Are ISO27001 Certified – not compliant.  
Due Diligence is the assessment of the risks (identification, likelihood, consequences if realized)

– Due care pertains to acting responsibly and “doing the right thing.”  
It is a legal term that defines the standards of performance that can be expected  
due care intends to set a minimum necessary standard of care to be employed by an organization  
The lack of due care is often considered negligence, and in most countries is actionable under law. If an organization is legally mandated to comply with regulations or information security requirements knowingly or unknowingly neglecting those requirements could lead to legal exposure from a due care perspective.  
This is something I would do for my company ensuring we follow the rules/regulations and best practices.  
Due Care is doing what a reasonable person would do about those risks

TOGAF (The Open Group Architecture Framework)  
TOGAF is a framework for enterprise architecture that provides an approach for designing, planning, implementing, and governing an enterprise information technology architecture.  
TOGAF is a high level approach to design  
It is typically modeled at four levels: Business, Application, Data, and Technology. It relies heavily on modularization, standardization, and already existing, proven technologies and products.  
<https://en.wikipedia.org/wiki/The_Open_Group_Architecture_Framework>

Virtualization sprawl (VM sprawl) :  
Virtualization sprawl is a phenomenon that occurs when the number of virtual machines (VMs) on a network reaches a point where the administrator can no longer manage them effectively  
To prevent virtualization sprawl, the administrator should define and enforce a process for the deployment of VMs and create a library of standardized VM image files

Erasure coding :  
RAID with parity (like RAID 5) and erasure coding improve data availability and safety. They enrich the original with redundancy data and spread it across disks. A subset of this data is enough to regenerate the original data. RAID is used for redundant storage of entire disks within a server. Erasure coding is usually used in distributed storage systems. So you can think of erasure coding as generalized and distributed RAID  
Erasure coding is a method of data protection in which data is broken into fragments that are expanded and encoded with a configurable number of redundant pieces of data and stored across different locations, such as disks, storage nodes or geographical locations.  
Erasure coding allows for the failure of two or more elements of a storage array and so offers more protection than Raid as commonly deployed.  
Erasure coding is also found in the context of object storage, with very large-volume cloud operators  
Erasure coding is a good option for latency tolerant, large capacity stores  
<https://www.quobyte.com/blog/2016/08/15/erasure-coding-in-production/>  
<https://www.computerweekly.com/feature/Erasure-coding-versus-RAID-as-a-data-protection-method>  
<https://www.snia.org/sites/default/files/SDC15_presentations/datacenter_infra/Shenoy_The_Pros_and_Cons_of_Erasure_v3-rev.pdf>  
<https://www.networkcomputing.com/storage/raid-vs-erasure-coding/1792588127>  
Ex: Ceph

AONT-RS: Blending Security and Performance in Dispersed Storage Systems  
In cryptography, an all-or-nothing transform (AONT), also known as an all-or-nothing protocol, is an encryption mode which allows the data to be understood only if all of it is known

**======—– Domain 2 – Cloud Data Security (20%)——-======**

Cloud Data Lifecycle (CSA Guidance) – *15 pages that is mandatory to read*  
Source : <https://cloudsecurityalliance.org/wp-content/uploads/2011/09/Domain-5.docx>

Data Controller, Data Owner, Cloud Customer : any entity collecting or creating data  
Data Processor, Data Custodian, Cloud Provider : any entity acting on behalf or at the behest of the Data Controller

IaaS, for public or private cloud, generally includes the following storage options:  
– Raw storage  
– Volume storage : includes volumes attached to IaaS instances, typically as a virtual hard drive.  
Volumes often use data dispersion to support resiliency and security.  
– Object Storage (aka File Storage)  
– CDN : Content Delivery Network

PaaS both provides and relies on a very wide range of storage options, including:  
PaaS may provide :  
– Database as a Service  
– Hadoop/MapReduce/Big Data as a Service  
– Application Storage  
PaaS may consume :  
– Database  
– Object/File Storage  
– Volume Storage  
– Other

SaaS uses a very wide range of storage and consumption models.  
SaaS storage is always accessed via a web-based user interface or client/server application  
SaaS may provide :  
– Information Storage and Management  
– Content/File Storage  
SaaS may consume :  
– Database  
– Object/File Storage  
– Volume Storage

Data (Information) Dispersion : A technique that is commonly used to improve data security, but without the use of encryption mechanisms

Homomorphic encryption : able to process data while it’s encrypted

**/!\ The Data Security Livecycle** – 6 phases :  
– create  
– store  
– use  
– share  
– archive  
– destroy (ex: using crypto shredding)

DAM : Database Activity Monitoring  
Database Activity Monitors capture and record, at a minimum, all Structured Query Language (SQL) activity in real time or near real time, including database administrator activity, across multiple database platforms; and can generate alerts on policy violations.

FAM : File Activity Monitoring  
Products that monitor and record all activity within designated file repositories at the user level, and generate alerts on policy violations

Movement to the Cloud :  
A combination of URL filtering (web content security gateways) and Data Loss Prevention (DLP) can detect data moving from the enterprise into the cloud.

Protecting Data Moving To (And Within) The Cloud, 3 options :  
– Link/Network Encryption : SSL, VPN, SSH  
– Client/Application Encryption  
– Proxy-Based Encryption: Data is transmitted to a proxy appliance or server which encrypts before sending further on the network

Content discovery includes the tools and processes to identify sensitive information in storage.  
Content discovery is normally a feature of Data Loss Prevention tools, and for databases is sometimes available in Database Activity Monitoring products.

Protecting Data in cloud

IaaS encryption  
– Volume Storage Encryption  
3 methods :  
– Instance-managed encryption  
– Externally managed encryption  
– Proxy encryption

– Object Storage Encryption  
– File/Folder encryption and Enterprise Digital Rights Management  
– Client/Application encryption  
– Proxy encryption

– PaaS Encryption  
– Database encryption  
– Client/Application encryption  
– Proxy encryption

– SaaS encryption  
– Provider-managed encryption: Data is encrypted in the SaaS application and generally managed by the provider.  
– Proxy encryption

– Data Loss Prevention (DLP)  
– Dedicated appliance/server  
– Virtual appliance  
– Endpoint agent  
– Hypervisor agent

– Database and File Activity Monitoring

ISO/IEC 27040 is Information technology — Security techniques — Storage security. Was published 5th january 2015  
ISO/IEC 27040 provides specific, detailed implementation guidance relevant to storage security for the general security controls described in ISO/IEC 27002.  
Source : <https://en.wikipedia.org/wiki/ISO/IEC_27040>

SIEM : Security Information and Event Management  
SEM : Security Event Management  
SIM : System Information Management

The term security information event management (SIEM), coined by Mark Nicolett and Amrit Williams of Gartner in 2005 :  
– the product capabilities of gathering, analyzing and presenting information from network and security devices  
– identity and access-management applications  
– vulnerability management and policy-compliance tools  
– operating-system, database and application logs  
– external threat data  
Source : <https://en.wikipedia.org/wiki/Security_information_and_event_management>

Tokenization (data security) is the process of substituting a sensitive data element with a non-sensitive equivalent, referred to as a token, that has no extrinsic or exploitable meaning or value.  
The token is a reference (i.e. identifier) that maps back to the sensitive data through a tokenization system.  
The tokenization system must be secured and validated using security best practices  
Only the tokenization system can tokenize data to create tokens, or detokenize back to redeem sensitive data under strict security controls  
Tokenization systems may be operated in-house within a secure isolated segment of the data center, or as a service from a secure service provider.  
The choice of tokenization as an alternative to other techniques such as encryption will depend on varying regulatory requirements, interpretation, and acceptance by respective auditing or assessment entities  
Example of use : The PCI Council defines tokenization as “a process by which the primary account number (PAN) is replaced with a surrogate value called a token  
Source : <https://en.wikipedia.org/wiki/Tokenization_(data_security)>

Data Masking = Data obfuscation = Data anonymisation

Static Data Masking (SDM): permanently replaces sensitive data by altering data at rest.  
SDM is primarily used to provide high quality (i.e., realistic) data for development and testing of applications without disclosing sensitive information.  
Additional uses include protecting data for use in analytics and training as well as facilitating compliance with standards and regulations (such as GDPR, PCI, HIPAA) that require limits on the use of data that identifies individuals.  
SDM also facilitates cloud adoption because DevOps workloads are among the first that organizations migrate to the cloud. Masking data on premises prior to uploading it to the cloud reduces risk for organizations concerned with cloud-based data disclosure.

Dynamic Data Masking (DDM) : aims to replace sensitive data in transit leaving the original at-rest data intact and unaltered  
DDM is primarily used to apply role-based (object-level) security for databases/applications.  
In practice, the complexities involved in preventing masked data from being written back to the database essentially mean DDM should only be applied in read-only contexts such as reporting or customer service inquiry functions.  
Not well suited for use in a dynamic (read/write) environment such as an enterprise application because masked data could be written back to the database, corrupting the data.

Source : <https://www.imperva.com/blog/2017/07/static-versus-dynamic-data-masking/>

Technics for Datamasking :  
– Substitution is one of the most effective methods of applying data masking and being able to preserve the authentic look and feel of the data records.  
– Shuffling method is a very common form of data obfuscation. the data is randomly shuffled  
– Numeric variance method is very useful for applying to financial and date driven information fields  
– Encryption is often the most complex approach to solving the data masking problem  
– Nulling out or deletion  
– Masking out : Character scrambling or masking out of certain fields is also another simplistic yet very effective method. This system is not very effective for test systems but is very useful for the billing scenario detailed above. It is also commonly known as a dynamic data masking method

Data masking invariably becomes the part of these processes in SDLC as the development environments’ SLAs are usually not as stringent as the production environments’ SLAs regardless of whether application is hosted in the cloud or on-premises.

Source : <https://en.wikipedia.org/wiki/Data_masking>

Direct Identifiers / indirect Identifiers

Information that is sufficient on its own to identify an individual includes a person’s full name, social security number, email address containing the personal name, and biometric identifiers such as fingerprints, facial image, voice patterns, hand geometry, iris scan, or manual signature.  
This type of data are often called direct identifiers.

Other information that may be used to fairly easily identify an individual include a person’s postal address, phone number, vehicle registration number, bibliographic citation to publications, email address not in the form of the personal name, web address to a web page containing personal data, unusual job title, rare disease, position held by only one person at a time (e.g. chairperson in an voluntary organization).  
The Finnish Social Science Data Archive calls this type of data strong indirect identifiers.  
The data archive also counts as strong indirect identifiers the types of codes that can be used to unequivocally identify an individual from among a group of individuals. These include, for instance, student ID number, insurance or bank account number, or IP address of a computer etc.

Source : <http://www.fsd.uta.fi/aineistonhallinta/en/anonymisation-and-identifiers.html>  
<https://www.slideshare.net/StevenMeister/are-you-prepared-for-eu-gdpr-indirect-identifiers-what-are-indirect-identifiers>

Cryptographic Bit splitting (aka cryptographic data splitting)  
The technique involves encrypting data, splitting the encrypted data into smaller data units, distributing those smaller units to different storage locations, and then further encrypting the data at its new location  
One application of cryptographic splitting is to provide security for cloud computing. The encrypted data subsets can be stored on different clouds, with the information required to restore the data being held on a private cloud for additional security  
Source : <https://en.wikipedia.org/wiki/Cryptographic_splitting>

Homomorphic encryption : you can perform useful operations on encrypted values without decrypting them first  
Source : <https://blog.cryptographyengineering.com/2012/01/02/very-casual-introduction-to-fully/>

Key Management :  
– Level of protection : encryption key must be secure at the same level of control or higher as the data they protect  
– Key recovery  
– Key Distribution : keys should never be passed in clear  
– Key revocation  
– Key escrow  
– Outsourcing Key Management : example using a CASB (Cloud Access Security Broker)  
Source : <https://en.wikipedia.org/wiki/Key_management>

Data Discovery techniques  
Data discovery is not a tool. It is a business user oriented process for detecting patterns and outliers by visually navigating data or applying guided advanced analytics.  
Automated data discovery methods like data loss prevention (DLP) tools can help, as can open source tools designed to find certain kinds of regulated data (for example, the open source ccsrch tool that finds and flags credit card information)  
Application inventories are a required part of HIPAA and PCI DSS compliance activities and can be directly leveraged to find areas of regulated information at a service provider.  
Source : <https://bi-survey.com/data-discovery>  
<https://searchcloudsecurity.techtarget.com/tip/Techniques-for-sensitive-data-discovery-in-the-cloud>

Data Classification  
– Data States : Data exists in one of three states : at rest, in process, or in transit  
– Data Format : Data can be either structured or unstructured  
– Data Discovery : Data discovery is a process for identifying and providing visibility into the location, volume, and context of structured and unstructured data stored in a variety of data repositories.  
– Data Sensitivity. Data is classified according to its sensitivity level—high, medium, or low  
– Compliance Requirements

Data Classification Process :  
– Execute data discovery  
– Define data classification policies  
– Execute data classification process  
– Implement enforcement technologies to protect classified data  
Source : <https://www.imperva.com/data-security/data-security-101/data-classification/>

PII : Personally Identifiable Information

The Organization for Economic Co-operation and Development (OECD) Privacy Guidelines are the most widely-accepted privacy principles. The OECD identified the following Fair Information Practices :  
– Collection Limitation  
– Data quality  
– Purpose Specification  
– Use Limitation  
– Security Safeguard  
– Openess  
– Individual participation  
– Accountability

Privacy-Specific Safeguards:  
– Minimize Collection, Use and Retention of PII  
– Conducting Privacy Impact Assessments  
– De-Identifying Information : records that have had enough PII removed or obscured, also referred to as masked or obfuscated  
– Anonymizing Information :  
– Generalizing the Data : Making information less precise  
– Suppressing the Data : Deleting an entire record or certain parts of records  
– Introducing Noise into the Data : Adding small amounts of variation into selected data  
– Swapping the Data : Exchanging certain data fields of one record with the same data fields of  
another similar record  
– Replacing Data with the Average Value : Replacing a selected value of data with the average value  
for the entire group of data

Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)  
<https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-122.pdf>

DRM : Digital Right Management

Digital Rights Management (DRM) : 2 kinds  
– Customer DRM (ex: to protect usage of music, video, eBook)  
– Enterprise DRM (ex: Microsoft Information Right Protection): DRM is used to protect the content of an organization internally and with business partners

DRM implementation  
– Rudimentary reference checks  
– Online reference checks  
– Local Agent checks  
– Presence of licensed media (ex: a CD/DVD)  
– Support-based licensing

DRM Challenge  
– Replication restrictions  
– Jurisdictional Conflicts (ex: Netflix movies access depends on countries)  
– Agent/Enterprise Conflicts  
– Mapping Identity & Access Management (IAM) & DRM  
– API Conflicts

DRM functions  
– Persistent Protection  
– Dynamic Control Access  
– Automatic Expiration  
– Continuous auditing  
– Replication restrictions  
– Remote Rights revocation

Data Retention policy (take place in the Archive phase of data life cycle) includes :  
– Retention Period  
– Applicable Regulation  
– Retention Formats  
– Data Classification  
– Archiving and retrieval procedures  
– Monitoring, Maintenance and enforcement

Data Audit policy includes :  
– Audit periods  
– Audit scope  
– Audit responsibilities (internal and/or external)  
– Audit processes & procedures  
– Applicable regulations  
– Monitoring, Maintenance and enforcement

Having the logs is one thing, reviewing the logs you have is something else

Log review : challenges :  
– Log review and analysis is not often a priority  
– Log review is mundane and repetitive  
– Log review requires someone both new to the field and experienced  
– The reviewer needs to have an understanding of the operation

Data destruction / Disposal (in the Destroy Phase of Data life cycle)  
– Physical destruction of media or hardware  
– Degaussing  
– Overwriting  
– cryptoshredding (aka Cryptographic Erasure)

**Cryptoshredding is the only pragmatic option for data disposal in the cloud**

NIST Released Special Publication 800-88 Revision 1, Guidelines for Media Sanitization  
<https://csrc.nist.gov/News/2014/Released-SP-800-88-Revision-1,-Guidelines-for-Medi>

**======—– Domain 3 – Cloud Platform and Infrastructure Security (19%)——-======**

BIA : Business Impact Analysis  
Assessment of the priorities given to each asset and process withing the organization  
A proper analysis should consider the effect (=impact) any harm or loss of each asset might mean to the organization overall  
Assets can be tangible or intangible

Criticality : denotes those aspects of the organization without which the organization could not operate or exist

— RISK Management

Risk appetite : level or amount or type of risk that the organization finds acceptable

Risk to health or human safety –> must be addressed

4 ways to address risk :  
– Avoidance  
– Acceptance  
– Transference  
– Mitigation

Remaining leftover risk is called Residual Risk

NIST 800-37 : “Guide for Applying the Risk Management Framework to Federal Information Systems”  
The purpose of SP 800-37 Rev 1 is to provide guidelines for applying the Risk Management Framework to federal information systems to include conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring  
Source : <https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final>

Risk Management Framework (cf. NIST 800-37)  
– Step 1 : CATEGORIZE Information System  
– Step 2 : SELECT security controls  
– Step 3 : IMPLEMENT security controls  
– Step 4 : ASSESS security controls  
– Step 5 : AUTHORIZE Information System  
– Step 6 : MONITOR security controls

Enterprise Risk Management (ERM) is the overall management of risk for an organization  
Risk management in cloud is based on the shared responsibilities model  
The cloud user is ultimately responsible for ownership of the risks; they only pass on some of the risk management to the cloud provider.  
One of the core tenants of risk management is that you can manage, transfer, accept,  
or avoid risks

— SABSA  
SABSA is a proven framework and methodology used successfully around the globe to meet a wide variety of Enterprise needs including Risk Management, Information Assurance, Governance, and Continuity Management  
Although copyright protected, SABSA is an open-use methodology, not a commercial product.  
Managed by an Institute in UK  
<http://www.sabsa.org/node/5>

**Under the current and legal regulatory regime, the cloud customer is ALWAYS ultimately legally liable for any loss of data**

Risk with cloud providers :  
– Vendor Lock-in  
– Vendor Lock-out

**======—– Domain 4 – Cloud Application Security (15%) ——-======**

RESTful  
OWASP Top 10

Cloud Security Alliance – Notorious Nine  
<https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf>

Software Development Life-Cycle (SDLC) Process  
<https://stackify.com/what-is-sdlc/>  
<https://handouts.secappdev.org/handouts/2014/Bart%20De%20Win/SDLC%20v1.0.pdf>  
Phases :  
– Analyze  
– Design (Risk analysis including threat modeling using methodology like Microsoft STRIDE)  
– Implement  
– Test  
– Deploy  
– Maintain

ISC2 Book – SDLC, core stages  
– Defining  
– designing  
– Development  
– Testing

SAST : Static Application Security Testing (White Box testing)  
ex: Source Code Analysis (SCA)  
God for devops or CI/CD environment  
SAST is becoming the go-to option due to the growing needs of the new development era.

DAST : Dynamic Application Security Testing (Black Box testing)  
ideally suited for Waterfall environments  
not ideal for Continuous Integration scenarios  
<https://www.checkmarx.com/2015/04/29/sast-vs-dast-why-sast-3/>

Fuzzing or fuzz testing : automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failing built-in code assertions or for finding potential memory leaks.

**Treat Modeling : Microsoft STRIDE**  
S : Spoofing  
T : tampering  
R : Repudiation  
I : Information disclosure  
D : Denial of Service  
E : Elevation of privilege  
<http://download.microsoft.com/download/9/3/5/935520EC-D9E2-413E-BEA7-0B865A79B18C/Introduction_to_Threat_Modeling.ppsx>  
<https://docs.microsoft.com/en-us/azure/security/azure-security-threat-modeling-tool-getting-started>

The Smurf attack is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim’s spoofed source IP are broadcast to a computer network using an IP broadcast address. Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim’s computer will be flooded with traffic.  
source : https://en.wikipedia.org/wiki/Smurf\_attack

A variation to the Smurf attack is the Fraggle attack. The attack is essentially the same as the Smurf attack but instead of sending an ICMP echo request to the direct broadcast address, it sends UDP packets.  
Source: <https://usa.kaspersky.com/resource-center/definitions/smurf-attack>

“Snarfing” is the action of grabbing data and using it without the owner’s consent  
<https://lifars.com/2015/03/weird-security-term-of-the-week-snarfing/>

OWASP Top 10 2017  
<https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf>

Cross-Site Request Forgery (CSRF) Attack

XSS Attack : XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim’s browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites

3 types of XSS Attacks :  
– Reflected XSS  
– Stored XSS  
– DOM XSS

WAF : Web Application firewall  
DAM : Database Activity Monitoring

API Gateway

RASP (Runtime Application Self-Protection)

ISO/IEC 27034-5:2017 : Information technology — Security techniques — Application security  
ISO/IEC 27034-5 outlines and explains the minimal set of essential attributes of ASCs and details the activities and roles of the Application Security Life Cycle Reference Model (ASLCRM).  
<https://www.iso.org/standard/55585.html>

**======—— Domain 5 – Operations (15%) ———==========**

ASHRAE (American Society of Heating, Refrigerating and Air-Conditioning Engineers)  
is a global professional association seeking to advance heating, ventilation, air conditioning and refrigeration systems design and construction

HVAC : Heating, Ventilation, Air Conditioning

FM200 Fire Suppression (aka HFC227ea)  
is a water-less fire protection system, it is discharged into the risk within 10 seconds and suppresses the fire immediately.  
FM200 gas is extremely safe for occupied spaces with the correct fire suppression design.  
FM200 is classed as a clean agent which means that it is safe to use within occupied spaces  
FM200 fire suppressant does not deplete stratospheric ozone, and has minimal impact on the environment relative to the impact a catastrophic fire would have  
leaves no residue on valuable equipment after discharge

Halon 1301  
It is considered good practice to avoid all unnecessary exposure to Halon 1301  
Is an effective gaseous fire suppression fixed systems agent  
Is an ozone depleter  
<https://en.wikipedia.org/wiki/Bromotrifluoromethane>

Spot-type Smoke detector  
– ionization-based : using a small amount of radioactive material  
– photoelectric : using a light source and a photosensitive sensor

Air aspiring / Air Sampling Smoke Detector (ASSD)

Codes require detectors under the floor or above the ceiling where HVAC piping, electrical feeders, or IT cables are placed within these plenum spaces

sources : [https://www.facilitiesnet.com/datacenters/article/Evaluating-Fire-Detection-Options-For-Data-Centers-Facilities-Management-Data-Centers-Feature–14594](https://www.facilitiesnet.com/datacenters/article/Evaluating-Fire-Detection-Options-For-Data-Centers-Facilities-Management-Data-Centers-Feature--14594)  
<http://digital.bnpmedia.com/publication/?i=170081&article_id=1473573&view=articleBrowser&ver=html5#{%22issue_id%22:170081,%22view%22:%22articleBrowser%22,%22article_id%22:%221473573%22}>

Plenum : in building construction, a plenum (pronounced PLEH-nuhm, from Latin meaning full) is a separate space provided for air circulation for heating, ventilation, and air-conditioning (sometimes referred to as HVAC) and typically provided in the space between the structural ceiling and a drop-down ceiling

Temperature and humidity levels in accordance with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) guidelines

Temperature range is typically between 18 degrees Celsius to 27 degrees  
(64.4 degrees to 80.6 degrees Fahrenheit); (ASHRAE 67 -> 82)

Humidity is measured by Relative Humidity Percentage Non-Condensing  
with the current range between 40% and 55% (60% in ISC2 book) (ASHRAE 65%)

Source : <https://www.ashrae.org/File%20Library/Technical%20Resources/Technical%20FAQs/TC-02.01-FAQ-92.pdf>

Raised floors :  
The height of the legs/pedestals is dictated by the volume of cables and other services provided beneath, but typically arranged for a clearance of at least six inches or 15 cm with typical heights between 24 inches to 48 inches  
<https://en.wikipedia.org/wiki/Raised_floor>

Deterrent : a thing that discourages or is intended to discourage someone from doing something.  
“cameras are a major deterrent to crime”

TPM : Trusted Platform Module

Secure KVM :  
– Isolated Data Channels  
– Housing Intrusion Detection  
– Tamper-Proof Labels  
– “No-Buffer” Design  
– Restricted USB function  
– Push-Button Control  
<http://www.42u.com/secure-kvm-switches>  
ex: <https://www.tripplite.com/pages/niap-secure-kvm>

DRS : Distributed Resource Scheduling  
DO : Dynamic Optimization

IDS  
IPS  
HoneyPod

ITIL, ISO/IEC 20000-1

ISMS : Information Security Management System  
ex: ISO/IEC 27001 specifies a management system that is intended to bring information security under management control and gives specific requirements  
<https://en.wikipedia.org/wiki/ISO/IEC_27001>

CMDB : Configuration Management Database

COBIT stands for Control Objectives for Information and Related Technology.  
It is a framework created by the ISACA (Information Systems Audit and Control Association) for IT governance and management. It was designed to be a supportive tool for managers—and allows bridging the crucial gap between technical issues, business risks, and control requirements

Compartmentalization (information security)  
is the limiting of access to information to persons or other entities who need to know it in order to perform certain tasks.  
<https://en.wikipedia.org/wiki/Compartmentalization_(information_security)>

Understand the Collection, Acquisition and Preservation of Digital Evidence Forensic

Uptime Institute’s Tier Classification System for data centers  
<https://journal.uptimeinstitute.com/explaining-uptime-institutes-tier-classification-system/>

Tier I : Basic capacity -> UPS, generator, dedicated cooling equipment  
Tier II : Redundant capacity components -> includes redundant critical power and cooling components. The redundant components include power and cooling equipment such as UPS modules, chillers or pumps, and engine generators.  
Chiller : machine that removes heat from a liquid via a vapor-compression or absorption refrigeration cycle. This liquid can then be circulated through a heat exchanger to cool equipment, or another process stream  
Tier III : Concurrently Maintainable -> requires no shutdowns for equipment replacement and maintenance. A redundant delivery path for power and cooling is added to the redundant critical components of Tier II  
Tier IV: Fault Tolerance -> adding the concept of Fault Tolerance to the site infrastructure topology

The Tier Classification System does not prescribe specific technology or design criteria beyond those stated above  
Tier Certification is a performance based evaluation of a data center’s specific infrastructure, and not a checklist or cookbook  
<https://uptimeinstitute.com/tiers>  
<https://en.wikipedia.org/wiki/Uptime_Institute>

CM (Configuration Management)

— BCDR

BCDR (Business Continuity / Disaster Recovery)

Event : any unscheduled adverse impact to the operating environment  
An event is distinguished from a disaster by the duration of impact  
we consider an event’s impact to last 3 days or less. A disaster’s impact lasts longer

The paramount importance in BC/DR planning and efforts should be health and human safety, as in all security matters

MAD : Maximum Allowable Downtime  
RTO : Recovery Time Objective  
RPO : Recovery Point Objective

For all datacenters, a minimum of at least 12 hours of fuel for all generators

For BCDR purposes, the plan should anticipate at least 72 hours of generator operation before other alternative are available

BCDR testing methodology  
– Tabletop testing : essential participants, a sort of role-playing game  
No impact on production  
– Dry Run : whole organization take part in a scenario at a scheduled time but without performing the tasks in real  
More impact on productivity than Tabletop  
– Full Test : Entire organization takes part in an unscheduled, unannounced practice scenario

**======—– Domain 6 – Legal & Compliance (12%) ——-======**

ISO/IEC 27050-1:2016 : Information technology — Security techniques — Electronic discovery  
<https://www.iso.org/standard/63081.html>

HIPAA : Health Information Portability and Accountability Accountability  
GLBA : Graham-Leach-Bliley Accountability  
PCI-DSS : Payment Card Industry Data Security Standard  
PCI PA-DSS : PCI Payment Application DSS  
SOX : Sarbanes Oxley Act

— Privacy

PII : Personally Identifiable Information  
PLA : Privacy Level Agreement

ISO/IEC 27018 Code of Practice for Protecting Personal Data in the Cloud  
<https://www.microsoft.com/en-us/trustcenter/compliance/iso-iec-27018>

Privacy  
the data controller (typically the entity that has the primary relationship with an  
individual) is prohibited from collecting and processing personal data unless certain criteria are met.  
These laws define numerous obligations, such as confidentiality and security obligations, for theentities that access personal data.  
Many countries prohibit or restrict the transfer of information out of their borders. In most cases, the transfer is permitted only if the country to which the data is transferred offers an “adequate level of protection” (as defined in the relevant national law) of personal information and privacy rights of affected individuals.

PII : Personally Identifiable Information

Data Subject : individual who the PII refers to  
Data Controller, Cloud Customer, Data Owner : any entity collecting or creating PII  
Data Processor, Cloud Provider, Data Custodian: any entity acting on behalf or at the behest of the Data Controller

**Data Controller is ultimately responsible for any unauthorized disclosure of PII**

EU Network Information Security Directive (NIS Directive) :  
The NIS Directive entered into force in August 2016, requiring each EU/EEA member state to implement the Directive into its national legislation by May 2018.

Difference between a Regulation, Directive and Decision in Europe:  
– Regulations have binding legal force throughout every Member State and enter into force on a set date in all the Member States  
– Directives lay down certain results that must be achieved but each Member State is free to decide how to transpose directives into national laws  
– Decisions are EU laws relating to specific cases and directed to individual or several Member States, companies or private individuals. They are binding upon those to whom they are directed.

— GDPR (General Data Protection Regulation)  
The European Union (EU) adopted the General Data Protection Regulation (GDPR) in 2016, which is binding on all EU member states, as well as members of the European Economic Area (EEA).  
The GDPR will become enforceable as of May 25, 2018. On that date, Directive 95/46/EC on the Protection of Personal Data, which had been the legal basis of the provisions of the national data protection laws of all EU and EEA member states, will be repealed.  
From a security standpoint, the Network Information Security Directive (NIS Directive) is paving the way to more stringent security requirements. Adopted in 2016, the NIS Directive requires EU/EEA member states to implement new information security laws for the protection of critical infrastructure and essential services by May 2018  
General Data Protection Regulation (GDPR)  
The new GDPR is directly binding on any corporation that processes the data of EU citizens  
Breaches of Security: The GDPR requires companies to report that they have suffered a breach of security. The reporting requirements are risk-based, and there are different requirements for reporting the breach to the Supervisory Authority and to the affected data subjects. Breaches must be reported within 72 hours of the company becoming aware of the incident.  
Sanctions: Violations of the GDPR expose a company to significant sanctions. These sanctions may reach up to the greater of 4% of their global turnover or gross income, or up to EUR 20 million.

To be able to demonstrate compliance with the GDPR, the data controller should implement measures, which meet the principles of data protection by design and data protection by default. Privacy by design and by default (Article 25) require data protection measures to be designed into the development of business processes for products and services. Such measures include pseudonymising personal data, by the controller, as soon as possible (Recital 78).

Each member state will establish an independent supervisory authority (SA) to hear and investigate complaints, sanction administrative offenses, etc  
GDPR : severe penalties of up to 4% of worldwide turnover or €20 million

Pseudonymisation : The GDPR refers to pseudonymisation as a process that is required when data are stored (as an alternative to the other option of complete data anonymization)[26] to transform personal data in such a way that the resulting data cannot be attributed to a specific data subject without the use of additional information

A right to be forgotten was replaced by a more limited right of erasure in the version of the GDPR that was adopted by the European Parliament in March 2014.

More info on GDPR : <https://www.imperva.com/data-security/regulation-glossary/gdpr/>

EFTA (European Free Trade Association) is a regional trade organization and free trade area consisting of four European states: Iceland, Liechtenstein, Norway, and Switzerland

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data  
<http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>

Safe Harbor  
<https://en.wikipedia.org/wiki/Safe_harbor_(law)>  
<https://en.wikipedia.org/wiki/International_Safe_Harbor_Privacy_Principles>

Privacy Shield  
The EU–US Privacy Shield is a replacement for the International Safe Harbor Privacy Principles, which were declared invalid by the European Court of Justice in October 2015  
<https://en.wikipedia.org/wiki/EU%E2%80%93US_Privacy_Shield>

— PIPEDA (Personal Information Protection and Electronic Documents Act)  
Is a Canadian law relating to data privacy.  
It governs how private sector organizations collect, use and disclose personal information in the course of commercial business.  
In addition, the Act contains various provisions to facilitate the use of electronic documents.  
The act was also intended to reassure the European Union that the Canadian privacy law was adequate to protect the personal information of European citizens  
<https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/>

— FERPA (Family Educational Rights and Privacy Act)  
Is a Federal law that protects the privacy of student education records.  
FERPA gives parents certain rights with respect to their children’s education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are “eligible students.”  
<https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html?>

— ISO 27018  
ISO/IEC 27018:2014 specifies guidelines based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of PII which might be applicable within the context of the information security risk environment(s) of a provider of public cloud services  
<https://www.iso.org/standard/61498.html>

Numerous federal laws and their related regulations—such as the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Children’s OnlinePrivacy Protection Act of 1998 (COPPA)—contain provisions that pertain to the privacy and the security of personal information

Companies are the custodians of data entrusted to them

——– PCI DSS

PCI : Payment Card Industry

PCI DSS : applies if you store, process or transmit Cardholder information  
PCI DSS is a contractual requirement

QSA : Qualified Security Assessor  
RoC : Report of compliance  
SAQ : Self Assessment Questionnaire

PCI DSS –> Report of Compliance (RoC) if merchant is doing more than 6 millions of transactions a year  
PCI DSS –> Self Assessment Question (SAQ) if merchant is doing less than 6 millions of transactions a year

SAD : Sensitive Authentication Data

If merchant suffer a data breach –> Report of Compliance

PCI DSS  
12 requirements, >280 sub-requirements

1- Install and maintain firewalls + personal firewall on device + written policies  
2- Do not use vendors default password or security settings  
3- Protect Stored Cardholder Data : retain minimum cardholder data, encrypt properly, never store track data CVV2 or PIN  
4- Encrypt transmission of cardholder data across Open network : TLS (instead of SSL) + documented policies + no cardholder data send with email or Impact  
5- Use anti-malware up to date + AV logs  
6- Develop and maintain system : patch regularly, have secure SDLC, use WAF  
7- Restrict access to cardholder data : use access control system  
8- Identify and Authenticate access to system component :s strong password, MFA, documented policies  
9- Restrict physical access to cardholder data  
10- Track and monitor all access. retain logs at least one year : review logs every days  
11- Regularly test security systems and process : have IDS, IPS, pen test..  
12- maintain a policy that addresses Information Security for All personnel : risk assessment, people screening…

PAN :Primary Account Number  
SAD : Sensitive Authentication Data (ex: CVV2 on the card, PIN, )

Assessment every year

ASV : Approved Scanning Vendor (they are approved by PCI SCC)  
a quarterly ASV Scan is a PCI DSS requirement

PFI : PCI Forensic Investigator

—— SOC, SSAE16

AICPA : American Institute of Certified Public Accountants

Cloud provider generally don’t want to share a detailed audit of security controls for the same reason they don’t want to allow physical access.  
Instead the provider is likely to publish an audit assurance statement. A kind of seal of approval  
Currently this usually takes the form of an SOC 3 Audit report.

SOC : Service Organization Control

Example : Microsoft has achieved SOC 1 Type 2, SOC 2 Type 2, and SOC 3 reports. In  
general, the availability of SOC 1 and SOC 2 reports is restricted to customers  
who have signed nondisclosure agreements with Microsoft; the SOC 3 report is  
publicly available (<http://aka.ms/soc3>)

SOC reports are a part of the SSAE reporting format created by the AICPA  
SSAE 16 : Statement on Standards for Attestation Engagements

SOC 1 report are strictly for auditing the financial reporting instruments of a corporation  
SOC 2 report are intended to report audit of any controls on an organization security  
SOC 2 Type 1 : review the design of controls not how they are implemented and maintained or their function  
SOC 2 Type 2 : is extremely detailed and provides information about configuration and implementation  
Cloud provider are trying to restrict this document from wide dissemination  
SOC 3 is the seal of approval : it contains no actual data about the security controls of the audit target and is just an assertion that the audit was conduct and that the target company passed

—- Cloud Security Alliance (CSA) Certifications

CSA STAR Program  
<http://cloudsecurityalliance.org/star>  
<https://cloudsecurityalliance.org/star/#_overview>

CSA STAR is the industry’s most powerful program for security assurance in the cloud. STAR encompasses key principles of transparency, rigorous auditing, and harmonization of standards.

STAR consists of three levels of assurance, which currently cover four unique offerings all based upon a succinct yet comprehensive list of cloud-centric control objectives in the CSA’s Cloud Controls Matrix (CCM)

LEVEL 3 (Continuous Monitoring based certification)  
CSA STAR Continuous Monitoring  
LEVEL 2 (3rd party assessment based Certification) :  
CSA STAR Certification : rigorous third-party independent assessment of the security of a cloud service provider. The technology-neutral certification leverages the requirements of the ISO/IEC 27001:2005 management system standard together with the CSA Cloud Controls Matrix.  
CSA STAR Attestation : is a collaboration between CSA and the AICPA to provide guidelines for CPAs to conduct SOC 2 engagements using criteria from the AICPA (Trust Service Principles, AT 101) and the CSA Cloud Controls Matrix. STAR Attestation provides for rigorous third party independent assessments of cloud providers.  
CSA C-START Assessment : robust third party independent assessment of the security of a cloud service provider for the Greater China market that harmonizes CSA best practices with Chinese national standards.  
LEVEL 1 : CSA STAR Self-Assessment

Example : Microsoft Azure  
<https://www.microsoft.com/en-us/trustcenter/compliance/csa-star-certification>

— Common Criteria Evaluation

EAL : Evaluation Assurance Level  
The Evaluation Assurance Level (EAL1 through EAL7) of an IT product or system is a numerical grade assigned following the completion of a Common Criteria security evaluation, an international standard in effect since 1999. The increasing assurance levels reflect added assurance requirements that must be met to achieve Common Criteria certification  
The EAL level does not measure the security of the system itself, it simply states at what level the system was tested.  
To achieve a particular EAL, the computer system must meet specific assurance requirements. Most of these requirements involve design documentation, design analysis, functional testing, or penetration testing.  
TOE : Target of Evaluation  
Assurance levels :  
– EAL1: Functionally Tested  
– EAL2: Structurally Tested  
– EAL3: Methodically Tested and Checked  
– EAL4: Methodically Designed, Tested and Reviewed –> EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line  
– EAL5: Semi formally Designed and Tested  
– EAL6: Semi formally Verified Design and Tested  
– EAL7: Formally Verified Design and Tested –> applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs.  
Source : <https://en.wikipedia.org/wiki/Evaluation_Assurance_Level>

— EuroCloud Star Audit Certification (ECSA)  
<https://staraudit.org/>  
[https://www.eurocloud.org](https://www.eurocloud.org/)  
The StarAudit scheme evaluates cloud services according to a well-defined and transpa­rent catalogue of criteria. The result of this audit process shows the respective maturity and compliance levels of a service.  
The certification procedure is based on best practices and provides answers to the fundamental questions managers are likely to ask when looking for a suitable cloud service provider. Unlike pure security or data protection audits, it covers the entire range of cloud service functions and validates compliance against the requirements in clearly understandable terms.

— Sarbanes-Oxley  
Sarbanes-Oxley Act (SOX)  
<https://www.sec.org/about/laws/soa2002.pdf>

— FISMA  
Federal Information Security Management Act (FISMA) : is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats  
FISMA assigns specific responsibilities to federal agencies, the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) in order to strengthen information security systems  
<https://searchsecurity.techtarget.com/definition/Federal-Information-Security-Management-Act>  
<https://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act_of_2002>

— FEDRAMP  
The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.  
FedRAMP enables Agencies to rapidly adapt from old, insecure legacy IT to mission-enabling, secure, and cost effective cloud-based IT.  
FedRAMP created and manages a core set of processes to ensure effective, repeatable cloud security for the government  
<https://www.fedramp.gov/>  
ex: <https://www.microsoft.com/en-us/trustcenter/compliance/fedramp>

— HITECH (Health Information Technology for Economic and Clinical Health) Act of 2009  
The HITECH is a legislation that was created to stimulate the adoption of electronic health records (EHR) and the supporting technology in the United States.  
<https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html>

— Personal Data Privacy and Security Act of 2009  
This bill did not come up for debate during the 111th United States Congress and at the end of the 2009-2010 session and never became law  
<https://en.wikipedia.org/wiki/Personal_Data_Privacy_and_Security_Act_of_2009>

SLA : Service Level agreement  
GAAP : Generally Accepted Accounting Principles -> a standard framework of guidelines for financial accounting

ISO/IEC 27036 : The ISO 27036-1 standard provides detailed guidance on implementing the ISO 27002 information security controls that deal with supplier relationships. It addresses the supplier relationship from both the suppliers’ and the acquirers’ points of view.

CSA CCM (Cloud Control Matrix) includes :  
– AICPA Trust Service Criteria  
– PCI-DSS  
\_ BITS Shared Assessments  
– BSI Germany  
– Canada PIPEDA  
– CIS-AWS-Foundation  
– COBIT ==> (Control Objectives for Information and Related Technologies) is a good-practice framework created by international professional association ISACA for information technology (IT) management and IT governance.  
– COPPA ==> Children’s Online Privacy Protection Act  
– CSA Enterprise Architecture (formely Trusted Cloud Initiative)  
– ENISA IAF ===> Cloud Computing Information Assurance Framework  
– EU Data Protection Directive  
– FedRAMP  
– FERPA  
– GAPP ==========> Generally Accepted Privacy Principles is a framework (Canada & USA) <https://en.wikipedia.org/wiki/Generally_Accepted_Privacy_Principles>  
– HIPAA/HITECH  
– HITRUST  
– ISO/IEC 27002  
– ISO/IEC 27017  
– ISO/IEC 27018  
– ITAR =====> International Traffic in Arms Regulations (ITAR) is a United States regulatory regime to restrict and control the export of defense and military related technologies to safeguard U.S. national security and further U.S. foreign policy objectives.  
– Jericho Forum ==> international group working to define and promote de-perimeterisation  
– NIST SP800-53  
– NZISM ===> New Zealand Information Security Manual (NZISM) <https://www.gcsb.govt.nz/publications/the-nz-information-security-manual/>

Intellectual property Protections :  
– Copyright : protect expression of an idea.  
A copyright protects original works of authorship including literary, dramatic, musical, and artistic works, such as poetry, novels, movies, songs, computer software, and architecture  
Lasts 70 years after author’s death  
or 120 years after first publication of a work for hire  
Fair use for : Academic Fair Use, Critique, News Reporting, Scholarly Research…  
U.S Copyright Office  
(c)  
– Trademark : protection of representations of an organization (brand, logo…)  
US Patent and Trademark Office (USPTO) (R)  
State (TM)  
Last into perpetuity until trademark owner use it for commercial purpose  
– Patents : protect intellectual property in the form of invention, process, material  
Patent and Trademark Office (USPTO) (R)  
Last for 20 years from the time of the patent application  
– Trade Secret  
Last into perpetuity until trademark owner use it for commercial purpose

ISO/IEC 27036 Security techniques — Information security for supplier relationships  
<https://www.iso.org/standard/59689.html>

**==== Other**

TCI Reference Model : Trusted Cloud Initiative  
<https://cloudsecurityalliance.org/wp-content/uploads/2011/10/TCI-Reference-Architecture-v1.1.pdf>

ISO/IEC 27001:2013 (Information technology – Security techniques – Information security management systems – Requirements)

ISO/IEC 27002 (Information technology – Security techniques – Code of practice for information security controls)

ISO/IEC 27002 is an information security standard published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC), titled Information technology – Security techniques – Code of practice for information security controls.  
source : <https://en.wikipedia.org/wiki/ISO/IEC_27002>

The official name of ISO/IEC 27017 is Code of practice for information security controls based on ISO/IEC 27002 for cloud services, which means this standard is built upon the existing security controls of ISO 27002.

NIST SP 800-37 : Guide for Applying the Risk Management Framework to Federal Information Systems  
<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-37r1.pdf>

NIST SP 800-53 : Security and Privacy Controls for Federal Information Systems and Organizations  
NIST SP 800-53 is a publication that recommends security requirements & controls for federal information systems and organizations and documents security controls for all US federal information systems, except those designed for national security.  
<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf>