Term	Definition
Anything-as-a-Service	Anything-as-a-service, or "XaaS," refers to the growing diversity of services available over the Internet via cloud computing as opposed to being provided locally, or on premises
Apache CloudStack	open source cloud computing and Infrastructure as a Service (IaaS) platform developed to help Infrastructure as a Service make creating, deploying, and managing cloud services easier by providing a complete "stack" of features and components for cloud environments
Cloud Administrator	This individual is typically responsible for the implementation, monitoring, and maintenance of the cloud within the organization or on behalf of an organization (acting as a third party)
Application	Short for cloud application, cloud app is the phrase used to describe a software application that is never installed on a local computer. Instead, it is accessed via the Internet
Application Architect	Typically responsible for adapting, porting, or deploying an application to a target cloud environment
Application Management For Platforms	specification designed to ease management of applications — including packaging and deployment — across public and private cloud computing platforms
Cloud Architect	He or she will determine when and how a private cloud meets the policies and needs of an organization's strategic goals and contractual requirements (from a technical perspective)
Backup Service Provider	third-party entity that manages and distributes remote, cloud-based data backup services and solutions to customers from a central data center
Cloud Backup Solutions	Enable enterprises or individuals to store their data and computer files on the Internet using a storage service provider rather than storing the data locally on a physical disk, such as a hard drive or tape backup
Cloud Computing	type of computing, comparable to grid computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications
Cloud Computing Accounting Software	Accounting software that is hosted on remote servers
Cloud Computing Reseller	company that purchases hosting services from a cloud server hosting or cloud computing provider and then re-sells them to its own customers

Cloud Data Architect	Ensures the various storage types and mechanisms utilized within the cloud environment meet and conform to the relevant SLAs and that the storage components are functioning according to their specified requirements
Cloud Database	database accessible to clients from the cloud and delivered to users on demand via the Internet
Cloud Developer	Focuses on development for the cloud infrastructure itself. This role can vary from client tools or solutions engagements, through to systems components
Cloud Enablement	process of making available one or more of the following services and infrastructures to create a public cloud-computing environment: cloud provider, client, and application
Cloud Management	Software and technologies designed for operating and monitoring the applications, data, and services residing in the cloud. Cloud management tools help to ensure a company's cloud computing-based resources are working optimally and properly interacting with users and other services
Migration	process of transitioning all or part of a company's data, applications, and services from on-site premises behind the firewall to the cloud, where the information can be provided over the Internet on an on-demand basis
Cloud OS	phrase frequently used in place of Platform as a Service (PaaS) to denote an association to cloud computing
Portability	ability to move applications and its associated data between one cloud provider and another
Cloud Provider	service provider who offers customers storage or software solutions available via a public network, usually the Internet
Cloud Provisioning	deployment of a company's cloud computing strategy, which typically first involves selecting which applications and services will reside in the public cloud and which will remain on-site behind the firewall or in the private cloud
Cloud Server Hosting	type of hosting in which hosting services are made available to customers on demand via the Internet. Rather than being provided by a single server or virtual server, cloud server hosting services are provided by multiple connected servers that comprise a cloud
Cloud Services Broker	Typically a third-party entity or company that looks to extend or enhance value to multiple customers of cloud-based services through relationships with multiple cloud service providers

Cloud Storage	storage of data online in the cloud, wherein a company's data is stored in and accessible from multiple distributed and connected resources that comprise a cloud
Cloud Testing	Load and performance testing conducted on the applications and services provided via cloud computing — particularly the capability to access these services — in order to ensure optimal performance and scalability under a wide variety of conditions
Community Cloud	This cloud infrastructure is provisioned for exclusive use by a specific community of organizations with shared concerns
Converged Networking Model	Optimized for cloud deployments and utilizes standard perimeter protection measures. underlying storage and IP networks are converged to maximize the benefits for a cloud workload
Desktop-As-A-Service	form of virtual desktop infrastructure
Domain Name System	hierarchical, distributed database that contains mappings of DNS domain names to various types of data, such as Internet Protocol (IP) addresses
Domain Name System Security Extensions	suite of extensions that adds security to the Domain Name System (DNS) protocol by enabling DNS responses to be validated. Specifically, DNSSEC provides origin authority, data integrity, and authenticated denial of existence
Enterprise Application	term used to describe applications — or software — that a business would use to assist the organization in solving enterprise problems
Host Intrusion Detection Systems	Monitors the inbound and outbound packets from the device only and will alert the user or administrator if suspicious activity is detected
Hybrid Cloud	composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability
Hybrid Cloud Storage	combination of public cloud storage and private cloud storage where some critical data resides in the enterprise's private cloud while other data is stored and accessible from a public cloud storage provider
Logical Design	Part of the design phase of the SDLC in which all functional features of the system chosen for development in analysis are described independently of any computer platform
Mobile Cloud Storage	form of cloud storage that applies to storing an individual's mobile device data in the cloud and providing the individual with access to the data from anywhere

Multi-Tenancy	Data center networks that are logically divided into smaller, isolated networks. They share the physical networking gear but operate on their own network without visibility into the other logical networks
Online Backup	Leverages the Internet and cloud computing to create an attractive off-site storage solution with little hardware requirements for any business of any size
Oversubscription	Occurs when more users are connected to a system than can be fully supported at the same time
Personal Cloud Storage	form of cloud storage that applies to storing an individual's data in the cloud and providing the individual with access to the data from anywhere
Platform As A Service	way for customers to rent hardware, operating systems, storage, and network capacity over the Internet from a cloud service provider
Private Cloud	This cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on- or off-premises
Private Cloud Storage	form of cloud storage where the enterprise data and cloud storage resources both reside within the enterprise's data center and behind the firewall
Public Cloud	This cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider
Qualitative Assessments	Typically employ a set of methods, principles, or rules for assessing risk based on non-numerical categories or levels (e.g., very low, low, moderate, high, very high)
Quantitative Assessments	Typically employ a set of methods, principles, or rules for assessing risk based on the use of numbers. This type of assessment most effectively supports cost-benefit analyses of alternative risk responses or courses of action
Security Information And Event Management	method for analyzing risk in software systems. It is a centralized collection of monitoring of security and event logs from different systems. SIEM allows for the correlation of different events and early detection of attacks
Software As A Service	distributed model where software applications are hosted by a vendor or cloud service provider and made available to customers over network resources

Storage Clusters	use of two or more storage servers working together to increase performance, capacity, or reliability. Clustering distributes workloads to each server, manages the transfer of workloads between servers, and provides access to all files from any server regardless of the physical location of the file
Traditional Networking Model	layered approach with physical switches at the top layer and logical separation at the hypervisor level. =
Vendor Lock-In	Highlights where a customer may be unable to leave, migrate, or transfer to an alternate provider due to technical or non-technical constraints
Vertical Cloud Computing	optimization of cloud computing and cloud services for a particular vertical (e.g., a specific industry) or specific-use application
Virtualization Technologies	Enable cloud computing to become a real and scalable service offering due to the savings, sharing, and allocations of resources across multiple tenants and environments
Remote Desktop Protocol	protocol that allows for separate channels for carrying presentation data, serial device communication, licensing information, and highly encrypted data
Ballooning	process that allows the hypervisor to reclaim physical memory pages by forcing the virtual machine operating system to flush memory pages to disk.
Bandwidth	measure of network performance defined by the amount of data that can travel through the network over a period of time. Typically given in bits per seconds.
Bare-Metal	computer server without any operating system software installed.
Bridged Network	connection type that allows a virtual machine adapter to have a direct connection to the physical network with a unique IP address.
Central Processing Unit	core or brain of a computer where the user and system commands are executed. Today’s computers use microprocessor technology, and the term processor is often used interchangeably with CPU.
Clone	exact copy of a virtual machine. Once cloned, the new virtual machine still needs final customization to ensure a unique identity.
Common Internet File System	ocused on Microsoft Windows environments.
Compression	memory optimization technique that compresses memory pages and stores them in a designated cache in physical memory, rather than swap them from memory to disk storage.
Consolidation	practice of condensing multiple physical servers into one server through the use of virtualization.

Consolidation Ratio	measure of consolidation calculated by counting the number of virtual machines on an individual server.
Converged Network Adapter	single network adapter that supports multiple network-protocol types, usually at much greater bandwidths than older NICs.
Core	Microprocessors come in packages that contain one or more processing units. Each individual processing unit is a core.
Daemon	UNIX or Linux program that runs as a background process. Daemons typically perform certain system tasks such as cron (crond), the system scheduler, or managing the ftp capabilities (ftpd).
Data Center	large computer room, an entire floor in a building, or a separate building outfitted and dedicated to the health and well-being of a company’s computing infrastructure.
Deduplication	storage technology that compresses data and reclaims disk storage space by removing duplicate copies of information. Only one copy is retained and pointers to that copy replace the additional duplicates. Deduplication can be done on a byte, block, or file level.
Direct Attached Storage	disk drives that are internal to a physical computer.
Dynamic Host Configuration Protocol	is a widely used standard that allows servers to assign IP addresses to computers and other devices on a network.
Fault Tolerance	Hardware and/or software solutions and implementations that allow a server to lose one or more components to a failure without data loss or service interruption.
Fibre-Channel	industry standard protocol defined for connecting Storage Area Networks to computers.
Guest	virtual machine, or VM. Called a guest because it runs on a host server.
High Availability	Hardware and/or software solutions and implementations that provide greater uptime and resiliency for a computing infrastructure.
Host Bus Adapter	Also called a host adapter, it is a hardware device that connects a computer to either a network or a storage network. Originally associated with Fibre-Channel connectivity.
Human Interface Device	broad definition for a class of computer peripheral devices that either receive or deliver information to humans. Examples of these would be, but are not limited to, mice, touchpads, and joysticks. Newer candidates are Wii remotes and Kinect for Xbox.

Hyper-Threading	Intel microprocessor technology that improves performance by making more efficient use of the processing scheduling—effectively scheduling two threads of work where there was only one in the past.
Hypervisor	Originally called a Virtual Machine Manager, it is a layer of software that is installed either between an operating system and the virtual machines or directly onto the hardware, or “bare-metal,” and provides the environment in which the virtual machines operate.
Internet Small Computer System Interface	industry standard that defines how storage devices connect and transfer data to computers by sending the SCSI commands over Ethernet networks.
Linux	open-source operating system that is a UNIX derivative. Usually available for low or no cost, Linux runs on a wide variety of hardware, including mainframe computers, servers, desktops, mobile devices, and other commercial appliances such as cable/satellite boxes, and video game consoles.
Load Balancer	hardware or software appliance that balances traffic from multiple sources, preventing one pathway from being overloaded. Load balancers can also redirect traffic in the event of a pathway failure.
Memory Overcommit	ability of a hypervisor to allocate more virtual memory to its virtual machines than the amount of physical memory in the host it resides on through the use of memory management optimizations.
Modem	device that turns digital signals into analog signals and back again. modem allows a user on one computer to connect and share data with a second computer by using a telephone line as the transfer medium. base technology has evolved and is still in wide use today.
Multicore	microprocessor that contains more than one processing unit.
Multipathing	Having more than one path available from data storage to a server by having multiple I/O controllers, network switches, and NIC cards.
Network Address Translation	connection type that allows a virtual machine to share an IP address on the physical network with other virtual machines. Each virtual machine has a unique local address that is translated to the shared address for outbound traffic, and back again for inbound traffic for proper data delivery.
Network Attached Storage	disk storage that is connected to one or more computers across a network by a file-based protocol, such as CIFS or NFS. As a file-based system, network attached storage has file systems created and managed external to the computer systems it supports.

Network File System	is an open industry protocol standard that is typically used for computers to access Network Attached Storage systems.
Network Interface Card	device that allows a computer to connect to a network. Also called a network adapter.
Network Switch	device that connects computers, printers, file servers, and other devices, allowing them to communicate efficiently with each other. In some ways, switches create and define the networks that they manage.
Network Time Protocol	is an open standard that defines and implements a computer’s ability to synchronize with Internet time servers, or with other servers.
Open Virtualization Format	platform-independent industry standard that defines a format for the packaging and distribution of virtual machines.
Page Sharing	memory optimization technique in which identical pages in memory are stored only as a single copy and shared between multiple virtual machines. Also works for identical pages in one virtual machine. Similar to disk storage deduplication.
Paging	process that computers use to copy blocks, or pages, of data from disk to memory and back again.
Physical To Virtual	manual or automated process that transfers the data on a physical server into a virtual machine. data includes the operating system, applications files, and all data files.
Resource Pool	aggregation of resources that permits a virtualization administrator to allocate resources to virtual machines, groups of virtual machines, or groups of people.
Small Computer System Interface	is the industry standard that defines how storage devices connect and transfer data to computers.
Snapshot	snapshot is a set of files that preserve the state of a virtual machine at a given point in time so you can repeatedly revert back to that given state. virtual machine can have multiple snapshots.
Storage Area Network	Storage Area Network. combination of networking resources and disk arrays that provides data storage for computers. Multiple computers will access the SAN, which is external to the physical (or virtual) servers.
Symmetric Multiprocessing Virtualization	computer architecture that provides enhanced performance through the concurrent use of multiple processors and shared memory.

Template	virtual machine that is used as a mold for a commonly used configuration. Once deployed from a template, the virtual machine still needs final customization, such as a system name and network information.
Universal Service Bus	an industry standard for connecting external devices to a computer. standard defines the physical connections as well as the capabilities for the disparate devices it can support. In addition to data transfer, USB devices can draw electricity from the computer they are connected to for operational power or, in the case of mobile devices, to recharge their internal batteries.
vCPU	virtual representation of a computer processor.
Virtual Machine	container that runs a guest operating system and applications in a software abstraction of a physical server. powered-off virtual machine is merely a set of files that comprise and describe the virtual hardware and the data that make up the virtual machine.
Virtualization	process by which physical servers are abstracted into software constructs that, from their user's standpoint, appear and behave identically to their physical counterparts.
VM-Affinity (And Anti-Affinity)	Rules that link together two or more virtual machines so they reside on the same virtualization host. Anti-affinity rules ensure that two machines do not reside on the same virtualization host. Live migration, automatic and manual, as well as high-availability recovery, will respect these rules.
Vmware Tools	combination of device drivers and processes that enhance the user's experience with the virtual machine, improve virtual machine performance, and help manage the virtual machine. VMware tools is specific to VMware, but other virtualization vendors provide similar suites.
Anonymization	act of permanently and completely removing personal identifiers from data, such as converting personally identifiable information (PII) into aggregated data
Bit Splitting	Usually involves splitting up and storing encrypted information across different cloud storage services
Control	Acts as a mechanism to restrict a list of possible actions down to allowed or permitted actions
Crypto-Shredding	process of deliberately destroying the encryption keys that were used to encrypt the data originally
Data Loss Prevention	Audit and prevent unauthorized data exfiltration

Degaussing	Using strong magnets for scrambling data on magnetic media such as hard drives and tapes
Digital Rights Management	Focuses on security and encryption to prevent unauthorized copying limit distribution to only those who pay
Encryption	overt secret writing technique that uses a bidirectional algorithm in which humanly readable information is converted into humanly unintelligible information
Encryption Key	special mathematical code that allows encryption hardware/software to encode and then decipher an encrypted message
Homomorphic Encryption	Enables processing of encrypted data without the need to decrypt the data. It allows the cloud customer to upload data to a cloud service provider for processing without the requirement to decipher the data first
Key Management	generation, storage, distribution, deletion, archiving, and application of keys in accordance with a security policy
Masking	weak form of confidentiality assurance that replaces the original information with asterisks or X's
Non-Repudiation	assurance that a specific author actually did create and send a specific item to a specific recipient, and that it was successfully received. With assurance of non-repudiation, the sender of the message cannot later credibly deny having sent the message, nor can the recipient credibly claim not to have received it
Obfuscation	convoluting of code to such a degree that even if the source code is obtained, it is not easily decipherable
Personal Data	Any information relating to an identified or identifiable natural person data subject; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity
Record	data structure or collection of information that must be retained by an organization for legal, regulatory or business reasons
Service Level Agreement	formal agreement between two or more organizations: one that provides a service and the other the recipient of the service. It may be a legal contract with incentives and penalties
Tokenization	process of replacing sensitive data with unique identification symbols that retain all the essential information about the data without compromising its security.
Activation	to start business continuity processes

Alert	Notification that a potential disaster situation exists or has occurred
Alternate Site	location to perform the business function
Backup	copy of files and programs made to facilitate recovery if necessary.
Business Continuity Plan	documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.
Business Continuity Program	ongoing process supported and funded by executive staff to ensure business continuity requirements are assessed, resources are allocated and, recovery and continuity strategies and procedures are completed and tested.
Business Continuity Steering Committee	group of decision makers, business owners, technology experts and continuity professionals, tasked with making strategic recovery and continuity planning decisions for the organization.
Business Impact Analysis	detailed review of information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.
Business Interruption	Any event, whether anticipated or unanticipated which stops the normal course of business operations at an organization location.
Business Interruption Insurance	contract to pay for disaster related expenses that may be incurred until operations are fully recovered.
Business Recovery Team	group of individuals responsible for maintaining the procedures and coordinating return of business functions and processes.
Business Recovery Timeline	chronological sequence of recovery activities, or critical path, that must be followed to resume an acceptable level of operations following a business interruption. may range from minutes to weeks, depending upon requirements and methodology.
Business Unit Recovery	component which deals specifically with the relocation of a key function or department in the event of a disaster.
Call Tree	internal list of contact information used for the communication of incident information, designed in a distributed manor so that no one person is responsible for contacting everyone.
Checklist Test	(desk check) a test that answers the questions: Does the organization have the documentation it needs? Can it be located?
Cold Site	recovery alternative, a building only with sufficient power, and HVAC

Continuity Of Operations Plan	predetermined set of instructions or procedures that describe how an organization's mission essential functions will be sustained within 12 hours and for up to 30 days as a result of a disaster event before returning to normal operations.
Coordinator	person responsible for overall recovery of an organization or unit(s).
Crisis	critical event, which may dramatically impact an organization's profitability, reputation, or ability to operate.
Critical Functions	Business activities or information that could not be interrupted or unavailable for several business days without significantly jeopardizing operation of the organization.
Critical Infrastructure	Systems whose incapacity or destruction would have a debilitating impact on the economic security of an organization
Critical Records	documents that, if lost, would cause considerable inconvenience and/or require replacement or recreation at considerable expense.
Data Backup Strategies	processes determined by an organization to be necessary to meet its recovery and restoration objectives. these will determine the timeframes, technologies, media and offsite storage of the backups, and will ensure that recovery point and time objectives can be met.
Data Backups	confidential system, application, program and/or production files on media that can be stored both on and/or offsite.
Data Recovery	restoration of computer files from backup media to restore programs and production data to the state that existed at the time of the last safe backup.
Database Replication	partial or full duplication of data from source to one or more destinations.
Declaration	formal announcement by pre-authorized personnel that a disaster or severe outage is predicted or has occurred and that triggers pre-arranged mitigating actions.
Desk Check Test	test that answers the questions: Does the organization have the documentation and people it needs. Do they understand the documentation?
Disaster	an event which stops business from continuing.
Disaster Recovery Plan	written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.
Disaster Recovery Teams	structured group of teams ready to take control of the recovery operations if a disaster should occur.
Disk Mirroring	Disk mirroring is the duplication of data on separate disks in real time to ensure its continuous availability, currency and accuracy.

Disruption	unplanned event that causes an information system to be inoperable for a length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).
Distributed Processing	a back up type, where the organization has excess capacity in another location.
Drills - Test	practice of activity typically targeted to a specific response. purpose is to have the participants follow the designated response activities specified in their plans to become more proficient in executing the response activity.
Electronic Vaulting	transmission of backup data to an offsite facility; it eliminates the need for tape shipment and therefore significantly shortens the time required to move the data offsite.
Emergency	sudden, unexpected event requiring immediate action due to potential threat to health and safety, the environment, or property.
Emergency Operations Center	location where coordination and execution of BCP or DRP is directed
Emergency Procedures	plan of action to commence immediately to prevent the loss of life and minimize injury and property damage.
Executive Succession	planning for the delegation of authority required when decisions must be made without the normal chain of command
Exercise	activity that is performed for the purpose of training and conditioning team members, and improving their performance.
File Shadowing	asynchronous duplication of the production database on separate media to ensure data availability, currency and accuracy.
Forward Recovery	process of recovering a database to the point of failure by applying active journal or log data to the current backup files of the database.
Full Interruption Test	live, very high risk test.
Hot Site	recovery alternative, everything needed for the business function, except people and last backup
Impact	magnitude of harm that can be expected to result from consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.
Impact Level	classify the intensity of a potential impact that may occur if the information system is jeopardized.

Incident Manager	highest level of authority at EOC with knowledge of the business process and the resources available
Incident Response Plan	documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's information system(s).
Information System Contingency Plan	management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disasters.
Integrated Test	test conducted on multiple components of a plan, in conjunction with each other, typically under simulated operating conditions
Journaling	process of logging single changes or updates to a database since the last full backup.
Live Walk-Through Test	an exercise where the plan is executed as if a real disaster has taken place at a specific point in the facility and is typically conducted with multiple BC/DR teams. (simulation test)
Maximum Tolerable Downtime	amount of time mission/business process can be disrupted without causing significant harm to the organization's mission.
Mirrored Site	recovery alternative, complete duplication of services including personnel
Mission-Critical Application	essential to the organization’s ability to perform necessary business functions.
Mobile Site	recovery alternative, short-term, high cost movable processing location
Near Site	backup of data located where staff can gain access readily and a localized disaster will not cause harm
Off Site	backup of data located where staff can not gain access readily and a regional disaster will not cause harm
On-Site	backup of data located where staff can gain access immediately
Operational Impact Analysis	determines the signifigance of the loss of an operational or technological resource. loss of a system, network or other critical resource may affect a number of business processes.
Operational Test	test conducted on one or more components of a plan under actual operating conditions.
Parallel Test	operational test is held at the same time with the actual processing of critical systems to ensure that the systems will run correctly at the alternative site.

Reciprocal Agreement	between two organizations (or two internal business groups) with basically the same equipment/same environment that allows each one to recover at each other's site.
Recovery Period	time period between a disaster and a return to normal functions, during which the disaster recovery plan is employed.
Recovery Point Objective	determinant of the amount of data that may need to be recreated after the systems or functions have been recovered.
Recovery Time Objective	target time which respects tolerance for loss of certain business function, basis of strategy
Remote Journaling	database backup type which records at the transaction level
Replication	backup type which creates a complete copy
Resilience	bility to quickly adapt and recover from any known or unknown changes to the environment through holistic implementation of risk management, contingency, and continuity planning.
Restoration	planning with a goal of returning to the normal business function
Resumption	process of planning for and/or implementing the restarting of defined business operations following a disaster, usually beginning with the most critical or time-sensitive functions first.
Risk Mitigation	Implementation of measures to limit specific threats to the continuity of business operations, and/or respond to any occurrence of such threats in a timely and appropriate manner.
Service Bureau	recovery alternative which outsources a business function at a cost
Shadowing	backup type, for databases at a point in time
Simulation	scenario based test that answers the question: Can the organization replicate the business process?
Standalone Test	test conducted on a specific component of a plan, in isolation from other components, typically under simulated operating conditions.
Structured Walkthrough	One method of testing a specific component of a plan. Typically, a team member makes a detailed presentation of the component to other team members (and possibly non-members) for their critique and evaluation.
System Development Life Cycle	scope of activities associated with initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal
System Downtime	planned or unplanned interruption in system availability.

Tabletop Walk-Through Test	is a test that exercises all or part of the BC/DR plan as specified in the scope of the test plan.
Test Plan	document designed to periodically exercise specific action tasks and procedures to ensure viability in a real disaster.
Triage	to evaluate the current situation and make basic decisions as to what to do
Walk-Through Test	first test conducted to familiarize the team leader and members with the plan. It addresses all components of the BC/ DR plan.
Warm Site	recovery alternative which includes cold site and some equipment and infrastructure is available
Application Normative Framework	subset of the ONF that will contain only the information required for a specific business application to reach the targeted level of trust
Application Programming Interfaces	set of routines, standards, protocols, and tools for building software applications to access a Web-based software application or Web tool
Application Virtualization	Software technology that encapsulates application software from the underlying operating system on which it is executed
Data Masking	method of creating a structurally similar but inauthentic version of an organization's data that can be used for purposes such as software testing and user training
Database Activity Monitoring	database security technology for monitoring and analyzing database activity that operates independently of the database management system (DBMS) and does not rely on any form of native (DBMS-resident) auditing or native logs such as trace or transaction logs
Dynamic Application Security Testing	process of testing an application or software product in an operating state
Federated Identity Management	arrangement that can be made among multiple enterprises that lets subscribers use the same identification data to obtain access to the networks of all enterprises in the group
Federated Single Sign-On	allow a single user authentication process across multiple IT systems or even organizations. SSO is a subset of federated identity management, as it relates only to authentication and technical interoperability
Identity and Access Management	security discipline that enables the right individuals to access the right resources at the right times for the right reasons

Multi-Factor Authentication	method of computer access control which a user can pass by successfully presenting authentication factors from at least two of the three categories: knowledge factors, such as passwords. Combines two or more independent credentials: what the user knows, what the user has and what the user is
Organizational Normative Framework	framework of so-called containers for all components of application security best practices catalogued and leveraged by the organization
Quality Of Service	Refers to the capability of a network to provide better service to selected network traffic over various technologies, including Frame Relay, Asynchronous Transfer Mode (ATM), Ethernet and 802.1 networks, SONET, and IP-routed networks that may use any or all of these underlying technologies
Sandbox	testing environment that isolates untested code changes and outright experimentation from the production environment or repository, in the context of software development including Web development and revision control
Security Assertion Markup Language	standard for exchanging authentication and authorization data between security domains
Static Application Security Testing	set of technologies designed to analyze application source code, byte code and binaries for coding and design conditions that are indicative of security vulnerabilities
STRIDE Threat Model	Derived from an acronym for the following six threat categories; Spoofing identity, Tampering with data, Repudiation, Information disclosure, Denial of service, Elevation of privilege
Web Application Firewall	appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection
Analysis	third phase of the computer and network forensic process, which involves using legally justifiable methods and techniques, to derive useful information that addresses the questions that were the impetus for performing the collection and examination.
Anti-Forensic	technique for concealing or destroying data so that others cannot access it.
Collection	first phase of the computer and network forensics process, which involves identifying, labeling, recording, and acquiring data from the possible sources of relevant data, while following guidelines and procedures that preserve the integrity of the data.

Directory	Organizational structures that are used to group files together.
Disk Imaging	Generating a bit-for-bit copy of the original media, including free space and slack space. Also known as a bit stream image.
Forensically Clean	Digital media that is completely wiped of all data, including nonessential and residual data, scanned for malware, and verified before use.
Logical Backup	copy of the directories and files of a logical volume.
Logical Volume	partition or a collection of partitions acting as a single entity that has been formatted with a filesystem.
Network Intrusion Detection System	Software that performs packet sniffing and network traffic analysis to identify suspicious activity and record relevant information.
Network Traffic	Computer network communications that are carried over wired or wireless networks between hosts.
Non-Volatile Data	Data that persists even after a computer is powered down.
Packet	logical unit of network communications produced by the transport layer.
Reporting	final phase of the computer and network forensic process, which involves reporting the results of the analysis; this may include describing the actions used, explaining how tools and procedures were selected, determining what other actions need to be performed (e.g., forensic examination of additional data sources, securing identified vulnerabilities, improving existing security controls), and providing recommendations for improvement to policies, guidelines, procedures, tools, and other aspects of the forensic process. formality of the reporting step varies greatly depending on the situation.
Slack Space	unused space in a file allocation block or memory page that may hold residual data.
Volatile Data	Data on a live system that is lost after a computer is powered down.
Wiping	Overwriting media or portions of media with random or constant values to hinder the collection of data.
5 Rules Of Evidence	evidence must be: admissible, authentic, complete, accurate, and convincing
Accurate	pertaining to law, high degree of veracity
Administrative Law	a set of laws that the organization agrees to be bound by
Admissible	pertaining to law, accepted by a court
Archival Data	information that the organization maintains for long-term storage and record keeping purposes

Attacker	black hat, someone who wants to cause harm
Authentic	pertaining to law, verified as real
Baselining	Monitoring resources to determine typical utilization patterns so that significant deviations can be detected.
Bit	measurement of data. It is the smallest unit of data. bit is either the "1" or "0" component of the binary code.
Bit Stream Imaging	bit-for-bit copy of the original media, including free space and slack space. Also known as disk imaging.
Boot	To load the first piece of software that starts a computer.
Byte	Eight bits.
Byte Level Deletion	may render the data inaccessible to the application intended to be used in processing the file, but may not actually remove the data
Cache	type a computer memory that temporarily stores frequently used information for quick access.
Chain Of Custody	recording the Who What When Where How of evidence
Civil Or Code Law	system of law based upon what is good for society
Cluster	group of contiguous sectors.
Common Law	system of law based upon precedence, with major divisions of criminal, tort, and administrative
Complete	pertaining to law, no omissions
Computer Forensics	practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.
Containment	to stop damage from spreading
Convincing	pertaining to law, lending it self to one side of an argument
Cookie	Small data files written to a user's hard drive by a web server.
Criminal Law	wrong against society
Data	Distinct pieces of digital information that have been formatted in a specific way.
Debriefing/Feedback	communicate to stakeholders
Deleted File	disk space it used to occupy has been designated by the computer as available for reuse. deleted file remains intact until it has been overwritten with a new file.
Digital Forensics	application of science to the identification, collection, examination, and analysis, of data while preserving the integrity of the information and maintaining a strict chain of custody for the data.

Disk-To-Disk Copy	Copying the contents of media directly to another media.
Disk-To-File Copy	Copying the contents of media to a single logical data file.
Due Care	policy or stated actions
Due Diligence	actions measured against either a policy or what a reasonable person would do
Egress Filtering	process of blocking outgoing packets that use obviously false Internet Protocol (IP) addresses, such as source addresses from internal networks.
Event	Any observable occurrence in a network or system.
Examination	second phase of the computer and network forensics process, which involves forensically processing large amounts of collected data using a combination of automated and manual methods to assess and extract data of particular interest, while preserving the integrity of the data.
False Negative	Incorrectly classifying malicious activity as benign.
False Positive	Incorrectly classifying benign activity as malicious.
File	collection of information logically grouped into a single entity and referenced by a unique name, such as a filename.
File Allocation Unit	group of contiguous sectors, also known as a cluster.
File Extension	tag of three or four letters, preceded by a period, which identifies a data file's format or the application used to create the file.
File Header	Data within a file that contains identifying information about the file and possibly metadata with information about the file contents.
File Integrity Checker	Software that generates, stores, and compares message digests for files to detect changes to the files.
File Level Deletion	Deletion on the file level renders the file inaccessible to the operating system, available to reuse for data storage.
File Sharing	One of the key benefits of a network is the ability to share files stored on the server among several users.
Filename	unique name used to reference a file.
Filesystem	method for naming, storing, organizing, and accessing files on logical volumes.
Firewall	system designed to prevent unauthorized access to or from a private network.
Forensic Copy	exact bit-by-bit copy of the entire physical hard drive or floppy disk, including slack and unallocated space. Only forensic copy quality will hold up in court.

Fragmented Data	Fragmented data is live data that has been broken up and stored in various locations on a single hard drive or disk.
Free Space	area on media or within memory that is not allocated.
Hard Disk	data storage device that may be found inside a computer as permanent storage solution. may also be a transportable version.
Hearsay	third party evidence or weak evidence as opposed to direct evidence.
Honeypot	a computer designed for the purpose of studying adversaries
Incident	event(s) that cause harm
Indication	sign that an incident may have occurred or may be currently occurring.
Ingress Filtering	process of blocking incoming packets that use obviously false IP addresses, such as reserved source addresses.
Intrusion Detection And Prevention System	Software that automates the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents.
Investigation	methodical research of an incident with the purpose of finding the root cause
Legacy Data	Information which has been created or stored by the use of software and/or hardware that has been rendered obsolete.
Liability	responsibility for actions
Message Digest	hash that uniquely identifies data. Changing a single bit in the data stream used to generate the message digest will yield a completely different message digest.
Metadata	Information about a particular data set
Mirroring	duplication of data for purposes of backup or to distribute network traffic among several computers with identical data.
Multiple Component Incident	single incident that encompasses two or more incidents.
Normalize	process by which differently formatted data is converted into a standardized format and labeled consistently.
Operating System	program that runs on a computer and provides a software platform on which other programs can run.
Packet Sniffer	Software that observes and records network traffic.
Partition	logical portion of a media that functions as though it were physically separate from other logical portions of the media.
Patent	intellectual property protection for an invention

Pointer	index entry in the directory of a disk that identifies the space on the disk in which an electronic document or piece of electronic data resides
Port Scanning	Using a program to remotely determine which ports on a system are open (e.g., whether systems allow connections through those ports).
Proxy	Software that receives a request from a client, then sends a request on the client.s behalf to the desired destination.
Record Level Deletion	Renders the record inaccessible to the database management system
Recovery	return to a normal state
Remote Access Server	Devices, such as virtual private network gateways and modem servers, that facilitate connections between networks.
Residual Data	or Ambient Data - data that is not active on a computer system.
Sector	smallest unit that can be accessed on media.
Security Event Management Software	Software that imports security event information from multiple data sources, normalizes the data, and correlates events among the data sources.
Signature	recognizable, distinguishing pattern associated with an attack, such as a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a system.
Steganography	Embedding data within other data to conceal it.
Subdirectory	directory contained within another directory.
Threat	potential source of an adverse event.
Write-Blocker	tool that prevents all computer storage media connected to a computer from being written to or modified.
Common Vulnerabilities And Exposures	Identifies high level requirements for enumerating common vulnerabilities that can be used to exchange continuous monitoring cybersecurity information.
Common Vulnerability Scoring System	vulnerability scoring system designed to provide a method for rating IT vulnerabilities in a manner that helps organizations prioritize and coordinate a joint response to security cloud computing vulnerabilities by communicating the properties of the vulnerability.
Extensible Markup Language	set of rules for encoding documents in machine-readable form. XML's design goals emphasize simplicity, generality, and usability over the Internet. It is a textual data format with strong support via Unicode for the languages of the world. Although the design of XML focuses on documents, it is widely used for the representation of arbitrary data structures, for example in web services.

File Transfer Protocol	standard network protocol used to copy a file from one host to another over a TCP/IP-based network, such as the Internet. FTP is built on a client-server architecture and utilizes separate control and data connections between the client and server. FTP users may authenticate themselves using a clear-text sign-in protocol but can connect anonymously if the server is configured to allow it.
Hypertext Markup Language	language for web pages
Hypertext Transfer Protocol	networking protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web.
Internet Protocol Suite	set of communications protocols used for the Internet and other similar networks. It is commonly also known as TCP/IP, named from two of the most important protocols in it: the Transmission Control Protocol (TCP) and the Internet Protocol (IP), which were the first two networking protocols defined in this standard.
Javascript Object Notation	lightweight text-based open standard designed for human-readable data interchange. It is derived from the JavaScript programming language for representing simple data structures and associative arrays, called objects. Despite its relationship to JavaScript, it is language-independent, with parsers available for virtually every programming language.
Key Management Interoperability Protocol	defines a single, comprehensive protocol for communication between encryption systems and a broad range of new and legacy enterprise applications, including email, databases, and storage devices. By removing redundant, incompatible key management processes, KMIP will provide better data security while at the same time reducing expenditures on multiple products. KMIP specification covers both the syntax for encoding key data and the protocols/APIs of how client interacts with server to perform key management related tasks using these encoded messages.
Representational State Transfer	architectural pattern for use of application-layer communications in a manner that uses standards, but is not a standard in and of itself. primary programming paradigm for the use of REST is that access to a given resource returns a representation of that resource, putting the client application into a state. REST accesses and returned data can take place over any application-layer protocol and are not limited to HTTP.
Security Content Automation Protocol	Provides guidelines for the development of a continuous monitoring program that provides visibility into organizational assets, awareness of threats and vulnerabilities as well as the effectiveness of security controls.

Simple Mail Transfer Protocol	standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.
Simple Object Access Protocol	protocol specification for exchanging structured information in the implementation of Web Services in computer networks. SOAP can form the foundation layer of a web services protocol stack, providing a basic messaging framework upon which web services can be built. SOAP is a strongly-typed variant of XML-based communication that provides a full description of the required actions taken by a SOAP node on receiving a SOAP message. To resolve ambiguities inherent in the specification, this protocol is generally used according to specific restrictions and clarifications encoded into externally documented profiles. (use of SOAP in web services settings, for example, is carried out in the context of the WS-Interoperability Basic Profile.)
Transport Layer Security	cryptographic protocols that "provide communications security over the Internet". above the Transport Layer, using symmetric cryptography for privacy and a keyed message authentication code for message reliability.
X.509 Public Key Infrastructure Certificate	Defines a standard method of production for proxy certificates, including the ability to support extended attribute certificates conforming to an external profile. Such certificates can be used to convey delegation information and policy restrictions for use of PKI-based credentials in remote settings.
XML Path Language	language for addressing parts of a document. It is based on a tree representation and provides methods to navigate, select nodes from, and perform manipulations on the tree elements. While there is a 2.0 specification available, the 1.0 subset is interpreted correctly and so can be used by 2.0-compliant implementations.
Aggregated Information	Information elements collated on a number of individuals, typically used for the purposes of making comparisons or identifying patterns.
Anonymized Information	Previously identifiable information that has been de-identified and for which a code or other association for re-identification no longer exists.
Confidentiality	“Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Context Of Use	purpose for which PII is collected, stored, used, processed, disclosed, or disseminated.

De-Identified Information	Records that have had enough PII removed or obscured such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual.
Distinguishable Information	Information that can be used to identify an individual.
Harm	Any adverse effects that would be experienced by an individual (i.e., that may be socially, physically, or financially damaging) or an organization if the confidentiality of PII were breached.
Linkable Information	Information about or related to an individual for which there is a possibility of logical association with other information about the individual.
Linked Information	Information about or related to an individual that is logically associated with other information about the individual.
Obscured Data	Data that has been distorted by cryptographic or other means to hide information. It is also referred to as being masked or obfuscated.
Personally Identifiable Information	Information that can be traced back to an individual user, e.g. your name, postal address, or e-mail address. Personal user preferences tracked by a Web site via a cookie is also considered personally identifiable when linked to other personally identifiable information provided by you online
Confidentiality Impact Level	PII confidentiality impact level—low, moderate, or high—indicates the potential harm that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.
Privacy Impact Assessment	"analysis of how information is handled that ensures handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; determines the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronicinformation system; and examines and evaluates protections and alternative processes for handling information to mitigate potential privacy risks.‖101
System Of Records	"group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual
Traceable	Information that is sufficient to make a determination about a specific aspect of an individual's activities or status.

Australian Privacy Act 1988	Regulates the handling of personal information about individuals. This includes the collection, use, storage, and disclosure of personal information, and access to and correction of that information.
Doctrine Of The Proper Law	When a conflict of laws occurs, this determines in which jurisdiction the dispute will be heard.
Ediscovery	Refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case.
Eu General Data Protection Regulation 2012	Will introduce many significant changes for data processors and controllers. following may be considered as some of the more significant changes: concept of consent, Transfers Abroad, right to be forgotten, Establishment of the role of the "Data Protection Officer", Access Requests, Home State Regulation, Increased Sanctions
Gramm-Leach-Bliley Act (Glba)	Federal law enacted in the United States to control the ways that financial institutions deal with the private information of individuals.
Health Insurance Portability And Accountability Act	Adopt national standards for electronic healthcare transactions and national identifiers for providers, health plans, and employers. Protected Health information can be stored via cloud computing under HIPAA.
Information Gathering	Refers to the process of identifying, collecting, documenting, structuring, and communicating information from various sources in order to enable educated and swift decision making to occur.
ISO 27018	Address the privacy aspects of cloud computing for consumers and is the first international set of privacy controls in the cloud.
Sarbanes Oxley Act (SOX)	Legislation enacted to protect shareholders and the general public from accounting errors and fraudulent practices in the enterprise.
Service Organization Controls 1 (Soc 1)	Reports on Controls at Service organizations relevant to user entities' Internal Control over financial reporting.
Service Organization Controls 2 (Soc 2)	Reports on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy.
Stored Communication Act	Enacted in the United States in 1986 as part of the Electronic Communications Privacy Act. It provides privacy protections for certain electronic communication and computing services from unauthorized access or interception.
Tort Law	body of rights, obligations, and remedies that sets out reliefs for persons suffering harm as a result of the wrongful acts of others.

Qualitative	a risk assessment method, intrinsic value
Quantitative	a risk assessment method, measurable real money cost
Residual Risk	quantity of risk remaining after a control is applied
Risk	the chance that something negative will occur
Risk Assessment	the collection and summation of risk data relating to a particular asset and controls for that asset
Risk Management	total process of identifying, controlling, and mitigating information system–related risks. It includes risk assessment; cost-benefit analysis; and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws.
Threat Agent	those who initiate the attack
Threat Analysis	examination of threat-sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment.
Threat-Source	Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability.
Threats	vehicle or tool that exploits a weakness
Total Risk	calculation encompassing threats, vulnerabilities and assets
Transfer	a choice in risk management, to convince another to assume risk, typically by payment
Vulnerability	weakness or flaw in an asset
Authentication	act of identifying or verifying the eligibility of a station, originator, or individual to access specific categories of information. Typically, a measure designed to protect against fraudulent transmissions by establishing the validity of a transmission, message, station, or originator
Authorization	granting of right of access to a user, program, or process
Content Delivery Network	service where data is replicated across the global Internet
Corporate Governance	relationship between the shareholders and other stakeholders in the organization versus the senior management of the corporation
Demilitarized Zone	Isolates network elements such as e-mail servers that, because they can be accessed from trustless networks, are exposed to external attacks
Enterprise Risk Management	set of processes and structure to systematically manage all risks to the enterprise

Hardware Security Module	device that can safely store and manage encryption keys. This can be used in servers, data transmission, protecting log files, etc
Management Plane	Controls the entire infrastructure, and parts of it will be exposed to customers independent of network location, it is a prime resource to protect
Object Storage	files are stored with additional metadata (content type, redundancy required, creation date, etc.). These objects are accessible through APIs and potentially through a web user interface
Redundant Array of Inexpensive Disks	Instead of using one large disk to store data, one can use many smaller disks
Cloud Controls Matrix	framework to enable cooperation between cloud consumers and cloud providers on demonstrating adequate risk management
Software Defined Networking	broad and developing concept addressing the management of the various network components.