CCSP CLOUD GUARDIANS

A BULLETED LOOK AT THE CRITICAL TOPICS FOR THE (ISC)2 CERTIFIED CLOUD SECURITY PROFESSIONAL EXAM

GWEN BETTWY

CCSP Cloud Guardians

A bulleted look at the critical topics for (ISC)2 Certified Cloud Security Professional exam

Gwen Bettwy

ISBN-13: 9781234567890
ISBN-10: 1477123456

Library of Congress Control Number: 2018675309
Printed in the United States of America

This page left blank intentionally.

Table of Contents

Data Retention
Data Discovery
Data Rights Management (DRM) a.k.a. IRM
Data Security Strategies
Capability Maturity Model Integration (CMMI)
Capability Maturity Model ISO/IEC 21827

Domain 3 - Cloud Platform and Infrastructure Security – 17%

Abstraction layers
Hypervisors
ARCHITECTURE
Service orchestration
Networking Basic
Network Security Group
Data Storage
SAN – storage area network
Network attached storage – NAS
Risk Assessment Tools
Risk Assessment Terms
Risk Assessment Methodologies
Risk Response
Treacherous 12 – Cloud Security Alliance
Egregious 11 – Cloud security alliance
Identity and Access Management
Authorization decisions
SSO – Single sign on
Cloud Access Security Brokers (CASB)
Firewalls
Intrusion Detection System (IDS)
Intrusion Prevention System (IPS)
Designs to improve security controls
Database Activity Monitor (DAM)
File Activity Monitor (FAM)
DLP (Data Leak Prevention)
DRM (Data Rights Management)
Physical Data Center Design

Domain 4 - Cloud Applications Security – 17%

Supply chain management
Software development lifecycle
Software development methodologies
Software testing
CWE/SANS Top 25 Most Dangerous Programming Errors
OWASP Top 10
ISO/IEC 27034 – Security Techniques – application security
Sandboxing
Application Virtualization
Threat Modeling
Orchestration Tools

Domain 5 - Operations – 17%

Data Center Tiers
Operations and Maintenance of Systems
Preventing successful attacks
Security Operations Center (SOC)
ITIL/ISO/IEC 20000
Packet Capture
Logging of Events
Security Information and Event Management (SIEM)
Data and Media Sanitization
When it all goes wrong
Planning for Eventualities

Domain 6 -Legal and Compliance – 13%

Privacy
AICPA/CICA Privacy Maturity Model
PCI-DSS (Payment Card Industry – Data Security Standards
Industrial Control Systems (ICS)
Audits
Gap Analysis
Forensics
Basic Forensics Rules

Domain 1 - Cloud Concepts, Architecture and Design – 17%

According to NIST the cloud can be explained by:

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models. *(NIST, 2011)*(NIST SP 800-145 2)

- ISO/IEC 17788 and NIST SP 800-145 define the basics of cloud
- NIST SP 800-146 is a Cloud Computing Synopsis and Recommendation
- ISO/IEC 17789 is the Cloud Computing Reference Architecture (CCRA)
- NIST SP 500-299 is the Cloud Computing Security Reference Architecture

All 5 of these documents are publicly available and good reads/references.

Service Capabilities(ISO)/Service models(NIST)

"This is a classification of the functionality provided by a cloud service." (International Standards Organization, 2014)

There is little overlap between these three.

1. SaaS – Software as a Service – an application e.g. Dropbox, Office 365. The customer has access to Enterprise apps, Desktop apps, Mobile apps.
2. PaaS – Platform as a Service – a platform. e.g. Windows Server. The customer has access to development and runtime tools and environment
3. IaaS – Infrastructure as a Service – e.g. processing, storage or networking resources – a virtual Data Center. The customer has access to CPU, disk drives, networks and data centers.

Cloud Service Categories as defined by ISO 17788

ISO/IEC 17788 defines the following as "a group of cloud services that possess some common set of capabilities"

CaaS – Communications as a Service. Real time interaction and collaboration

CompaaS – Compute as a Service. Processing resources to run software.

DSaaS – Data Storage as a Service. Data storage

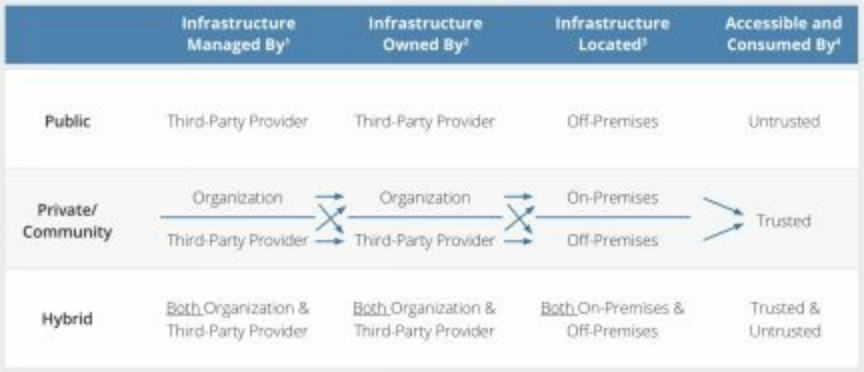
NaaS – Network as a Service. Transport connectivity and related network capabilities

	Cloud Capabilities Type		
Cloud service categories	Infrastructure	Platform	Software
Compute aaS	X		
Communications aaS		X	X
Data Storage aaS	X	X	X
Infrastructure aaS	X		
Network aaS	X	X	X
Platform aaS		X	
Software aaS			X

Deployment Models

1. Public cloud – potentially available to any cloud customer
2. Private cloud – used exclusively by a single cloud customer
3. Community cloud – shared by a specific collection of cloud customers
4. Hybrid cloud – a combination of at least two of the above three deployment models

The following picture is from the CSA Guidance 4.0 (Cloud Security Alliance, 2017)



Essential Characteristics

1. On-demand self-service – customer can provision computing capabilities as needed or with minimal service provider interaction.
2. Broad network access – resources are available over a network and accessed through standard mechanisms
3. Resource pooling – resources are aggregated and used to serve one or more cloud customers
4. Rapid elasticity and scalability – physical or virtual resources rapidly adjusted, often automatically, to increase or decrease resources
5. Measured service – pay only for the resources the customer uses
6. Multi-tenancy – physical and virtual resources in a way that multiple customers and their computations and data are isolated from and inaccessible to each other

Drivers to move to the cloud and major changes

1. Shift from CapEx to OpEx

2. Shift from Infrastructure centric to Data centric

Contracts, SLA, PLA, MSA

This is a topic that carries through all cloud discussions. Just about any question that starts with 'Can I have…?" or 'Tell me what my billing is based on…?", or so many others are answered with "Well it depends on your contract".

- In order to have the service level that you need…
- In order to fully comprehend your billing…
- In order to have your data protected as required by Law or Policy…
- In order to be able to obtain forensic evidence when needed…
- In order to….
    - It must be documented within your Contract or related documents.
        - Master Services Agreement (MSA)
            - Defines the working relationship between two entities
        - Service Level Agreement (SLA)
            - Defines the specific measurable level of service required/promised/needed
        - Privacy Level Agreement (PLA)
            - Defines the Providers responsibility in protecting the privacy of the data
            - Under GDPR this would be the Data Processing Agreement (DPA) ..???

Building Block Technologies

Building cloud is a lot of work if you are on the cloud provider side or if you are building your own private cloud. The fundamentals of the networks begin the same with Servers, Routers, Switches and all of the security devices from Firewalls to Intrusion Detection Systems and Intrusion Prevention Systems. Then add all of the software controls such as Anti-Malware, Anti-Bot, Anti-Rootkit, Data Leak Prevention and Data Rights Management. Oh and don't forget to build a data storage network (SAN). It's a lot, right?! Then the real work begins to build the cloud with virtualization, abstraction

layers, containers.

This is all explored in domains further on in this guide. For now, just know we have a lot to get through to understand this, even at its most basic levels.

Cloud computing roles

If you can remove the word “cloud” from the front of these terms and you know what it is… you are there.

- Cloud service customer – consumer of cloud services a.k.a. tenant or user
- Cloud service provider – company that provides cloud services
- Cloud service partner – provides services to customer or provider e.g. auditor, reseller
- Cloud auditor – verifies the security controls of a cloud service provider
- Cloud reseller – Resells the services of a single company e.g. Office 365 Reseller
- Cloud architect – designs a corporation’s approach to the cloud
- Cloud administrator – builds a clouds structure according to the architect’s design
- Cloud operator – manages cloud technology on a day to day basis
- Cloud Application Architect – designs applications for use within a cloud architecture
- Cloud Developer – the coder that creates applications according to its design
- Cloud Data Architect – designs the structures for storing and using data within the cloud
- Cloud Storage Administrator – builds cloud data storage according to the design from the architect
- Cloud Services Manager – watches over cloud services to ensure that SLAs are being met
- Cloud Computing Reseller – See reseller above
- Cloud Backup Service Provider – data backup cloud provider
- Cloud Services Broker – Negotiates services between providers and customers

- Cloud Security Architect – designs the security of the cloud to meet corporate strategy and governance
- Cloud Security Operator – manages security on a daily basis, probably from the security operations center (SOC)
- Cloud Carrier – the provider that connects the corporate location to the Internet. Such as a DSL or MPLS provider

Now I have to tell you of a term that I find hysterical. I have said for years that we are just taking terminology and adding the word CLOUD to anything and you have a new term. The term for this is Cloud Washing!

Governance, Risk Management and Compliance (GRC)

- This may be one of those **hidden secrets**. Hidden for an unknown reason. This test is a management test. If you begin at the highest level of a corporation there should be a strategy that has been created by senior management for the corporation to follow.
- The corporate strategy leads to the governance structure of the business.
- The governance of a business should be used to create the security governance.
- Once the security governance has been created it is possible to begin the work of creating an Information Security Management System (ISMS). The ISMS terminology comes from ISO/IEC 27001. It is not necessary to use this document, but it might be a very good idea to look into it.
- It is necessary to first use ISO/IEC 27002. I encounter a lot of people that say to me that is not where you start, but the truth is it is. ISO/IEC 27002 is a document of security controls. You cannot use ISO/IEC 27001 to build a security program without knowing security controls first. The process of learning security controls is the process of learning ISO/IEC 27002
- Alternatively NIST SP 800-53 is also a list of all security controls similar to ISO/IEC 27002
- ISMS could be alternately known as a Security Program. The security program is full of documents to guide a business to create its security presence. The program is comprised of the following

documents:

- Policy – Expression of senior management of their intentions and direction
- Standards – written document stating the authorized security actions. can be created either internally or externally, compliance is mandatory either way
- Baselines – a starting point to use for comparison / minimum security settings and configuration
- Procedures – written step-by-step actions to accomplish a task
- Guidelines – a set of recommendations and good practices typically informative, but not mandatory in nature

Enterprise Security Architecture (ESA)

This is arguably an alternate name for the process of creating a security program through GRC

ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002

These documents are used to create an Information Security Management System (not computer based, more project based) within a corporation. You could think of this as fundamentally a security program within a business. Everything from the Policy that guides all security activity to the selection of every vendor product should be carefully and logically controlled. These documents give you that logic

- ISO/IEC 27000 is an overview and glossary
- ISO/IEC 27002 contains a list of all security terms/tools/technologies (you could think of this as being similar to sitting through a CISSP class and all of the topics covered)
- ISO/IEC 27001 is the tool to create the ISMS. It is also perfect for auditing and certifying an organization and their security program
- ISMS is defined in 27001 as consisting of 'Policies, Procedure, Guidelines and associated resources and activities collectively managed by on organization" in order to protect the corporate assets

ISO/IEC 27017

This is the Code of practice for information security controls based on ISO/IEC 27002 for cloud services. It is a subset of all of the controls that is found inside of ISO/IEC 27002.

Implementation Models

- Managed Service Provider – Contract negotiation for cloud service where the IT department jobs would be handled by the MSP
- Cloud Service Provider – Standard offerings – usually defined as SaaS as a distinction from MSP

Impact of Related Technologies

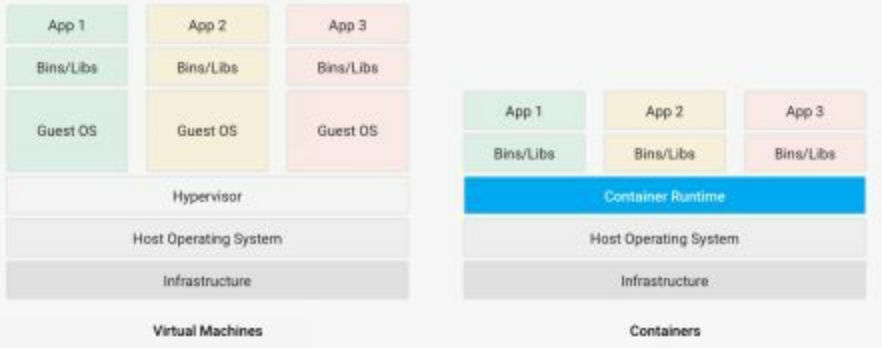
With cloud technology and its capabilities the impact it is having on business requirements is amazing. The scalability allows business access to expanded CPU cycles when needed. The technologies that this has had an impact on include:

- Artificial Intelligence - AI is aiming at the ability of computers to duplicate the thought process of a human brain. While we work on getting there at least they can approximate the learning, reasoning and problem solving capabilities of humans.
- Machine learning - Simply defined as the ability for computers to learn using algorithms rather than be specifically programmed to do something. This is arguably a subset of AI.
    - Supervised learning – taught from known outputs
    - Unsupervised learning – The computer and its algorithms must find patterns in the data on their own.
    - Reinforced learning – The computer and its algorithms are rewarded or reprimanded for its actions
    - (Wellers, 2019)
- Blockchain - A timestamped series of unalterable record of data. The blocks of data are bounds to each other using cryptographic principles. (Rosic, 2016)
- Internet of Things - A giant network of connected things like computers, light bulbs, drilling rigs, tweeting kettles and so on.

- Quantum Computing - These rely on qubits or quantum bits to store information rather than traditional bits in todays computer. These qubits must be kept very cold (near absolute zero) so as to now have errors introduced by heat. “This all relies on the mechanical phenomenon of superposition and entanglement to create states that scale exponentially” (IBM, 2019)

Virtualization

- Hypervisor – Is software that allows for the creation of pools of resources that are used to create virtual machines.
- Hypervisor Type 1 – Often referred to as Bare Metal because it IS the operating system installed directly on the hardware of a server
- Hypervisor Type 2 – This runs on top of another OS. It then allows the creation of virtual machines
- Containers – Allow for a lighter weight method of developing and running applications than virtual environments that involve VMs and hypervisors. Requires a Linux kernel for the container to connect into.



(Google LLC, n.d.)

- Application virtualization – Two that ISC2 mentions, App-V and WINE. App-V allows the running of Linux programs on a Windows computer. WINE works on MAC OS to allow for Windows applications to be run there.

Threats

It is always critical to think about and understand the threats to our information systems. Most threats come from malicious actors, but defiantly not all. Some come from simply being at the wrong place at the wrong time.
Provider Lock-in – Once the creation of the virtual machines is done and the customers data is in the cloud there is no straightforward way out. They have locked you in due to contract or proprietary formats.

Provider Lock-out – Occurs when a provider goes bankrupt and the customers VMs and data are stuck inside.

Provider exit – When the cloud provider decides to sell off or shut down the cloud service.

Guest escape – An attacker able to get out of the guest operating system and land in the hypervisor.

Guest hopping - An attacker moving from one VM to another. From one cloud customer to another

Lack of Due Diligence - Getting into the cloud without care.

Man-in-the-Cloud (MITC) (Imperva, Inc., 2015) - Hacker steals/obtains copy of synchronization token for online synchronized storage system

HyperJacking – Hijacking the hypervisor

Controls

Control Types

- Administrative/Managerial - written or orally communicated controls such as a policy
- Technical/Logical - security controls executed in the hardware and or software mechanisms of a system. see technical control
- Physical - tangible control, such as a lock or guard

Control Categories

- Preventive - controls deployed to avert or stop unauthorized and/or undesired actions
- Deterrent - used to discourage desire to perform an action, e.g. the part of a policy that states that negative actions will be taken against individuals who violate the policy
- Detective - to record or alert, often used to inform security personnel that an event occurred, e.g. a log file
- Corrective - to stop bad behavior from continuing or to restore to a functional condition, not usually to normal, just simply working. e.g. UPS, diesel generator
- Recovery - to return to a normal condition e.g. restoring from backup
- Directive - controls that have a specific consequence if they are not followed. e.g. a policy that states failure to comply could result in anything up to and including termination of employment
- Compensating - a control designed to make up for a deficiency or lack of another existing control

Trusted Cloud Initiative (TCI)

Reference Architecture – CSA defines this as "comprehensive approach for the architecture of a secure, identity-aware cloud infrastructure". It is designed to assist through a methodology and set of tools to design and assess security in the cloud. Divided into 4 columns:

- BOSS – Business Operation Support Services
  - Points to SABSA – Sherwood Applied Business Security Architecture
    - SABSA – Security architecture and management framework
- ITOS – Information Technology Operation and Support
  - Points to ITIL
    - ITIL – IT service management tool
- Services – Presentation, Application, Information and Infrastructure
  - Points to TOGAF – The Open Group Architecture

Framework
        - TOGAF – framework for designing and managing enterprise architecture
- Security and Risk Management
    - Points to Jericho from The Open Group
        - Jericho – Forum and tools for defining and promoting de-perimeterization
        - Jericho has a cube formation to describe the approach to the cloud. There are four sides to this cube:
            - Perimiterization or de-perimerterized
                - Clearly defined edges to the network, or not
            - External or Internal
                - Inside (Internal) or the organizations physical boundaries, or not
            - In-Source or Out-Source
                - Create the cloud with the personnel within your business (In-Source) or hire someone else (out-source)
            - Proprietary or Open
                - Use a HV with vendor specific code (proprietary) or use open code that is customizable (open)

NIST SP 500-299

From the NIST cloud security working group. A framework to identify and define security controls for the cloud

ISO/IEC 15408 – Common Criteria – Evaluation criteria for IT security

CC is used to evaluate security products. Vendors submit their products to approved test labs. Common criteria is a standardized test methodology so

that a situation such as a Cisco FW and a Checkpoint FW can be tested by two different labs in 2 different countries, but the test results can be compared to determine the best FW for a given use.

- Protection Profile (PP) establishes the category of the product
- Target of Evaluation (TOE) identifies the exact product being tested
- Security Target (ST) establishes the conditions of the test
- Evaluation Assurance Level is the resultant grade

- EAL 1 – Functionally tested
- EAL 2 – Structurally tested
- EAL 3 – Methodically tested and checked
- EAL 4 – Methodically designed tested and reviewed
- EAL 5 – Semi-formally designed and tested
- EAL 6 – Semi-formally verified design and tested
- EAL 7 – Formally verified design and tested

FIPS 140-2 - Security Requirements for Cryptographic Modules

A standard for the quality of physical security that must be within a cryptographic module within a system.

1. Level 1 – Lowest level. Must have basic security requirements such as an approved algorithm but **NO** physical security mechanisms. (e.g. MACOS High Sierra 10.13 T2)
2. Level 2 – level 1 plus **tamper evident** coatings or seals (e.g. MAC OS Mojave 10.14 T2 chip)
3. Level 3 – level 2 plus attempts to prevent the intruder from gaining access such as **tamper detection/response** circuitry that zeroizes the data/key when the cover is removed (e.g. Thales TSPP in payShield 9000)
4. Level 4 – level 3 plus complete protection with a high level of probability of detecting and responding to attempts at physical access that results in the immediate zeroization of data/keys. **Tamper active**.

Critical Security Terms

As with all certification exams it is necessary to have a strong comprehension of the words used within that industry. I highly recommend that you work on words such as those below throughout all 6 domains.

The following terms are defied in ISO/IEC 17788

- Availability – Property of being accessible and usable upon demand by an authorized entity
- Confidentiality - Property that information is not made available or disclosed to unauthorized individuals, entities, or processes
- Integrity - Property of accuracy and completeness
- Interoperability - The ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged
- Portability – Ability to easily transfer data from one system to another without being required to re-enter the data
- Reversibility - Process for cloud service customers to retrieve their cloud service customer data and application artifacts and for the cloud service provider to delete all cloud service customer data as well as contractually specified cloud service derived data after an agreed period
- Security – Preservation of confidentiality, integrity and availability of information
- Tenant - One or more cloud service users sharing access to a set of physical and virtual resources
- Auditability - The capability of collecting and making available necessary evidential information related to the operation and use of a cloud service, for the purpose of conducting an audit
- Governance - The system by which the provision and use of cloud services are directed and controlled
- Interoperability - The ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged.
- Maintenance - refers to changes to a cloud service or the resources it uses in order to fix faults or in order to upgrade or extend capabilities for business reasons

- Performance - A set of behaviors relating to the operation of a cloud service, and having metrics defined in a SLA
- Resiliency - Ability of a system to provide and maintain an acceptable level of service in the face of faults (unintentional, intentional, or naturally caused) affecting normal operation
- Versioning - Versioning implies the appropriate labelling of a service so that it is clear to the cloud service customer that a particular version is in use

Additional Terms

- Separation of Duties (Segregation of Duties) – To split a task amongst at least 2 people in order to prevent fraud since one person cannot complete the task by themselves.
- Dual Control – in concert, together, accomplish a task
- Privacy - Most commonly associated with the confidentiality of Personally Identifiable Information (PII)

Domain 2 - Cloud Data Security – 19%

Data, the golden core of our businesses that we are protecting. I am thrilled that there is, finally, there is a domain dedicated to Data. The place to start our conversation is with its lifecycle. As with everything else there is a beginning and an end.

Data Life Cycle

Data must first be created. Data is not just word documents. Data is created by humans and by machines. Logs are just as much 'data' as is a 'word document'. Here is the Data Life Cycle as defined by CSA in their guidance 4.0

1. Create – Generation or alteration/updating or modifying content
    1. Data should be classified at this point
2. Store – Committing to storage repository – nearly simultaneous with create
3. Use – Viewed, processed or used (not modification)
4. Share – Made accessible to others
5. Archive -Leaves active use and enters long term storage
6. Destroy – Permanently destroyed using physical or digital means

Functions, Actors and Controls

- Functions include Access, Process, and Store
    - Access occurs at every step of the data life cycle
    - Process occurs at only two steps of the data life cycle:
        - Create and Use
        - The data is being used in a transaction,

updated, or just viewed
    - Storage occurs at two steps of the data life cycle. Probably quite obviously:
        - Store and Archive
        - This data is held for future use or verification, etc.
- Actors is person, application, system/process
- Controls possible actions

Information Classification

What we should do is classify the data as soon as its created. That would be optimal. Instead we might just have to classify it when we find it…

Classification is the identification and labeling of the sensitivity of our data. Classification schemas must have at least 2 different level to be able to distinguish the sensitivity of data. These levels should be identified with words that assist the users in handling the data appropriately.

Familiar identifiers for sensitivity levels include words like secret, sensitive, public, or top secret

API – Application Programming Interface

- APIs are fundamentally a request and response protocol. They are used throughout cloud extensively, not just for customer apps, but also for the fundamental building blocks of cloud to be able to function.
- APIs are not new, but their prevalence has raised them to the top of lists that describe attack prevalence. The more we know and understand them the better we can use them properly
- The two types of APIs that are in use are:

- SOAP (Formerly Simple Object Access Protocol (it's not simple))
    - Heavy and complicated
    - Has many features
    - XML based

    - Has encryption capabilities built in
- REST – REpresenational State Transfer
    - Lighter protocol
    - Uniform Resource Indicator (URI) based
        - Uniform Resource Locator (URL)
            - Identifies the location or domain name such as "https://ISC2.org/Certifications/CCSP
        - URI
            - Identifies a particular resource such as "CCSP" in the above URL
    - Uses JSON (JavaScript Object Notation) or XML
    - Can be encrypted through the addition of TLS

Data structure

- Structured data is something like a database. Each record within a table can be connected (RDBMS) to another record in another table. This data works best in block storage.
- Unstructured data is data that does not have any relationship to each other. This type of data would be something like an email, an invoice, a word document, a picture, etc. This type of data is best stored in object storage.

Data storage

See chapter 3 – Cloud Platform and Infrastructure Security

Data terms

- Database – collection of data in an organized (structured/relational) format
- Metadata – data regarding data, describes additional information about data such as how and when data was collected and how it has been processed
- Big Data – "consists of extensive datasets_primarily in the

characteristics of volume, variety, velocity, and/or variability_that require a scalable architecture for efficient storage, manipulation, and analysis" (NIST SP 1500-1 A-1)

- The three Vs of Big Data:
  - Volume – size of the dataset
  - Variety – data from multiple sources
  - Velocity – rate of flow
  - Variability – change in other characteristics – (the other V)

Data Retention

A data retention policy should be created. Truly it should be a part of a larger policy regarding data and its structure and storage.

- Data deletion – If data is not required, or must legally remove according to the law
- Data archiving – Holding data for long periods
- Legal hold – A requirement to store and protect data until a judge makes a decision regarding issuing a warrant

Data Discovery

So now the question is how we find data. Location is only one question. We must also understand what kind of data we have and its quality and sensitivity. We are now on the edge of what we should probably call 'Data Science' that Dean Saxenian from UC Berkley has stated 'should not just be about the tools. It's also using the tools in a way that allows you to solve problems and make sense of data in a systematic way. (Staff, 2019)

From the point of view of the CCSP truly comprehending the data and turning it into useful information is not our job. Yet if we do not help those who do locate their data, we have not done our job.

Tools:
Content analysis

Data Rights Management (DRM) a.k.a. IRM

DRM controls access to files through

- Control is agnostic to location
- Access controlled through application such as Kindle or iTunes
- Information Rights Management for corporate data such as LockLizard
- Audit trail created

Control:

- Print capability
- Screen shot capability
- Watermarked visible on screen or on printed version if allowed
- Automatic expiration
- Access control list or Role Based Access Control
- Copy/paste restriction

Data Security Strategies

- This is the core to this domain. This is a security exam. There are fundamentally two things that are used nearly universally is encryption and access control.
- Encryption
    - Data at Rest
        - Based on the design of the software
        - A single file can be encrypted
        - A partition can be encryption
        - A folder can be encrypted
        - An entire drive can be encrypted
        - An instance can be encrypted
    - Data in Transit
        - SSH – Secure Shell. Layer 5
            - Perfect for Administrative connections to Routers, Switches, etc.

        - Can be used for VPN
    - TLS (formerly SSL). Transport layer security. Layer 4
        - Client – Server structure
        - Most commonly used for Web site connection (HTTPS)
        - Can be used for VPN
    - IPSec – IP Security. Layer 3
        - Can be used for anything
        - Great for site to site (Router to Router) connections
        - Can be used for VPN
- Data in Use – Keep data encrypted while in use. Theoretical/Partially theoretical. Work is being done to figure out how to keep data encrypted while it is being used. This would be most useful when processing something like credit cards through a transactional database. The encryption methodology that applies to this is known as homomorphic cryptography.

- Key Storage – location is critical
    - Primary site location is with the customer NOT the cloud provider
    - Should be stored securely NOT in a VM. If the key is stored in the VM that means that it would be saved in the object-based file that is the VM.
        - Store in HSM or TPM
    - Trusted Platform Module (TPM)
        - Designed for one thing. Security of the Key
        - A chip that is mounted on a mother board
    - Hardware Security Module (HSM)
        - Designed for one thing. Security of the Key. It can be used to create keys or store keys. Access to the HSM should be physically limited. Logical and physical controls need to be built into the box itself.
        - Key ceremonies are used to generate or duplicate keys

        - Rack mountable
        - Test against FIPS 140-2
- CSKM, RKM, IM, EM
- Key management interoperability protocol specification
- Masking – To hide data from visibility to the user (stars instead of password)
- Tokenization – To replace data with another value. Requires another database that stores the original and the token version to convert back to original data value. Great for credit card numbers in transit
- Anonymization – To remove sensitive data. This process is not reversible.
- Obfuscation – To confuse by obscuring data. Think about the font of "Wingdings". If you convert normal text to Wingdings than it is
- Digital Rights Management (DRM) – a.k.a. Information Rights Management. Control over intellectually property such as music or course content.

Capability Maturity Model Integration (CMMI)

The CMM Institute describes CMMI v2.0 as a proven set of global best practices that enables organizations to build and benchmark the key capabilities that address the most common business challenges *(CMMI Institute, 2019)*

Measurement of maturity levels towards a mature software process.

- Level 0 – Incomplete. Ad-hoc and unknown
- Level 1 – Initial. Process unpredictable, reactive
- Level 2 – Managed. Process characterized for projects and reactive
- Level 3 – Defined. Process characterized for the organization and proactive
- Level 4 – Quantitatively managed. Process measured and controlled
- Level 5 – Optimizing. Focus on continuous process improvement

Capability Maturity Model ISO/IEC 21827

ISO/IEC 21827 describes itself as ‘standard metric for security engineering practices covering … the entire life cycle… the whole organization’. This standard is used, hopefully with, ‘The objective is to facilitate an increase of maturity of the security engineering processes within the organization’. (ISO/IEC, 2008)

Levels:

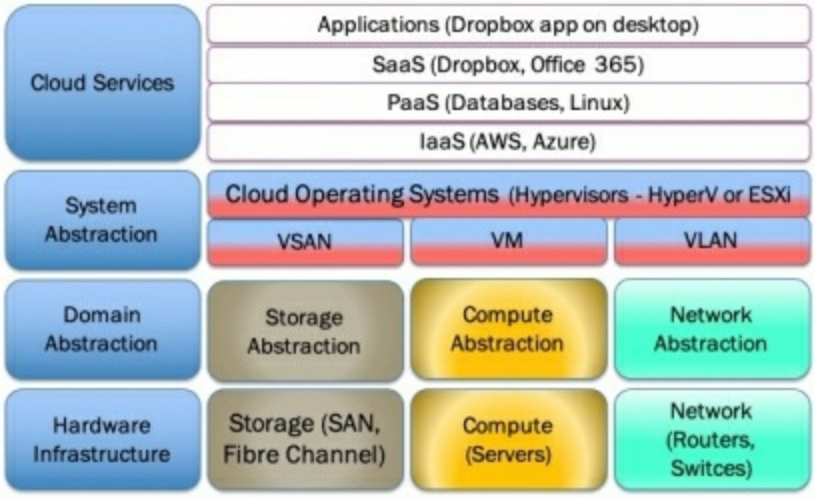
- Level 1 – Performed Informally
- Level 2 – Planned and Tracked
- Level 3 – Well Defined
- Level 4 – Quantitatively Controlled
- Level 5 – Continuously Improving

Domain 3 - Cloud Platform and Infrastructure Security – 17%

As the blog from Stragi states we are on the correct path to getting ready to be a CCSP. They said 'The key to understanding cloud computing is to not focus on any one definition, but to look at the common underlying attributes and characteristics of the technologies or concepts described within the definitions' (Strategi, 2009). That is from 2009 and I believe we are still seriously working on our understanding. Let's start with abstraction. The foundation to the creation of today's cloud. (Strategi, 2009)

Abstraction layers

Abstraction – Considered separate and apart from solid existence



The first level of abstraction is at the Domain level. There you have:

- Storage abstraction breaks the actual storage on drives down into

block or object storage

- Compute abstraction creates the ability to create VMs
- Network abstraction creates the ability to identify virtualized networks within a server

- Compute – Processing capability
- Network – Transmission capability
- Storage – Retention of data capability

Hypervisors

Type 1 – Bare Metal. It is the OS.
Type 2 – Requires a base OS to be loaded on top of

ARCHITECTURE

Physical – The actual hardware e.g. router, switch, server
Logical – The breakdown into the 4 layers of the architecture

- Applistructure – The deployed application and its underlying services e.g. message queues
- Infostructure – This is the structure of the actual data. SAN, vSAN
- Metastructure – This is where you encounter the visualizing of the physical. Everything from the hypervisor to virtual machines are found here.
- Infrastructure – This is the underlying physical structure to the cloud. It is comprised of switches, servers, routers, etc.

Service orchestration

NIST SP 500-292 defines the three layers of cloud service orchestration.

- The lowest layer is the physical layer which represents all of the hardware resources, e.g. router, switch, server, etc.
- The middle layer is the resource abstractions and control layer.
    - Resource abstraction includes the necessary elements to

manage the physical such as the hypervisor, virtual machines, virtual storage, etc.
    - Control element includes things like IAM, usage monitoring, resource pooling, etc.
- The top layer is the service layer. This is where you will find the cloud providers creating and providing their interfaces to SaaS, PaaS, IaaS.

Networking Basic

- **Switch** –A device found in the core and at the edge of networks. It is used to make quick decisions on the direction a frame or packet should be sent. The switch looks it up in the forwarding table.
- **MAC address** – A type of address used within LANs to identity devices. It is not globally significant so a switch will listen and remember where MAC addresses are currently on the network. A switch forwards based on MAC addresses when it is operating at L2.
- **VLAN** – Virtual Local Area Network. Emulates a LAN. Broadcast packets are forwarded within a LAN/VLAN. Often thought of as an element of security but all that is needed to move between VLANs is a router.
- **Routers** – Make routing decisions based on their knowledge of the network. Routers learn the network by talking to each other using a routing protocol such as OSPF or RIP
- **IP** – Internet Protocol is a L3 addressing structure. Currently we are using v4 and v6 on the planet. These addresses are globally significant, which is why routers can use them to make decisions on the route that a packet will take.
    - IPv4 addresses are 4 bytes/octets or 32 bits in length
    - IPv6 addresses are 16 bytes/octets or 128 bits in length
- **DHCP** – Dynamic Host Configuration Protocol is used to dynamically assign IP addresses to devices on a network.
- **SDN** – Software Defined Networking, a.k.a. SD-WAN, is a method of managing switches within a network. A SDN alleviates the switches work of making forwarding decision and places that

burden on a controller node. This effectively divides a switches work into two roles. The control plane and the data plane. The control plane allows the switch to request a decision to be made by the controller. The decision is sent from the controller to the switch. The data plane of the switch then forwards the data as usual. The controller allows for a single point of control within a network which is useful for management, security, and a host of many other benefits. SDN is typically found within the physical network (not virtual) at a cloud or service provider today.

- There are 5 planes within SDN. The first two may be the most important to know here are
  - Control Plane
    - The control plane is where the switches communicate with the controller to make forwarding decisions
  - Data Plane
    - The data plane is how and where user traffic is forwarded to the correct destination.
    - Data refers to: Data, Voice and Video, generically

- **DNS** – Domain Name System will convert the name/URI that the user is attempting to access into an IP address for transmission
- **DNSSec** – Domain Name System Security adds security to DNS a) origin authentication of DNS data, b) data integrity, and c) authenticated denial of existence. Designed to protect against attacks such as Cache poisoning.
- **VPN** – Virtual Private Networks are used to control the flow of traffic. VPNs are commonly used to identify traffic from one department or another for control purposes
- **OS Hardening** – Operating Systems need to be hardened or secured to minimize the attack surface.
  - Keep the system patched
  - Remove default account
  - If default account cannot be removed, then rename
  - Change the DEFAULT password!!!!!

    - Shut down unnecessary services
    - Close unused ports
- **Redundant Servers** are installed with one server actively processing data and the other passively waiting to be needed. So, the servers are active/passive
- **Server Clusters** install server with both/all actively handling or processing data. So, the servers are active/active
    - **Distributed Resource Scheduling (DRS)**
    - **Dynamic Optimization (DO)**
    -

Network Security Group

Microsoft is using NSGs to secure traffic flow within. It is a little bit of Firewall logic and a little bit of VLAN logic combined together. It is granular control for a virtual network.

Data Storage

There are fundamentally two ways to look at how data is stored within the cloud. The language changes as you move from IaaS to PaaS to SaaS

.

PaaS	Structured Data	Unstructured Data
	Block	Blob
IaaS	Volume	Object (file)
	Database	Big data

- **Block Storage** – This is perfect for something like a database. Data will be stored in volumes and blocks. The file or the data is split into equal sized pieces (blocks). A block is able to be located but does not have associated metadata with it.
- **Object Storage** – Storage of a piece of data at a time. Each object could be a file, video, picture, etc. Object storage is not a hierarchical storage like file storage is. Each object is stored with metadata and a unique identifier that allows it to be located.
- **Bucket** Storage is a type of Object storage.
- **Blob -** A bucket of sorts

- **Image** storage, an image is a type of Object. All VMs are stored as an image, which is a type of file.
- **Ephemeral** storage is temporary. It exists as long as the VM is running.

SAN – storage area network

Where do we store all of this data? The more we have, the more we need a SAN. You can think of a SAN as many massive drives attached to a LAN that is dedicated to this purpose. Therefore – SAN. In order to move the massive quantities of data across the network it is best to use fiber. With fiber comes a change in the protocol to something like Fibre Channel.

- Fibre Channel – Distinct protocol. Uses a different addressing scheme of LUNs (Logical Unit Number)
  - If necessary Fibre Channel can be run across Ethernet therefore FCoE
- iSCSI – SCSI (Small Computer System Interface) protocol run over TCP/IP. SCSI is a protocol developed by ANSI for attaching something like a printer to a computer. iSCSI then adapts SCSI to run over an IP network. There is a requirement for the identification of an iSCSI Target and the iSCSI initiator

Network attached storage – NAS

NAS is a server or data storage device attached to a network. The most common method of managing the data found on this device would most likely be a hierarchal file storage, although there are always options.

- RAID (Redundant Array of Independent Discs) is a tool that is designed to prevent a server from failure when a hard drive fails. There are many versions of RAID although the most common are probably RAID 1 and 5.
  - RAID 0 stripes data across many drives. Fast to write but a drive failure will cause data loss
  - RAID 1 mirrors the data to a second drive, drive failure will not cause data loss

    - RAID 5 stripes data across multiple drives. Parity info is also created for every block of data written to a drive, Parity is stored on a different drive. If a drive fails the lost data can be recreated from the parity.
- Erasure Coding emulates RAID in the cloud. Data is stored across multiple drives, but there are in different servers, possibly in different data centers. Then parity is created and stored separate from the block of data that it applies to.

Virtualization
Management Plane

Risk Assessment Tools

- ISO 31000 – Risk Management
- ISO/IEC 27005 – Information Security Risk Management
- NIST SP 800-37 - Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach
- NIST RMF – Risk Management Framework
- ENISA Information Assurance Framework – European cloud specific risk assessment

Risk Assessment Terms

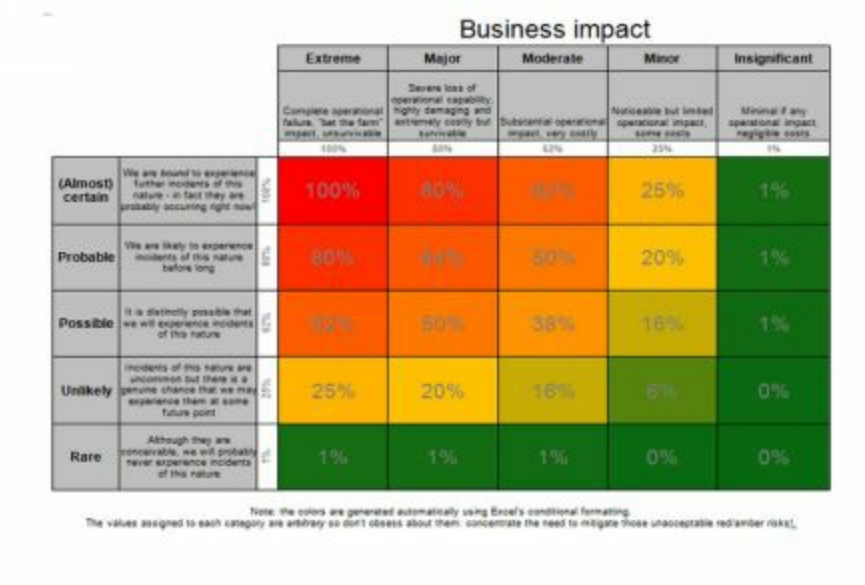
- Risk Appetite – the risk an organization is prepared to pursue, retrain or take by amount and type ~ ISO 31000
- Risk Tolerance – is the variance around objectives
- Risk Profile - the risk an organization can tolerate
- Asset – Something of value. (e.g. laptop)
- Threat – Harm that can occur to an asset impacting CIA (e.g. laptop can be stolen)
- Threat Source – is the who or what that causes the threat to be exploited (e.g. thief that stole laptop)
- Vulnerability – A weakness or flaw that must be exploitable. It is not possible for the threat to occur if the vulnerability is not there or

not exploitable. (e.g. laptop is small and lightweight making it easy to steal)

- Impact – This is the extent of the damage caused by this threat being exploited. (e.g. loss of productivity, compromise of sensitive data, etc.)
- Attack /Exploit– This is the actual exploitation. It takes this from a theoretical topic to real. It is happening right now or sometime in the past. (e.g. The thief walks into the room and takes the laptop)
- Likelihood – This is the chance that this attack is possible.
- Risk – The knowledge of the combination of Likelihood and Impact
- Control – Knowing that certain exploits are possible we do things to reduce the likelihood or the impact.
    - Safeguard – A safeguard works to reduce the chance of the attack occurring. (e.g. laptop lock)
    - Countermeasure – This is the type of control we put in place to reduce the impact of the attack. (e.g. A backup laptop with data backups performed regularly)

Risk Assessment Methodologies

- Quantitative
    - To assess the financial impact of specific threat events
    - Uses formulas to calculate the financial impact
    - If an incident occurred once…
        - Single loss expectancy (SLE) = Asset value (AV)* Exposure Factor (EF)
    - How many times does this occur a year?
        - Annual rate of occurrence (ARO)
    - Therefore, the annual cost is
        - Annualized Loss Expectancy (ALE) = SLE * ARO
- Qualitative
    - To assess the level of priority a threat should be assigned



(ISO/IEC, 2018)

Risk Response

- Risk Reduction/Mitigation - To apply controls to minimize the impact or likelihood
- Risk Transference/Sharing – Involving someone else in the recovery if a risk is realized, e.g. Insurance.
- Risk Avoidance - When a risk is determined to be too great that activity should not be started. If the business is already engaged in then it should be stopped.
- Risk Acceptance – No matter what else is done in response to Risk there is always at least a small likelihood of some impact. That risk must be accepted by management.

Treacherous 12 – Cloud Security Alliance

The Cloud Security Alliance defined the top 12 cloud computing threats in February 2016 (Top Threats Working Group, 2016) The previous version was known as the Notorious Nine.

1. Data breach – sensitive data is released or stolen
2. Insufficient identity, credential and access management – lack of access management because of a failure to use multi-factor authentication, weak passwords, or rotation of keys, passwords and

certificates

3. Insecure Interfaces and APIs – APIs and UIs are exposed outside trusted boundaries through IP addresses. They require authentication, access control, encryption and activity monitoring
4. System vulnerabilities – exploitable bugs
5. Account hijacking – phishing, fraud and vulnerability exploitation achieve system or account hijacking
6. Malicious Insiders – an insider to the organization that violates CIA of the organizations information and information systems
7. Advanced persistent threats – parasitical attack that infiltrates a company's infrastructure to smuggle data and intellectual property
8. Data loss – permanent loss of data
9. Insufficient due diligence – rushing to adopt cloud services without analyzing risks
10. Abuse and nefarious use of cloud services – poorly secured deployments, free trials, and fraudulent account sign up
11. Denial of service – prevent users from accessing services
12. Shared technology vulnerabilities – failure of separation of tenants within the multitenant cloud structure

Egregious 11 – Cloud security alliance

In 2019 the CSA redefined their top cloud computing threats into a slightly shorter list of 11 issues.

1. Data breaches – sensitive data is released or stolen
2. Misconfiguration and Inadequate Change Control – Cloud services incorrectly setup or not controlled alternations to the configuration
3. Lack of Cloud Security Architecture and Strategy – Lacking in design structure, just building silos to suit a need or respond to a problem
4. Insufficient Identity, Credential, Access and Key Management – lack of access management because of a failure to use multi-factor authentication, weak passwords, or rotation of keys, passwords and certificates
5. Account Hijacking – phishing, fraud and vulnerability exploitation achieve system or account hijacking

6. Insider Threat - an insider to the organization that violates CIA of the organizations information and information systems
7. Insecure Interfaces and APIs - APIs and UIs are exposed outside trusted boundaries through IP addresses. They require authentication, access control, encryption and activity monitoring
8. Weak Control Plane – The method of connection to the cloud infrastructure by a customers administrators/engineers is not secured properly. One of the best methods would be two-factor authentication
9. Metastructure and Applistructure Failures – Multiple issues here that involve things like poor API implementation to lack of encryption of data at rest and in transit
10. Limited cloud Usage Visibility – two main problems 1) shadow IT where users are setting up and using cloud apps that are not known to corporate it/security. 2) Use of sanctioned apps by specific unknown users or bad actors
11. Abuse and Nefarious Use of Cloud Services – Malicious actors using cloud services to launch attacks or to host malware are among the biggest problems here

Identity and Access Management

- IAAA – Identification, Authentication, Authorization, Accountability
    - Identification – Statement of who you claim to be
    - Authentication – Verify or Validate who you claim to be
        - Factor 1 – Something you know
            - Passwords, Passphrases, cognitive passwords. See NIST SP 800-63 for best recommendations
        - Factor 2 – Something you have
            - Hard Tokens, Soft Tokens, Cards, X.509 Public Key Certificate
        - Factor 3 – Something you are
            - Biometrics. Physiological or Behavioral characteristics of a user

        - Multi-factor authentication – using at least 2 of the 3 factors – HIGHLY RECOMMENDED especially for all cloud accounts (user and admin)
    - Authorization – Granting of access privileges (or not)
        - Decisions could be based on Classification/Clearance combinations. Or ACLs, or RBAC, etc.
    - Accountability – Create a log so as to be able to hold users accountable for action within their account.
        - Log all access?
        - Log all failed attempts at access?
        - Log what a user does access?

Authorization decisions

- Access Control List (ACL) – Basic list, usually, by object with a list of what subjects have access with permissions defined
    - Should be controlled at 3 levels:
        - Management plane
        - Public and internal sharing controls
        - Application level controls
- Access Control Matrix (ACM) – A table mapping Subjects to Objects. The matched cell between those two can define privileges to be granted
- Role based access control (RBAC) – Access control methodology that works well in large companies that can easily distinguish roles that contain many users
- Attribute based access control – Access is determined by assessing many different attributes such as:
    - Patch level
    - Known or unknown device
    - Wired or wireless
    - Within or outside of the business VLANs
    - Anti-malware status
    - Firewall status

SSO – Single sign on

Traditionally Kerberos. In the cloud we are using SAML or other.

- SAML – Security Assertion Markup Language
  - Older but well supported within industry today
  - Authentication that is XML based that results in a 'token'
  - Service provider is the destination web service that the user wants to communicate with
  - Service provider relies on the Identity provider to authenticate the user, so they are the 'relying party'
  - Identity provider verifies user identity through identification and authentication
  - The token is passed through the user's computer therefore they are the 'relaying party'
- OAuth – Open Authorization is the protocol that allows for the SAML tokens to be passed.
- OpenID – Open Identification protocol used for Authentication.
- WS Federation – Web Services Federation
  - Oasis standard for authentication that results in a 'security token'
  - Championed by Microsoft
  - Uses SOAP and XML

Cloud Access Security Brokers (CASB)

Monitoring services:

- DNS queries
- API connections
- Inline interception (man in the middle monitoring)
- DLP

Firewalls

- A device/software that filters traffic. It will make a block or allow

traffic to pass based on type of firewall and configuration. Firewalls work through a list of rules to match a packet to. They work top down through the list of the rules and the first rule that a packet matches is how the packet is handled.

- Firewalls should be installed between a trusted and an untrusted network. That includes between a LAN and a DC.
- XML Gateway – This is a type of firewall that lives at L7 of the OSI model. It monitors and controls XML traffic specifically
- API Gateway – This is a type of firewall that lives at L7 of the OSI model. It monitors and controls API traffic to include SOAP and REST

Intrusion Detection System (IDS)

- An IDS is a device/software that monitors and logs network events. An IDS can be installed/virtually installed as a tap on a line. In this instance it is effectively viewing traffic from the past. The packets will have been sent on to the destination, but the IDS will also receive a copy to view.
- Can be installed as a network appliance or on the destination/source host device.
- When installed on the host it often examines the logs not the packet
- Intrusion detection logic
    - Signatures – Signature files must be kept up to date. Detects known attacks
    - Anomalies – Must first learn what is normal on a device. Then it will detect anything that is different as an Intrusion.
- Actions that are possible include
    - Logging the event
    - Notifying the devices involved in the transmission path, e.g. the Firewall or the host so that that device can take an action on the intruder's packet flow
    - Notifying the NOC/SOC

Intrusion Prevention System (IPS)

- The IPS is an extension to an IDS. It makes the device/software become actively involved though the transmission of the packets. Traffic must pass through the IPS. Installed inline when it is network based. It could be installed on a host as well.
- Intrusion detection logic
  - Signatures are known attack patterns.
  - Anomalies – This is probably the most dangerous of devices to have on a network.
- Actions are the same as IDS. This device must seriously be cared for as it will drop the traffic and that could be detrimental to the business if it is not actually an intrusion

Designs to improve security controls

Micro-segmentation - Create very tiny controlled 'networks'. Control access to or from a specific resource using all security controls possible to include that resource being within its own virtualized network environment alone.

Hyper-segmentation - spans end to end, device to data center giving a more complete view of data flow, apps and their users

Blast radius - defines the extent of the possible damage when a virus (or something else) "explodes"

Database Activity Monitor (DAM)

DAMs are used to monitor, well, the activity on a Database (DB). The activity will include who logs in, possibly who does not login, and the actions they use on the data itself.

The logs are stored outside of the DB so users/hackers should not be able to access or modify them.

File Activity Monitor (FAM)

FAMs monitor, again, the activity that occurs on a file storage system.

DLP (Data Leak Prevention)

DLP is the attempt to prevent data from leaking out of a corporation's network. A leak is an unacceptable transmission, either the format of the transmission or the destination. (a.k.a. Data Loss Prevention, Data Loss Protection, Data Leak Protection)

DLP can be installed in many different manners especially when you add cloud to the transmission and storage of an enterprises data. The CSA's SecaaS Category 2 defines DLP as 'describe the controls put in place by an organization to ensure that data (structured and unstructured) of value remains under authorized use and care' (Cloud Security Alliance, 2012)

DRM (Data Rights Management)

a.k.a. Information Rights Management especially within a corporation or digital rights management

- DRM software controls access to Intellectual Property (IP)
- Allows control of content to include, but not limited to:
  - Length of access
  - Print capability
  - Screen capture capability
  - Copy/Paste capability
  - Sharing controls
- Examples: Netflix app, Kindle, iTunes, Spotify, Locklizard

Physical Data Center Design

Most of this document/exam is looking at the cloud really from the customers side. Even a lot of this domain is that way. There are several things that need to be taken into consideration when looking at this from the cloud providers side. It is necessary to look at some of this!!!

- Location
  - Natural disasters – are you in the range of hurricanes, mud slides, earthquakes, wildfires etc. would factor into choosing a location or what controls need to be put in place to minimize the impact of those threats

    - Neighbors? – who are the neighbors of the facility and how could they cause you a problem?
- Outer perimeter controls
    - Fences – Height, material, Top guard, Outriggers
    - Walls – Material, height
    - Gates – Vehicle control, pedestrian control
    - Bollards – Stationary (possibly removable) concrete (or metal) pillars to block vehicle traffic
    - (it does not appear that depth of these are needed for this exam)
- Walls/Doors
    - Walls in a data center should be rated to hold back fire for 4 hours
    - Solid core – Door construction is a solid piece of wood or metal
    - Protected hinges – Capped or welded into place for example
    - (it does not appear that depth of these are needed for this exam)
- Internal access control
    - Guards – Perfect for discerning decision
    - Biometric controls – on gates or doors. Fingerprint, handprint, palm vein, hand geometry, etc.
    - Two factor authentication – on gates or doors. e.g. badge plus hand geometry
    - Double doors a.k.a. Mantrap
        - Weight sensors
        - Timed access to the DC

- Power
    - UPS
    - Generators
    - (it does not appear that depth of these are needed for this exam)

Domain 4 - Cloud Applications Security – 17%

First and foremost, it should be said that secure applications mean the code is clean and free of flaws and defects. Adding security, such as cryptography, helps to secure the data that is being process by the application, but it does not make the application secure. In fact, it might have been added incorrectly resulting in more bugs and flaws and an unrealistic sense of security for the customer.

Clean code requires the developers and everyone else that touches this project to be trained in how to develop clean code. There are many defensive coding classes out there today. Even lunch and learns would be a terrific idea to ensure developers are always expanding their knowledge.

Clean code involves things like:

- Create well named functions that explain themselves and do not need comments to try to explain them
- Use comments only when absolutely necessary
  - Well written code tells the story by itself
  - Comments do not need to be added if the code is clean and neat
- One maybe two functions at a time
- Clean, clear and consistent formatting
- Use validated code/libraries/encryption

Supply chain management

Where did that code come from?

- ISO 28000 – Specification for Security Management Systems for the Supply Chain
- ISO 27036 – Information Security for Supplier Relationships

Software development lifecycle

Fundamentally this is project management. How do you create something that your customer wants and needs? Care must be given to the process.

1. Requirements – Customer needs understood
2. Design – Plan what to build
3. Implementation – Time to code
4. Testing and debugging – Static and Dynamic testing
5. Installation – Push to production environment
6. Maintenance – Update with new features or fix bugs and flaws

Now there are actually many different versions of the SDLC so knowing a few variations is helpful. They are all fundamentally the same in the progress that they go through. Here is the one in the CSA guidance document.

1. Define
2. Design
3. Develop
4. Test

My personal favorite is:

1. Project Management and Initiation
2. Functional Design
3. Detailed Design
4. Develop and Document
5. Test and Update
6. Push to Production and Maintain
7. End of Life (this step is added if we actually call this the System Life Cycle…. Drop the word Development)

Software development methodologies

The lifecycle does not need to be strictly following in a linear format (waterfall). There are many other approaches that have been developed over the years. The ones that are showing up the most in business right now seems to be:

- Agile
- Scrum
- DevOPS
- DevSecOps

Software testing

- Verification – Does it work? The functions that exist within an application need to be verified for functionality.
- Validation – Was it built as it was designed? All of the features and function need to be verified against the original build plan. Was anything left out/forgotten? Was anything added that should not actually be there?

- SAST – Static Application Security Testing
  - Application is in a stopped condition
  - Code is reviewed
  - Security testing that analyzes application source code for software vulnerabilities and gaps against best practices (Moghnie, 2020)
- White box.
  - Similar to SAST in the code is being reviewed. Or just call it a Code Review
- DAST – Dynamic Application Security Testing
  - Application is in a running condition
  - Testing from the user's point of view
  - Security testing that analyzes a running application by exercising application functionality and detecting vulnerabilities based on application behavior and

response (Moghnie, 2020)

- Interactive Application Security Testing (IAST)
  - Software component deployed with an application that assesses application behavior and detects presence of vulnerabilities on an application being exercised in realistic testing scenarios (Moghnie, 2020)
- Black box.
  - Similar to DAST in that a program is being tested from the running condition
- Fuzz Testing/Fuzzing
  - Throw as much junk as you can at the users interface to discover where the application breaks
- Threat Modeling
  - Methodology to identify and understand threats impacting a resource or set of resources (Moghnie, 2020)

CWE/SANS Top 25 Most Dangerous Programming Errors

While it is not necessary to memorize all 25 of these elements, nor their score or ID, it would be a good idea to start with number 1 and get to know these issues. If you are a programmer, managing programmers, managing a project these issues can cause a great deal of harm to your company or that of your customers. A great deal more info can be found at: https://cwe.mitre.org/top25/#Listing

1. Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)
2. Improper Neutralization of Special Elements used in an OS Command (OS Command Injection)
3. Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
4. Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
5. Missing Authentication for Critical Function
6. Missing Authorization
7. Use of Hard-coded Credentials
8. Missing Encryption of Sensitive Data

9. Unrestricted Upload of File with Dangerous Type
10. Reliance on Untrusted Inputs in a Security Decision
11. Execution with Unnecessary Privileges
12. Cross-Site Request Forgery (CSRF)
13. Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
14. Download of Code Without Integrity Check
15. Incorrect Authorization
16. Inclusion of Functionality from Untrusted Control Sphere
17. Incorrect Permission Assignment for Critical Resource
18. Use of Potentially Dangerous Function
19. Use of a Broken or Risky Cryptographic Algorithm
20. Incorrect Calculation of Buffer Size
21. Improper Restriction of Excessive Authentication Attempts
22. URL Redirection to Untrusted Site ('Open Redirect')
23. Uncontrolled Format String
24. Integer Overflow or Wraparound
25. Use of a One-Way Hash without a Salt

OWASP Top 10

ISC^2 no longer references OWASP in their Exam Outline. There are still some critical things to be familiar with from the top 10 such as: Injection

- Injection – one of the most common being SQL. Code that is injected into a form or field that should not be there. Input validation can confirm data entry that is appropriate versus a command that a hacker is trying to execute
- XSS - Cross Site Scripting is an attack against something like a website that has data/commands that is/are being pulled from another source into the current page. The problem is that the user may not know that they are actually interacting with a forged or compromised site and providing information to the hacker
- CSRF - Cross Site Request Forgery
- Insecure direct object reference - intitle:index of etc

ISO/IEC 27034 – Security Techniques – application security

ISO/IEC 27034 states that it 'provides guidance to assist organizations in integrating security into the processes used for managing their applications'

- Organization Normative Framework (ONF) – Allows an organization to define its application best practices
- Application Security Management Process (ASMP) – The process allows the organization to develop the ANF from the ONF
- Application Normative Framework (ANF) – Assists the organization to develop the plan for the best practices from the ONF that will be used for a specific application

Sandboxing

The initial term for sandboxing was Process Isolation. It is most commonly referred to as sandboxing at this point. To sandbox is to isolate the code (e.g. JavaScript) or anything up to an entire Virtual Network.

Application Virtualization

Programs like WINE allow the running of windows-based programs on other systems such as MACOS or LINUX. Another is App-V which allows applications to be streamed to any client from a virtual application server.

Threat Modeling

Imagine a hacker's perspective on how to attack a system. From there you can perceive the process that would be followed through the attack. Once you can imagine what would happen it become possible to put corrections in or tools in other domains to prevent the threat from being realized.

- OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation Framework from Carnegie Mellon.
- STRIDE - From Microsoft
    - Spoofing – To pretend to be another
    - Tampering – To alter

    - Repudiation – To deny or argue
    - Information Disclosure – Information in the wrong hands
    - Denial of Service – To prevent the users from being able to do their jobs
    - Escalation of Privileges – To increase permissions to root level
- PASTA - Process for Attack Simulation and Threat Analysis
- Trike - Open-source threat modeling methodology and tool

Orchestration Tools

Software versioning and management
Puppet
Chef
Ansible
Salt

Domain 5 - Operations – 17%

Data Center Tiers

Tiers are defined by the Uptime Institute. DCs must be certified against these criterion (Uptime Institute, n.d.)

- Tier 1 – Basic Capacity
  - Dedicated IT space
  - Dedicated cooling
  - UPS and Generator for power outages
- Tier 2 – Redundant capacity components
  - Tier 1 plus:
  - Add redundant power and cooling
- Tier 3 – Concurrently maintainable
  - Tier 2 plus:
  - Equipment maintenance does not require shutdown
  - Redundant delivery path for power
  - 2N
- Tier 4 – Fault tolerance
  - Tier 3 plus:
  - Fault tolerance to site infrastructure topology
  - 2N+1
- (Tier 5 – Rob Roy – Switch Networks) He has filed a patent

Operations and Maintenance of Systems

- Keyboard, Video and Mouse (KVM) is a reference to the physical equipment needed by operations when they first physically install systems such as servers, routers and switches. These devices come with a default configuration that must be modified in order to integrate into the physical network. In order to do that, usually, a

laptop is connected to the device physically which would supply the KVM needed.

- Remote Desktop Protocol (RDP) is used to remotely connect to a virtual machine. Once logged in the capabilities that the user has is matched to their user profile. This is commonly used by network administrators to manage their devices.
- Secure Shell (SSH) is commonly used to connect to appliances like routers, switches and firewalls for configuration. It is recommended to support SSH-2 and not SSH-1.
- Maintenance Mode – Virtual machines are put into maintenance mode in order to patch or change configurations. Once the system has been updated as needed a snapshot should be taken. This creates the Image file of the virtual machine. All virtual machines that match this system should be sent through a reboot process that has it load from the newly modified image file. The image file is stored as an object in a VM storage system.

Preventing successful attacks

- Honeypots/Honeynet – A honeypot is a server that has been setup to distract the attackers. The goal is to detect their presence and contain their attack to that server. It should look and feel like a corporate server with valuable data, yet none of the data should be real. A honeynet is the extension to include what appears to be a full network of devices. Either of these can easily be created with VMs. Alerts should be setup to let the SOC know that they are actively being attacked so that they can respond appropriately.
- Vulnerability Assessments have the intention of detecting the location of vulnerabilities within an organization. Could be physical or logical such as an unlocked window or an unpatched server. Unfortunately this has the outcome of a high number of false positives. A false positive is a finding of a vulnerability that either does not exist or is not exploitable.
- Penetration Testing takes vulnerability assessments to the next level with an attempt to exploit any discovered vulnerabilities. The serious danger here is that damage will occur. This should not only

be done by teams that know what they are doing that have written & signed permission (get out of jail free card).

- The process follows:
  - Information gathering/reconnaissance – generally known as low tech stage. It is normal in this stage to do social engineering or dumpster diving as well as technical tools.
  - Enumeration – goal of creating fingerprints of all systems)
  - Vulnerability mapping – using knowledge found at cve.mitre.org or another similar site and the knowledge and experience of the tester.
  - Exploitation – attempt to exploit the vulnerability. Actions should only be taken as written in the Rules of Engagement document.
  - Document all actions and findings. The final report given to the person who hired the pen tester should also contain suggestions on how to fix it.

Security Operations Center (SOC)

This is where the security team is housed that would monitor and analyze the enterprise on an ongoing basis. The goal is to know that incidents are happening (detect) and then respond accordingly. Incidents should be contained and their impact minimized.

ITIL/ISO/IEC 20000

This is all about IT Service Management. Business today relies heavily on their IT. Move to the cloud and focus there and we have almost nothing left except IT to discuss within this certification.

- ITILv4 has the service value chain of:

1. Plan
2. Improve

3. Engage
4. Design and transitions
5. Obtain/build
6. Deliver and support

- Change Management – Fundamentally nothing should be changed within IT without going through a process. The process involves sending a request to the Change Advisory Board (CCB). That request should be analyzed for:
    - Is it in compliance with policy?
    - Does it create any additional compliance issues or solve issues?
    - How does it affect all of the departments of the business?
    - Has it been tested?
    - Is there a back-out plan?
- Continuity Management
- Patch Management
- Event -> Incident -> Problem -> Disaster

Packet Capture

Packet capturing is possible within a cloud of any kind. Who can collect those packets will differ when dealing with SaaS vs PaaS/IaaS.

- The customer will not be able to do any kind of packet capture within a **SaaS** but the Cloud Provider can.
- If the customer has bought **PaaS** packets can probably be collected from that platform, but that will depend on the type of platform.
- In **IaaS** the customer will be able to do packet captures from their own virtual machines.
- **What can actually** be seen in reality depends on the build, the XaaS type and the control

Logging of Events

Events always need logging. At this point the number of logs collected by a company is voluminous. What needs to be logged and who can see those logs will vary, as it does with packet capture (see above).

- In **SaaS** the customer should be able to see events related to their own user's access control events
- In **PaaS** logs from the applications and software installed on the platform should generate logs that are visible to the customer. Logs from the OS may provide the customer with access control information.
- In **IaaS** the customer should have access to all of the logs for the VMs that they build as well as logs for access to the Hypervisor for that creation and monitoring.
- **What can actually** be seen in reality depends on the build, the XaaS type and the control

Security Information and Event Management (SIEM)

SIEMs are used today to manage the logs from all of our different platforms. A SIEM will:

- Collect
- Correlate
- Analyze
- Alert

Data and Media Sanitization

- Deletion – Removes pointer in the FAT (File allocation Table). It does not actually remove the data
- Formatting – A format of the drives clears it enough for something like a reinstall of an OS, but all of the files can probably be recovered
- Overwriting – Doing a proper, government level, overwrite of a drive will remove the data to a point that special equipment is likely to be necessary to be able to recover any data
- Degaussing – This is a process which deceases or eliminates a

remnant magnetic field. A gauss is a unit of magnetism. This will remove the data to a point that special equipment is likely to be necessary to be able to recover any data

- Physical Destruction – There are standards to what size a drive should be shredded to. If properly followed it is highly unlikely that any data would ever be recoverable
- Defensible Destruction – Witnessed Shredding
- Crypto-Shredding a.k.a. cryptographic erasure – Since a cloud customer will not be able to do any of the above to the drives that are located within a public cloud provider… encrypt the data and destroy the key. Perhaps a second time with a different algorithm. Maybe even a third time depending on level of sensitivity. It should also be in the contract for the cloud provider to do the same when service is cancelled.
- Clear – Data will not be retrievable without state-of-the-art technology. It will likely have been written over once, seldom more than three times, with repetitive data such as all zeros.
- Purge – data would be destroyed to a level that it would likely not be recoverable even within a lab environment. Degaussing would be at this level.

When it all goes wrong

Event – ITIL defines this a s a change of state
Incident – An adverse event
Problem – A recurring incident, root cause must be found
Disaster– IT is now in BIG trouble
Business Continuity (BC) – The business may not survive this.

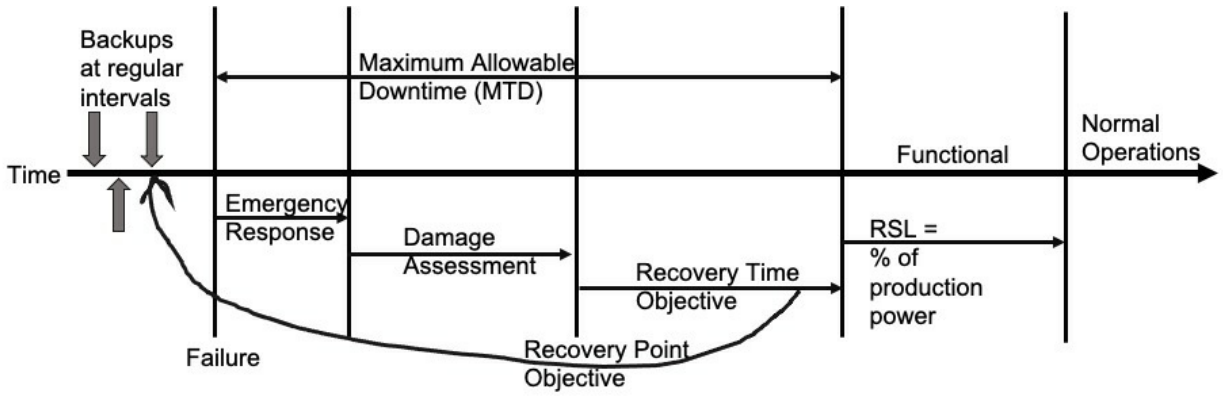
Planning for Eventualities

1. Policy
2. Project Management and Initiation (PMI)
3. Business Impact Analysis (BIA)
4. Recover Strategizing
5. Develop Plan Document
6. Implement, Test, Update

7. Embed in the User Community

1. Policies are written by Management to convey their goals and objectives. There needs to be a policy on the topic of Business Continuity that explains the goals and objectives for each of the levels of issues that can disrupt a business, from Incident to full BC.
2. In the PMI phase the basics of project management must be addressed.
    1. Project team leader
    2. Project team
    3. Steering committee
    4. Mini BIA to determine time needed
    5. Time needed for this project
    6. Assign tasks to team members
    7. Obtain and short review of existing documents
    8. Estimated/approved budget
3. Business Impact Assessment (BIA)
    1. Quantitative Risk Assessment - This is the calculation of the cost of an incident to the business.
        1. SLE = AV * EF
        2. ARO = # of times/year(s)
        3. ALE = SLE * ARO
    2. Qualitative Risk Assessment - This is the process of ranking and prioritizing incidents so as to determine what must be protected against.
    3. Maximum Tolerable Downtime (MTD) – the maximum amount of time a system can be offline
    4. Recovery Time Objective (RTO) – the time that a corporation has to do the actual work of recovery
    5. Recovery Point Objective (RPO) – the point in the past the last known good backup was created. It is expressed in a unit of time. It is the amount of data that can be lost.
    6. Service Delivery Objective (SDO) is considered the combination of RTO and RPO
    7. Recovery Service Level (RSL) is a percentage of production processing power that must be there for the

business to be able to function well enough to not cause too great a loss.



4. Recovery Strategies
    1. Normally things like Hot, Cold, Mobile sites are addressed here, but this is Cloud focused so only…
    2. Data Center failed over to the cloud
    3. Fail within a cloud provider to another region
    4. Fail from one cloud provider to another, e.g. AWS to Azure
5. Document
    1. Create the **procedural** documents that detail how to accomplish this failover when it finally happens, when your cloud has failed in some way
6. Implement, Test, Update
    1. You must first build the alternative plan in order to be able to test
    2. The level of test that a plan must go through should be determined by management. The question is what is their goal? To have an **idea** that it might work or to **know** it will work?
    3. There are 5 basic test level. Testing should begin at the, well, beginning and then work up through the tests. It is critical to test to a level of success that management wants.
        1. Checklist/Desk Check – confirm details have been added to the document
        2. Structure walk-through/Tabletop – talk through

a scenario

3. Simulation – emulate a fail over, e.g. a fire drill
4. Parallel - bring the alternate cloud environment up to a functional level while the business remains functional on the production network (cloud or not)
5. Full Interruption – a complete operational switch to the backup cloud environment. Production is now running on the backup cloud environment.

4. Testing will uncover issues with the procedural document. Fix these and then test again… to the level management wants.

7. Embed in the user community
    1. Practice, Practice, Practice

Domain 6 -Legal and Compliance – 13%

- FedRAMP – Federal Risk and Authorization Management Program
  - A standardized approach to cloud security
- Stored Communications Act
  - US Law for Internet Service Providers
  - It limits and controls access to stored wire and electronic communications and transactional records. They must be protected
- CLOUD Act (Clarifying Lawful Overseas Use of Data)
  - The purpose is to improve the US governments/law enforcements access to data stored across borders

Privacy

ISO/IEC 27018 - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

- EU Directive 95/46 EC – European Data Protection Directive
- EU Directive 2002/58/EC – ePrivacy Directive. GDPR Article 95 says that this is still supported. This specified more specific details regarding electronic communication. This includes things like marketing communications and cookies for example.
- GDPR – European General Data Protection Regulation
  - <u>Basic terms from GDPR and its definitions</u>
  - Personal data – ‘any information relating to an identifiable natural person (data subject)’
  - Data Subject – ‘one who can be identified, directly or indirectly’
  - Data Controller – ‘a person who alone or jointly with others processes or controls or authorizes the processing of data’
  - Data Processor – ‘a person who processes data solely on

behalf of the controller, excluding the employees of the data controller'

- Privacy Principles from GDPR
  - Data must be processed:
    - Lawfully, fairly and transparently
    - Only for a specific and explicit purpose
    - With only the minimal amount of information needed
    - Up to date or properly erased
    - With appropriate integrity and confidentiality controls

Additional Privacy terms defined in the CSA Guidance 4.0 document

- Data Owner - Your organization is always responsible for data and information and that can't be avoided when moving to the cloud.
  - Responsible for a piece or set of data
  - Responsible for classifying that piece or set of data

- Data Custodian - actually in possession, first group identified as a custodian normally is IT

- Privacy Act of 1988 – Australia
- PIPEDA – Personal Information Protection and Electronic Data Act – Canada
- Act on the Protection of Personal Information - 2017 – Japan
- Personal Data Protection Act No. 25,326 – Argentina
- Protection of Privacy Law, 5741-1981 and Protection of Privacy Regulation (Data Security), 5777-2017 – Israel
- Federal Act on Data Protection – Switzerland
- US Safe Harbor – defunct and replaced by US Privacy Shield
- US Privacy Shield
- HIPAA – Health Insurance Portability and Accountability Act – USA Protected Health Information (PHI)
- COPPA – Children's Online Privacy Protection Rule – USA –

Imposes requirements on websites that are targeted at and collecting information regarding children 13 and under

AICPA/CICA Privacy Maturity Model

The American Institute of Certified Public Accountants with the Canadian Institute of Chartered Accountants with help from ISACA created a Maturity Model based on the GAPP.

(AICPA and CICA, 2011)

AICPA/CICA PRIVACY MATURITY MODEL[1]
Based on Generally Accepted Privacy Principles (GAPP)[2]

GAPP - 72 CRITERIA	CRITERIA	MATURITY LEVELS				
CRITERIA	DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
MANAGEMENT (14 criteria)	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.					
Privacy Policies (1.1.0)	The entity defines and documents its privacy policies with respect to notice; choice and consent; collection; use, retention and disposal; access; disclosure to third parties; security for privacy; quality; and monitoring and enforcement.	Some aspects of privacy policies exist informally.	Privacy policies exist but may not be complete, and are not fully documented.	Policies are defined for notice, choice and consent; collection; use, retention and disposal; access; disclosure; security for privacy; quality; and monitoring and enforcement.	Compliance with privacy policies is monitored and the results of such monitoring are used to reinforce key privacy messages.	Management monitors compliance with policies and procedures concerning personal information. Issues of non-compliance are identified and remedial action taken to ensure compliance in a timely fashion.
Communication to Internal Personnel (1.1.1)	Privacy policies and the consequences of non-compliance with such policies are communicated, at least annually, to the entity's internal personnel responsible for collecting, using, retaining and disclosing personal information. Changes in privacy policies are communicated to such personnel shortly after the changes are approved.	Employees may be informed about the entity's privacy policies; however, communications are inconsistent, sporadic and undocumented.	Employees are provided guidance on the entity's privacy policies and procedures through various means; however, formal policies, where they exist, are not complete.	The entity has a process in place to communicate privacy policies and procedures to employees through initial awareness and training sessions and an ongoing communications program.	Privacy policies and the consequences of non-compliance are communicated at least annually; understanding is monitored and assessed.	Changes and improvements to messaging and communications techniques are made in response to periodic assessments and feedback. Changes in privacy policies are communicated to personnel shortly after the changes are approved.

PCI-DSS (Payment Card Industry – Data Security Standards

This is a contractual agreement with the Payment card company to be able to process card charges. There are 12 fundamental requirements. The level of compliance is based on the number of transactions per year that a company does.

1. Build and maintain a firewall
2. Do not use vendor supplied defaults
3. Protect stored cardholder data
    - Never store the CCV/CVV
4. Encrypt transmissions over public networks
5. Use regularly updated anti-virus
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data on a need to know basis
8. Use unique user IDs for all that have access to cardholder data
9. Restrict physical access to cardholder data
10. Track and monitor all network and cardholder data access
11. Regularly test security systems

12. Maintain an information security policy

Level 1 – Formal Audit
Level 2-4 self-audit
Level 1 – more than 6 million transactions a year

Industrial Control Systems (ICS)

Protection of the national electric grid is paramount. Connecting the systems that control the Programmable Logic Controllers (PLC) that control the grid to the Internet in any manner requires protection. Effectively the control systems need to be embedded deep within a network so that a hacker must go through so many control points that we would know they are there before any damage can be done. Applicable terms and standards include:

- North American Electric Reliability Corporation Critical Infrastructure Protection (NERC/CIP)
- Supervisory Control and Data Acquisition (SCADA)
- Distributed Control Systems (DS)
- NIST SP 800-82

Audits

An audit is the verification of the controls and configurations within systems of physical environments. The first requirement that must be fulfilled is a very strict methodology for conducting the audit. The American Institute of Certified Public Accountants (AICPA)

- SAS 70 – Old and outdated, but the beginning of the story
- SSAE 16/18 – 16 is being replaced by 18
- ISAE 3402/3400 – International equivalent of the AICPA SSAE 16/18

Once the auditors are started within the structure of something like SSAE 16 then the work begins. One of the most important things is to create the scope of the audit. It is essential to be as specific and accurate as to what systems are within scope of this audit.

- SOC 1 – From AICPA the ‘CPAs that audit the user entities’ financial statements (user auditors), in evaluating the effect of the controls at the service organization on the user entities’ **financial** statements. (AICPA, 2019)
    - Type I - report on the fairness of the presentation of management’s description of the service organization’s system and the suitability of the design of the controls
    - Type II - report on the fairness of the presentation of management’s description of the service organization’s system and the suitability of the design of the controls and operating effectiveness
- SOC 2 – These reports are ‘intended to meet the needs of a broad range of users that need detailed information and assurance about the controls at a service organization relevant to **security, availability, and processing integrity** of the systems the service organization uses to process users’ data and the **confidentiality** and **privacy** of the information processed by these systems.
    - Type I - management’s description of a system and the suitability of the design
    - Type II - management’s description of a system and the suitability of the design and operating **effectiveness** of controls
- SOC 3 - These reports meet the needs of users who need assurance controls at a service organization relevant to **security**, **availability**, **processing integrity, confidentiality**, or **privacy** without need for the details. General use reports and can be freely distributed

Gap Analysis

The difference between where we are and where we want to be. Don’t forget to “Mind the Gap” You must figure out where you are in relation to where you want to be, which might be in compliance with your policy, or GDPR, or PCI-DSS or…

GAPP – Generally Accepted Privacy Principles are based on the GAAP

GAAP – Generally Accepted Accounting Principles – These are the core principles of accounting such as “count the money twice”

GASP – Generally Accepted Security Principles – These are also based on the original GAAP, just targeted now at Security.

Forensics

When a policy is violated (operational investigation) or there is a civil dispute (between two parties – Civil investigation) or a law has been broken (Criminal of Regulatory investigation) the processes used to collect evidence and exam it must be carefully controlled.

It must be provable that the evidence came from the suspects computer and it remains unaltered.

- Hearsay - a witness of evidence that cannot be cross examined.
- Search and Seizure processes must be followed to ensure that evidence collected will be permissible in court because no laws were violated in the collection process

Basic Forensics Rules

1. Never do this unless you are trained and, in some places, certified
2. Follow all legal rules such as chain of custody
    1. Chain of Custody
    2. Data collection/seizure
3. Use only approved tools that are acceptable in your court system
4. Assume you are going to court and will have to testify
5. So, document exactly what is done in the collection and examination process
6. Collect evidence in order of volatility
    1. Screen
    2. RAM
    3. Cache
    4. Storage drives
7. Do not exceed your knowledge!!!

- ISO/IEC 27037 – Guidelines for identification, collection, acquisition and preservation of digital evidence
- ISO/IEC 27041 – Guidance on assuring suitability and adequacy of incident investigation method
- ISO/IEC 27042 – Guidelines for the analysis and interpretation of digital evidence
- ISO/IEC 27043 – Incident investigation principles and processes
- ISO/IEC 27050 – Code of practice for electronic discovery (E-Discovery)

Acronyms

A

ACL – Access Control List
ACM – Access Control Matrix
AICPA – American Institute of Certified Public Accountants
ALE – Annualized (Annual) Loss Expectancy
ANF – Application Normative Framework
API – Application Programming Interface
ARO – Annual Rate of Occurrence
ASMP – Application Security Management Process
AV – Asset Value
AWS – Amazon Web Services

B

BC – Business Continuity
BIA – Business Impact Analysis
Bins – Binaries
BOSS – Business Operation Support Services

C

CaaS – Communications as a Service
CAB – Change Advisory Board
CapEx – Capital Expenditure
CASB – Cloud Access Security Broker
CCB – Change Control Board
CCSP – Certified Cloud Security Professional
CIA – Confidentiality Integrity Availability
CLOUD Act – Clarifying Lawful Overseas Use of Data Act
CMM – Capability Maturity Model
CMMI – Capability Maturity Model Integration
CompaaS – Compute as a Service
COPPA – Child Online Protection and Privacy Act
CSA – Cloud Security Alliance
CSP – Cloud Service Provider
CSRF – Cross Site Request Forgery
CSS – Cross Site Scripting

D

DAM – Database Activity Monitor

DAST – Dynamic Application Security Testing
DB – Data Base
DBMS – Data Base Management System
DC – Data Center
DevOps – Development and Operations
DevSecOps – Development, Security and Operations
DHCP – Dynamic Host Configuration Protocol
DLP – Data Leak (Loss) Prevention (Protection)
DNS – Domain Name Service
DNSSec – Domain Name Service Security
DO – Dynamic Optimization
DPD – Data Protection Directive
DRM – Digital Rights Management
DRS – Distributed Resource Scheduling
DSaaS – Data Storage as a Service
DSL – Digital Subscriber Line

E

EAL – Evaluation Assurance Level
EF – Exposure Factor
ENISA – European Union agency for Cyber Security
ERM – Enterprise Rights Management
ESA – Enterprise Security Architecture
EU – European Union

F

FAM – Files Activity Monitor
FedRAMP – Federal Risk Assessment Management Program
FIPS – Federal Information Processing System

G

GAAP – Generally Accepted Accounting Principles
GAPP – Generally Accepted Privacy Principles
GASP – Generally Accepted Security Principles
GDPR – General Data Protection Regulation
GRC – Governance, Risk Management, and Compliance

H

HIPAA – Health Information Portability and Accountability Act
HSM – Hardware Security Module
HVAC – Heating, Ventilation and Air Conditioning

I

IaaS – Infrastructure as a Service

IaaS – Infrastructure as a Service

IAST – Interactive Application Security Testing

ICS – Industrial Control System

IDS – Intrusion Detection System

IEC – International Electro-Technical Committee

IP – Intellectual Property

IP – Internet Protocol

IPS – Intrusion Prevention (Protection) System

IPSec – Internet Protocol Security

IRM– Information Rights Management

ISAE 3402 – International Standards on Assurance Engagements No. 3402

ISC^2 – International Information Systems Security Certification Consortium

iSCSI – Internet Small Computer System Interface

ISMS – Information Security Management System

ISO – International Standards Organization

ITIL – formerly Information Technology Infrastructure Library

ITOS – Information Technology Operation and Support

J

JSON – JavaScript Object Notation

K

KVM – Keyboard, Video, Mouse

L

LAN – Local Area Network

Libs – Libraries

LUN – Logical Unit Number

M

MAC – Macintosh (Apple)

MAC – Media Access Control

MitC – Man in the Cloud

MPLS – Multi Protocol Label Switching

MSA – Master Services Agreement

MSP – Managed Service Provider

MTD – Maximum Tolerable Downtime

MTPD – Maximum Tolerable Period of Destruction

N

NaaS – Network as a Service

NAS – Network Attached Storage

NIST – National Institute of Standards and Technology

NOC – Network Operations Center

NSG – Network Security Group

O

OAuth – Open Authentication

OCTAVE – Operationally Critical Threat, Asset and Vulnerability Evaluation Framework

OECD – Organization for Economic Cooperation and Development

OpenID- Open Identification

OpEx – Operational Expenditure

Organization Normative Framework

OS – Operations System

OSI – Open System Interconnection

P

PaaS – Platform as a Service

PASTA – Process for Attack Simulation & Threat Analysis

PCI – Payment Card Industry

PCI DSS – Payment Card Industry Data Security Standard

PII – Personally Identifiable Information

PIPEDA – Personal Information Protection and Electronic Documents Act

PLA – Privacy Level Agreement

PMI – Project Management and Initiation

PP – Protection Profiles

Protected Health Information

R

RAID – Redundant Array of Independent (Inexpensive) Discs

RAM – Random Access Memory

RBAC – Role Based Access Control

RDBMS – Relational Data Base Management System

RDP – Remote Desktop Protocol

REST – REpresenational State Transfer

RIP – Router Information Protocol

RPO – Recovery Point Objective
RSL – Recovery Service Level
RTO – Recovery Time Objective

S

SaaS – Software as a Service
SABSA – Sherwood Applied Business Security Architecture
SAML – Security Assertion Markup Language
SAN – Storage Area Network
SAS 70 -Statement on Auditing Standards No. 70
SAST – Static Application Security Testing
SDLC – Software Development Life Cycle
SDN – Software Defined Network
SDO – Service Delivery Objective
SecaaS – Security as a Service
SIEM – Security Information (Incident) and Event Manager
SLA – Service Level Agreement
SLC – Software Life Cycle
SLE – Single Loss Expectancy
SOAP – formerly Simple Object Access Protocol
SOC - Security Operations Center
SOC Reports – Service Organization Control (audit reports)
SP – Special Publication
SQL – Structured Query Language
SSAE 16/18 – Statement on Standards of Attestation Engagements
SSH – Secure SHell
SSL – Secure Socket Layer (Now TLS)
ST – Security Target
STRIDE – Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Escalation of privileges

T

TCI – Trusted Cloud Infrastructure
TLS – Transport Layer Security
TOE – Target of Evaluation
TOGAF – The Open Group Architecture Framework
TPM – Trusted Platform Module
TRIKE -

U

UPS – Uninterruptible Power Supply
URI – Universal Resource Indicator
URL – Universal Resource Locator

V

VLAN – Virtual LAN
VM – Virtual Machine
VPN – Virtual Private Network
VSAN – Virtual SAN

W

WS Federation – Web Services Federation

X

XML – eXtensible Markup Language
XSS – Cross Site Scripting

IndeX

Study notes

1. This exam is a joint venture between ISC2 and the Cloud Security Alliance.
2. Documents from the CSA are both free and well written.
3. Start with either NIST SP 800-145 (https://csrc.nist.gov/publications/detail/sp/800-145/final) or ISO 17788 (https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html
4. A great follow up to that is ISO 17789 (https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html
5. Then NIST SP 800-146 (https://csrc.nist.gov/publications/detail/sp/800-146/final), NIST 500-299 (https://csrc.nist.gov/publications/detail/sp/500-299/draft)
6. A starting point within the CSA is the Cloud Security Alliance Guidance document. Which is currently at version 4 (https://cloudsecurityalliance.org/research/guidance)
7. From there I would recommend their SecaaS documents with initial focus on Category 8 – Encryption (https://downloads.cloudsecurityalliance.org/initiatives/secaas/Secaa and Category 2 DLP (https://downloads.cloudsecurityalliance.org/initiatives/secaas/Secaa

Bibliography

AICPA. (2019). *AICPASOC1report*. Retrieved from AICPA.org: https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/

Cloud Security Alliance. (2012, September). Category 2 // Data Loss Prevention. *SecaaS Implementation Guidance*. USA: CSA.

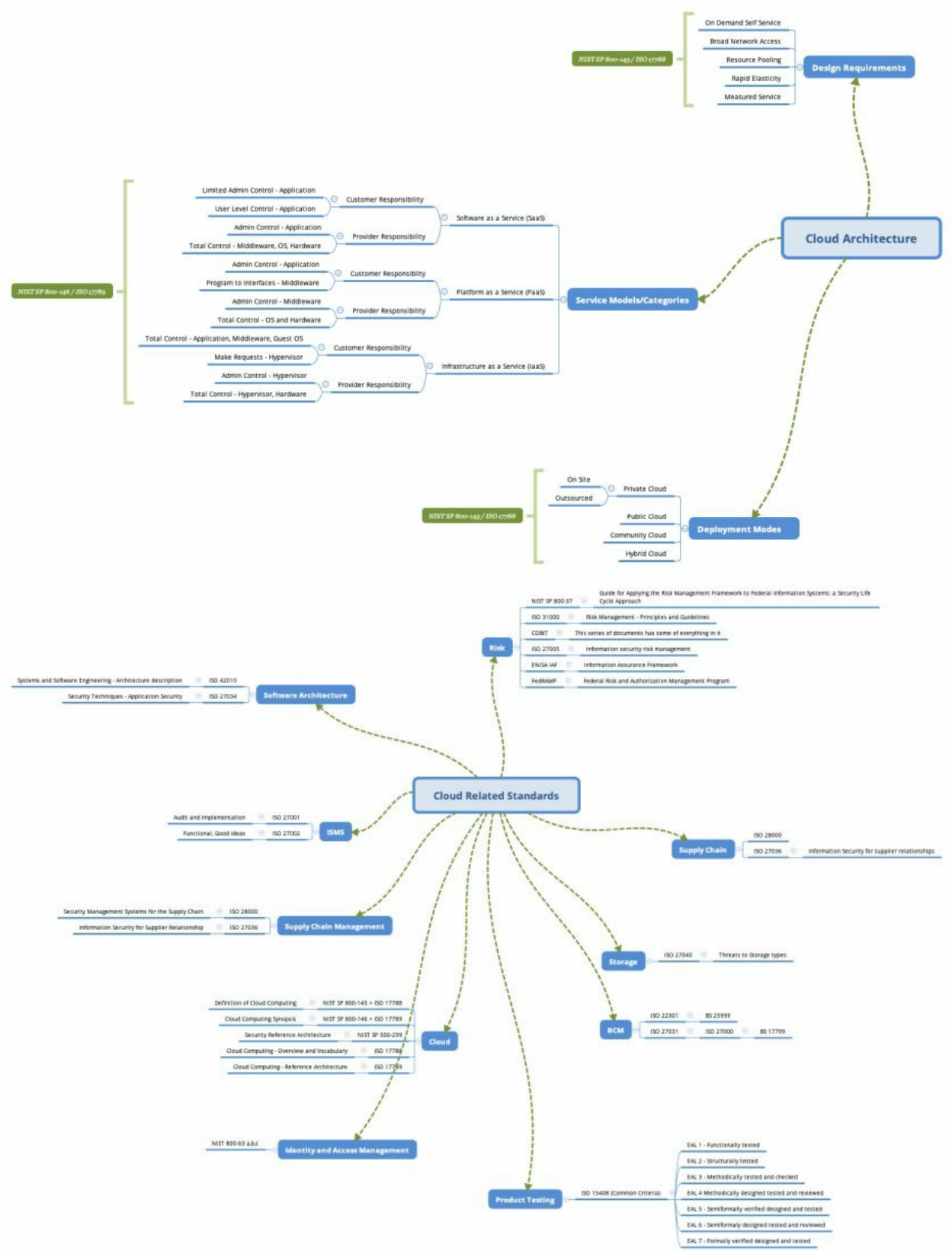
Cloud Security Alliance. (2017, 07 26). */research/guidance*. Retrieved from CloudSecurityAlliance.org: https://cloudsecurityalliance.org/research/guidance

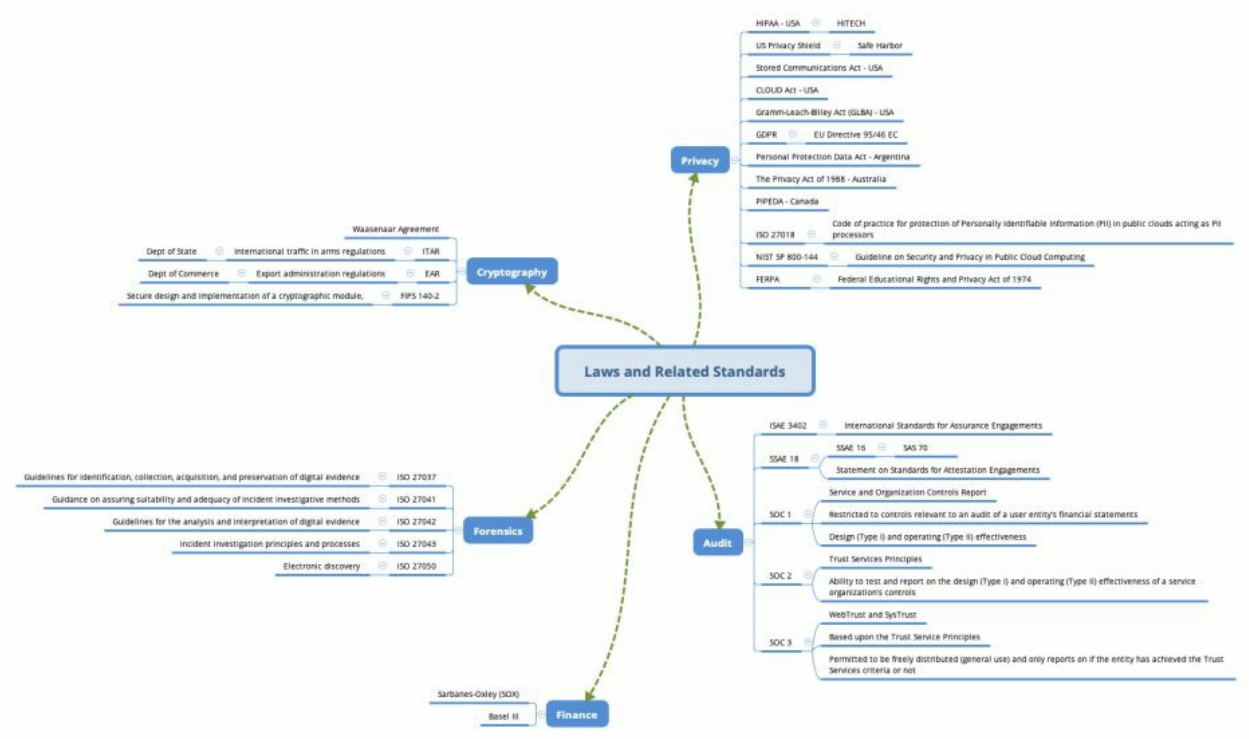
CMMI Institute. (2019). *CMMI*. Retrieved from CMMIInstitute.com: https://cmmiinstitute.com/cmmi

Google LLC. (n.d.). *Containers*. Retrieved from Google: www.cloud.google.com/containers

IBM. (2019). *What is quantum computing*. Retrieved from IBM.com: https://www.ibm.com/quantum-computing/learn/what-is-

quantum-computing/
Imperva, Inc. (2015). *Man_in_the_Cloud (MITC) Attacks*. Retrieved from Imperva Inc: www.Imperva.com/HII_Man_In_The_Cloud_Attacks.pdf
International Standards Organization. (2014, 10 15). 17788 Cloud Computing - Overview and Vocabulary. *Information Technology*. Switzerland: ISO.
ISO/IEC. (2008, 10). 21817 Systems Security Engineering - Capability Maturity Model. *Information Technology*. Switzerland.
ISO/IEC. (2018, July). 27005 Security Techniques - Information Security Risk Managment. *Information Technolgoy*. Switzerland: ISO.
NIST. (2011, September). Special Publication 800-145. *The NIST Definition of Cloud Computing*. National Institure of Standards and Technology, US Dept. of Commerce. Retrieved from National Institute of Standards and Technology.
Rosic, A. (2016). *What is Block Chain Technology?* Retrieved from BlockGeeks: https://blockgeeks.com/guides/what-is-blockchain-technology/
Staff, d. (2019, april 11). *What-is-Big-Data*. Retrieved from datascience.berkeley.edu: https://datascience.berkeley.edu/blog/what-is-big-data/
Strategi. (2009, April 14). *Abstraction-the-Key-Understanding-Cloud-Computing/*. Retrieved from Strategi.com: http://www.strategi.com/blog/abstraction-the-key-understanding-cloud-computing/
Top Threats Working Group. (2016). The Treacherous 12.
Uptime Institute. (n.d.). *Tier Classification System*. Retrieved from Tiers: https://uptimeinstitute.com/tiers
Wellers, W. J. (2019). *Why Machine Learning and Why Now?* SAP.


Cloud Architecture
Design Requirements
NIST SP 800-145 / ISO 17788
On Demand Self Service
Broad Network Access
Resource Pooling
Rapid Elasticity
Measured Service
Service Models/Categories
NIST SP 800-146 / ISO 17789
Software as a Service (SaaS)
Customer Responsibility
Limited Admin Control - Application
User Level Control - Application
Provider Responsibility
Admin Control - Application
Total Control - Middleware, OS, Hardware
Platform as a Service (PaaS)
Customer Responsibility
Admin Control - Application
Program to Interfaces - Middleware
Provider Responsibility
Admin Control - Middleware
Total Control - OS and Hardware
Infrastructure as a Service (IaaS)
Customer Responsibility
Total Control - Application, Middleware, Guest OS
Make Requests - Hypervisor
Provider Responsibility
Admin Control - Hypervisor
Total Control - Hypervisor, Hardware
Deployment Modes
NIST SP 800-145 / ISO 17788
Private Cloud
On Site
Outsourced
Public Cloud
Community Cloud
Hybrid Cloud
Cloud Related Standards
Risk
NIST SP 800-37
Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach
ISO 31000
Risk Management - Principles and Guidelines
COBIT
This series of documents has some of everything in it
ISO 27005
Information security risk management
ENISA IAF
Information Assurance Framework
FedRAMP
Federal Risk and Authorization Management Program
Software Architecture
Systems and Software Engineering - Architecture description
ISO 42010
Security Techniques - Application Security
ISO 27034
ISMS
Audit and Implementation
ISO 27001
Functional, Good Ideas
ISO 27002
Supply Chain
ISO 28000
ISO 27036
Information Security for supplier relationships
Supply Chain Management
Security Management Systems for the Supply Chain
ISO 28000
Information Security for Supplier Relationship
ISO 27036
Storage
ISO 27040
Threats to Storage types
BCM
ISO 22301
BS 25999
ISO 27031
ISO 27000
BS 17799
Cloud
Definition of Cloud Computing
NIST SP 800-145 + ISO 17788
Cloud Computing Synopsis
NIST SP 800-146 + ISO 17789
Security Reference Architecture
NIST SP 500-299
Cloud Computing - Overview and Vocabulary
ISO 17788
Cloud Computing - Reference Architecture
ISO 17789
Identity and Access Management
NIST 800-63 a,b,c
Product Testing
ISO 15408 (Common Criteria)
EAL 1 - Functionally tested
EAL 2 - Structurally tested
EAL 3 - Methodically tested and checked
EAL 4 Methodically designed tested and reviewed
EAL 5 - Semiformally verified designed and tested
EAL 6 - Semiformally designed tested and reviewed
EAL 7 - Formally verified designed and tested


Laws and Related Standards
Privacy
HIPAA - USA
HITECH
US Privacy Shield
Safe Harbor
Stored Communications Act - USA
CLOUD Act - USA
Gramm-Leach-Bliley Act (GLBA) - USA
GDPR
EU Directive 95/46 EC
Personal Protection Data Act - Argentina
The Privacy Act of 1988 - Australia
PIPEDA - Canada
ISO 27018
Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors
NIST SP 800-144
Guideline on Security and Privacy in Public Cloud Computing
FERPA
Federal Educational Rights and Privacy Act of 1974
Cryptography
Wassenaar Agreement
Dept of State
International traffic in arms regulations
ITAR
Dept of Commerce
Export administration regulations
EAR
Secure design and implementation of a cryptographic module,
FIPS 140-2
Forensics
Guidelines for identification, collection, acquisition, and preservation of digital evidence
ISO 27037
Guidance on assuring suitability and adequacy of incident investigative methods
ISO 27041
Guidelines for the analysis and interpretation of digital evidence
ISO 27042
Incident investigation principles and processes
ISO 27043
Electronic discovery
ISO 27050
Audit
ISAE 3402
International Standards for Assurance Engagements
SSAE 18
SSAE 16
SAS 70
Statement on Standards for Attestation Engagements
SOC 1
Service and Organization Controls Report
Restricted to controls relevant to an audit of a user entity's financial statements
Design (Type I) and operating (Type II) effectiveness
SOC 2
Trust Services Principles
Ability to test and report on the design (Type I) and operating (Type II) effectiveness of a service organization's controls
SOC 3
WebTrust and SysTrust
Based upon the Trust Service Principles
Permitted to be freely distributed (general use) and only reports on if the entity has achieved the Trust Services criteria or not
Finance
Sarbanes-Oxley (SOX)
Basel III

About The Author

Gwen Bettwy

Ms. Gwen Bettwy, CISSP-ISSAP, ISSMP, CISM, CISA, CCSP, SSCP, CCSI is CEO of Tactical Security Inc. located in Wellsville, Pennsylvania. Tactical Security, Inc. provides content development and knowledge product development services for the creation of Instructor Led Training (ILT), online, e-Learning training, and self-study knowledge products for Cyber Security curriculums and courseware. TSI incorporates instructional design methodology in the creation of knowledge transfer solutions for professional training and certification programs.

Her expertise is in the design, creation, and program management of large-scale development projects for ILT, online, e-Learning, or self-study knowledge products. Professional development services include: curriculum and courseware design, content development, online, e-Learning conversion, desktop publishing, and quality control for all TSI created curriculums, courseware, and content. Currently, Ms. Bettwy is an (ISC)2 Certified Instructor and teaches the CISSP, CISSP-ISSAP, CCSP, and SSCP CBK Review Seminars.

Ms. Bettwy training accomplishments include providing training services for industry leaders such as The Learning Tree, American Research Group, Global Knowledge, The Training Camp, and Firebrand. Her speaking

engagements include INTEROP, Hacker Halted and MISTI. Additionally, Ms. Bettwy served as a panel member at EMCOMWEST. Over her career Ms. Bettwy has taught courses at NSA, NASA, FEMA, US Army, US Navy, Novell, and Raytheon to name a few.

She lives in North Carolina with her dogs Sophie and Finneas.

I hope you enjoyed this book.

If you did please take a moment to write a review here.
Even the short review help a lot!