CSA Data Security Glossary

cloud security alliance®

The permanent and official location for Data Security Working Group is https://cloudsecurityalliance.org/research/working-groups/data-security/

© 2024 Cloud Security Alliance – All Rights Reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance at https://cloudsecurityalliance.org subject to the following: (a) the draft may be used solely for your personal, informational, non-commercial use; (b) the draft may not be modified or altered in any way; (c) the draft may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the draft as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance.

Acknowledgments

Lead Authors

Alex Kaluza
Oliver Forbes
Rocco Alfonzetti
Onyeka Illoh

Contributors

Michael Roza
Pan Maszyna
Paola Garcia Cardenas
Parth Jamodkar
Sanjeewa Fernando

CSA Global Staff

Claire Lehnert
Stephen Lumpe

Purpose

Identify, define, and reference relevant data security terms to assist cybersecurity professionals and practitioners to better comprehend data security. Based on the CSA Cloud Security Glossary and other sources, this compilation of relevant data security terms will serve as a foundational reference for Data Security working group publications.

Process

- Identify and alphabetically list terms that are relevant to data security
- Add applicable terms that are referenced from the CSA Glossary, NIST Glossary, and other public sources
- Include and review suggested definitions from Data Security working group members
- Include and review suggested definitions from public peer review suggestions
- Finalize definitions and references

Cloud Security Glossary: https://cloudsecurityalliance.org/cloud-security-glossary/

Data Security Glossary

Term	Definition
Access Control Lists (ACLs)	Indicate the permissions that subjects are granted regarding accessing or changing the objects within a system. Source: Enterprise Architecture Reference Guide v2 : CSA: Technology Solution Services (TSS) Domain - Information Services
Adversarial Simulation	The practice of security experts impersonating the actions and behaviors of skilled cyber threat actors to attack an organization's information technology or operational technology environment. Using real-world attacker breach techniques and a feedback loop from the organization's security stack, adversary simulation exercises help test and improve cyber resilience against attacks such as ransomware and persistent threats. Source: AON: Adversary Simulation
Anonymized Data	is data that has been stripped of personally identifiable information, also known as PII. Source: https://www.secoda.co/glossary/anonymized-data

Application Monitoring	This capability is a collection of application-related events, including logins, access to sensitive data, transactions, administrative activity. Source: Enterprise Architecture Reference Guide v2 : CSA: Business Operation Support Services (BOSS) Domain
Artificial Intelligence[1]	A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs (data) to: (A) perceive real and virtual environments; (B) abstract such perceptions into models through analysis in an automated manner; And, (C) use model inference to formulate options for information or action Source: https://www.cisa.gov/sites/default/files/2023-11/2023-2024_CISA-Roadmap-for-AI_508c.pdfources/roadmap-ai
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system. Source: https://csrc.nist.gov/glossary/term/authentication
Authorization	The decision to permit or deny a subject access to system objects (network, data, application, service, etc. Source: https://csrc.nist.gov/glossary/term/authorization
Automated Incident Response	The use of AI-driven processes to automate the identification, containment, and mitigation of cybersecurity incidents.Authorization - The decision to permit or deny a subject access to system objects (network, data, application, service, etc. Source: https://csrc.nist.gov/glossary/term/authorization
Big Data	is a combination of structured, semi-structured and unstructured data collected by organizations that can be mined for information and used in machine learning projects, predictive modeling and other advanced analytics applications. Source: https://www.techtarget.com/searchdatamanagement/definition/big-data

[1] Within this document, "Artificial intelligence" (AI) has the meaning set forth in the National Artificial Intelligence Initiative Act of 2020 (enacted as Division E of the William M (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116-283), Section 5002(3):

Business Continuity and Disaster Recovery (BCDR)	The implementation of measures designed to ensure operational resiliency in the event of any service interruptions. Source: Defined Categories of Service 2011 : CSA
Cloud Access Security Broker (CASB)	On-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement. Source: https://www.gartner.com/en/information-technology/glossary/cloud-access-security-brokers-casbs
Cyber Insurance	Refers to a contract that enterprises can purchase to reduce the risks associated with conducting online business. Cyber insurance covers your organization's liability for most data breaches caused by a cyber security incident. Source: Trend Micro: What Is Cyber Insurance?
Data	The digital representation of anything in any form Source: Enterprise Architecture Reference Guide v2 : CSA: Technology Solution Services (TSS) Domain - Infrastructure Services
Data Analytics	using data, techniques and tools that identify patterns and trends, which in turn generate actionable insights that support informed decision-making. The primary objective of data analytics is to address specific questions or challenges that are relevant to an organization to drive better business outcomes. Source: https://www.comptia.org/content/guides/what-is-data-analytics
Data Architecture	describes how data is managed--from collection through to transformation, distribution, and consumption. It sets the blueprint for data and the way it flows through data storage systems. It is foundational to data processing operations and artificial intelligence (AI) applications. Source: https://www.ibm.com/topics/data-architecture

Data, Assets, Applications, Services (DAAS)	• Data – The sensitive data that poses the greatest risk if exfiltrated or misused. • Examples include payment card information, protected health information, personally identifiable information, and intellectual property. • In the government context, this also includes Classified Information, National Security Information, and Controlled Unclassified Information. • Applications – applications using sensitive data or control critical assets. • Assets – The assets, including an organization's information technology (IT), operational technology (OT), or Internet of Things devices. • Services – The services an organization most depends on. • Examples include Domain Name System, Dynamic Host Configuration Protocol, Directory Services, Network Time Protocol, and customized Application Programming Interfaces. Source: https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Zero%20Trust%20and%20Trusted%20Identity%20Management%20%2810-17-22%29.pdf
Data at Rest	In information technology, data at rest refers to computer data in digital form, such as cloud storage, file hosting services, databases, or data warehouses. Data at rest includes both structured and unstructured data. Source: https://www.imperva.com/learn/data-security/data-at-rest/
Data Breach	A data breach occurs when unauthorized individuals gain access to sensitive or confidential information, such as personal information or financial data. Data breaches can occur due to a variety of reasons, such as cyber attacks, employee negligence, or physical theft. The consequences of a data breach can be severe, including financial loss, damage to reputation, and legal penalties. For example, a data breach at a healthcare organization may result in the theft of patient records, including medical history and personal information, which can be used for identity theft or sold on the dark web. Source: https://csrc.nist.gov/glossary/term/breach

© Copyright 2024, Cloud Security Alliance. All rights reserved.

Data/Asset Classification	A way to approach security policy and its implementation that involves the classification of information into one of several categories, each of which has an associated security policy. Other assets such as servers and endpoints, can be similarly classified. In some cases, data can only be processed or stored on computers that share the same classification designation. Source: Enterprise Architecture Reference Guide v2 : CSA: Security and Risk Management (SRM) Domain
Data Catalog	a detailed inventory of all data assets in an organization, designed to help data professionals quickly find the most appropriate data for any analytical or business purpose. Source: https://www.ibm.com/topics/data-catalog
Data Corpus	A corpus is a collection of authentic text or audio organized into datasets. Authentic here means text written or audio spoken by a native of the language or dialect. A corpus can be made up of everything from newspapers, novels, recipes, radio broadcasts to television shows, movies, and tweets. Source: Hypersense AI: Corpus
Data Discovery	Scanning and classifying data held in Network, Endpoint, and Server. Source: Enterprise Architecture Reference Guide v2 : CSA: Security and Risk Management (SRM) Domain
Data Fabric	An architecture that facilitates the end-to-end integration of various data pipelines and cloud environments through the use of intelligent and automated systems. Source: IBM: What is a data fabric?
Data Governance	As the organization manages data between Applications, Services, and Enterprise Information Integration activities, the need to have a well define governance model that outlines and looks for compliance on how data is massaged, transformed, and stored throughout the IT infrastructure including internal and external services (i.e., SaaS, PaaS, IaaS, ASP, or others). Processes included in data governance include data ownership, how data should be classified, and responsibilities that data/ asset owners have for their applications and services, and the necessary controls for data throughout the lifecycle. Source: Enterprise Architecture Reference Guide v2 : CSA: Business Operation Support Services (BOSS) Domain

© Copyright 2024, Cloud Security Alliance. All rights reserved.

Data Integrity	The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit. Source: https://csrc.nist.gov/glossary/term/data_integrity
Data in transit	data moving from one place to another. This includes information transmitted through email, collaboration platforms, instant messaging, and any other communication channel. This data is usually less secure than data at rest because it is exposed on the Internet or on a company's private network, as it moves from one location to another. Source: https://www.imperva.com/learn/data-security/data-at-rest / data in transit
Data in use	this is data accessed or used by employees, corporate applications, or customers. Data in this state is the most vulnerable—whether it is being processed, read, or modified. Granting direct access to individuals makes them vulnerable to attacks and human error, any of which can have serious consequences. Encryption is important for protecting data in use. Many companies complement encryption by adding security measures such as authentication and strict data access control. Source: https://www.imperva.com/learn/data-security/data-at-rest/
Data Interoperability	is the ability to access and process data from multiple sources without losing meaning and then integrate that data for mapping, visualization, and other forms of representation and analysis. Interoperability enables people to find, explore, and understand the structure and content of datasets. In essence, it is the ability to 'join-up' data from different sources to help create a contextual and holistic picture for simpler (sometimes automated) analysis, better decision-making, and greater accountability. Source: https://www.data4sdgs.org/initiatives/data-interoperability-collaborative
Data Lake	is a centralized repository that ingests and stores large volumes of data in its original form. The data can then be processed and used as a basis for a variety of analytic needs. Due to its open, scalable architecture, a data lake can accommodate all types of data from any source, from structured (database tables, Excel sheets) to semi-structured (XML files, webpages) to unstructured (images, audio files, tweets), all without sacrificing fidelity. Source: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-data-lake

© Copyright 2024, Cloud Security Alliance. All rights reserved.

Data Life Cycle Management	The Data Life Cycle Management covers the following six phases: create, store, use, share, archive, and destroy. Although it is shown as a linear progression, once created, data may flow between stages without restriction, and may not pass through all stages during usefulness. Source: Enterprise Architecture Reference Guide v2 : CSA: Security and Risk Management (SRM) Domain
Data Loss Prevention (DLP)	DLP refers to systems that enforce policies to safeguard critical data such as Intellectual Property and customer information and ensure it doesn't escape from the enterprise to unintended parties. These solutions discover and classify sensitive data, define and manage policies based on content and context, monitor and enforce movement of data, as well as report, audit, and document incidents of data leakage. Source: Enterprise Architecture Reference Guide v2 : CSA: Security and Risk Management (SRM) Domain
Data Loss	The exposure of proprietary, sensitive, or classified information through either data theft or data leakage. Source: https://csrc.nist.gov/glossary/term/data_loss
Data Leakage	The unauthorized transmission of data from within an organization to an external destination or recipient. Source: https://www.forcepoint.com/cyber-edu/data-leakage
Data lineage	is the process of tracking the flow of data over time, providing a clear understanding of where the data originated, how it has changed, and its ultimate destination within the data pipeline. Data lineage tools provide a record of data throughout its lifecycle, including source information and any data transformations that have been applied during any ETL (Extract, transform and load) processes. Source: https://www.ibm.com/topics/data-lineage
Data Localization	Data localization is the practice of keeping data within the region it originated from. Source: https://www.cloudflare.com/learning/privacy/what-is-data-localization/

Data Masking	The process of obscuring (masking) specific data elements within data stores. It ensures that sensitive data is replaced with realistic but not real data. The goal is that sensitive data are not available outside of the authorized environment. Source: Enterprise Architecture Reference Guide v2 : CSA: Security and Risk Management (SRM) Domain
Data Mesh	A data mesh is an architectural framework that solves advanced data security challenges through distributed, decentralized ownership. Organizations have multiple data sources from different lines of business that must be integrated for analytics. A data mesh architecture effectively unites disparate data sources and links them together through centrally managed data sharing and governance guidelines. Business functions can maintain control over how shared data is accessed, who accesses it, and in what formats it's accessed. Source: https://aws.amazon.com/what-is/data-mesh/
Data Mining	Data mining, also known as knowledge discovery in data (KDD), is the process of uncovering patterns and other valuable information from large data sets. Source: https://www.ibm.com/topics/data-mining
Data Obscuring	A method of protecting fields or records of data by some form of obfuscation such as encryption. Data obscuring techniques can be used in source code, for example, to prevent reverse engineering of applications. There are also low tech solutions such as ink stamps to redact sensitive information on hard copies. Source: Enterprise Architecture Reference Guide v2 : CSA: Security and Risk Management (SRM) Domain
Data Persistence	the longevity of data after the application that created it has been closed. In order for this to happen, the data must be written to non-volatile storage — a type of memory that can retain that information long-term, even if the application is no longer running. Source: https://www.mongodb.com/databases/data-persistence
Data Pipeline	is a method in which raw data is ingested from various data sources and then ported to data store, like a data lake or data warehouse, for analysis. Source: https://www.ibm.com/topics/data-pipeline

© Copyright 2024, Cloud Security Alliance. All rights reserved.

Data Preservation	is the process of keeping physical items and electronically stored information (ESI) intact for discovery during litigation. To preserve potential evidence, parties must protect that information from being destroyed, deleted, lost, or altered in any way. Source: https://zapproved.com/blog/what-is-preservation/
Data Provenance	In the context of computers and law enforcement use, it is an equivalent term to chain of custody. It involves the method of generation, transmission and storage of information that may be used to trace the origin of a piece of information processed by community resources. Source: https://csrc.nist.gov/glossary/term/data_provenance
Data Residency	Refers to the physical or geographic location where data is stored and processed, often influenced by legal and regulatory requirements. Source: TechTarget - What is data residency?
Data Retention	Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements. Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
Data Segregation	Data segregation is the process and controls that ensure data is segregated in a multi-tenant environment, so each tenant has access to his and only his data. Source: Enterprise Architecture Reference Guide v2 : CSA: Technology Solution Services (TSS) Domain - Information Services
Data Sovereignty	The notion that data is subject to the laws of the country or jurisdiction in which it is physically stored. Source: https://www.splunk.com/en_us/blog/learn/data-sovereignty-vs-data-residency.html
Data Storage	the retention of information using technology specifically developed to keep that data and have it as accessible as necessary. Data storage refers to the use of recording media to retain data using computers or other devices. Source: https://www.hpe.com/us/en/what-is/data-storage.html

Data Tagging	A data tag is a keyword or term assigned typically as a form of metadata to a piece of information. It helps describe an item and facilitates it being found again by browsing or searching. Source: Enterprise Architecture Reference Guide v2 : CSA: Security and Risk Management (SRM) Domain
Data Use Agreement ("DUA")	is a contract that governs the exchange of specific data between two parties. DUA's establish who is permitted to use and receive a unique data set, along with the allowable uses and disclosures of the data by the recipient. A DUA also assigns appropriate responsibility to the researcher and recipient for using the data. Source: https://ora.stanford.edu/resources/data-use-agreements
Data Wrangling	also called data cleaning, data remediation, or data munging—refers to a variety of processes designed to transform raw data into more readily used formats. The exact methods differ from project to project depending on the data you're leveraging and the goal you're trying to achieve. Source: https://online.hbs.edu/blog/post/data-wrangling
De-identification of Data	The process of removing personal data identifiers and sensitive information to preserve the privacy of individuals within a given data set. Source: NISTIR 8053 De-Identification of Personal Information
Denial of Service (DoS)	The act of making a system, feature or resource unavailable for intended users. In cloud testing, denial of service often takes the form of destruction or encryption of cloud resources, disablement of accounts, credentials or users. Source: Cloud Penetration Testing : CSA
Digital Certificate	A Digital Certificate is an electronic document that verifies the identity of an entity and is used to establish secure communication between parties. In the IAM domain, digital certificates are commonly used for authentication and encryption purposes. They are issued by a trusted third party called a Certificate Authority (CA). For example, an organization may use digital certificates to authenticate the identity of employees accessing the network remotely or to encrypt sensitive data transmitted over the Internet. Source: https://csrc.nist.gov/glossary/term/digital_certificate

© Copyright 2024, Cloud Security Alliance. All rights reserved.

Digital Forensics	The 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. Source: https://csrc.nist.gov/glossary/term/digital_forensics
Disaster Recovery as a Service (DRaaS)	A cloud computing service model that allows an organization to back up its data and IT infrastructure in a third-party cloud computing environment from which it is possible to regain access and functionality to IT infrastructure after a disaster. Source: Disaster Recovery as a Service : CSA
Decryption	The process of converting encrypted data back into its original, readable form. Source: NIST SP 800-53 Revision 5
Double Extortion	In double extortion, cybercriminals encrypt sensitive user data and threaten to publish it on the dark web, sell it to the highest bidder, or permanently restrict access if the ransom is unpaid by a deadline. Organizations can often recover lost information from previous backups, but it's much more difficult to stop sensitive data from being leaked after this attack. Source: ISAGCA: Double Extortion Ransomware: What It Is and How to Respond
Egress Filtering	Method of filtering outbound network traffic such that only explicitly allowed traffic is permitted to leave the network. Source: https://www.pcisecuritystandards.org/glossary/egress-filtering/
Encryption	Encryption is the process of converting plain text into an unreadable format using a cryptographic algorithm to protect the confidentiality, integrity and availability of data. Source: Defined Categories of Service 2011 : CSA
Endpoints	Endpoints are the devices that users interact with when using an IT solution. They are called Endpoints because they are at the edge of the solution where technology meets humans. Source: Enterprise Architecture Reference Guide v2 : CSA: Technology Solution Services (TSS) Domain

© Copyright 2024, Cloud Security Alliance. All rights reserved.

Entity	An entity refers to a unique, identifiable actor in a computer system. In the context of cybersecurity, an entity can be a user, a device, an application, or a system that is identified and authenticated by an IAM system. Entities can have different roles and permissions within the system, and their actions and access to resources are typically logged for auditing and security purposes. Source:
ETL Pipeline	Extract, transform and load (ETL) is a process in data warehousing responsible for pulling data out of the source systems and placing it into a data warehouse. Source: https://www.secoda.co/glossary/etl-pipeline
Federated Identity Management	Enables identity information to be developed and shared among several entities and across trust domains. Tools and standards permit identity attributes to be transferred from one trusted identifying and authenticating entity to another for authentication, authorization, and other purposes, thus providing "single sign-on" convenience and efficiencies to identified individuals, identity providers, and relying parties. Source: https://www.gartner.com/en/information-technology/glossary/federated-identity-management
Firewall	An inter-network connection device that restricts data communication traffic between two connected networks. A firewall may be either an application installed on a general-purpose computer or a dedicated platform (appliance), which forwards or rejects/drops packets on a network. Typically firewalls are used to define zone borders. Firewalls generally have rules restricting which ports are open. Source: https://csrc.nist.gov/glossary/term/firewall
General Data Protection Regulation (GDPR)	The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25, 2018. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros. Source: https://gdpr.eu/what-is-gdpr/

© Copyright 2024, Cloud Security Alliance. All rights reserved.

Hardware Security Module (HSM)	A physical computing device that safeguards and manages cryptographic keys and provides cryptographic processing. An HSM is or contains a cryptographic module. Source: https://csrc.nist.gov/glossary/term/hardware_security_module_hsm
Hashing	A cryptographic technique that converts data into a fixed-size value, called a hash value. Hashing is used to verify the integrity of data and to detect unauthorized changes. Source: NIST SP 800-53 Revision 5
Homomorphic Encryption (HE)	uses algorithms to enable computations with encrypted data. Partial HE (PHE) supports only limited use cases, such as subtraction and addition, but with little performance impact. Fully homomorphic encryption (FHE) supports a wider range of repeatable and arbitrary mathematical operations; however, it worsens performance Source: https://www.gartner.com/en/information-technology/glossary/homomorphic-encryption-he
Hypertext Transport Protocol Secure (HTTPS)	A secure network communication method, technically not a protocol in itself, HTTPS is the result of layering the hypertext transfer protocol (HTTP) on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications. Source: https://iapp.org/resources/article/hypertext-transfer-protocol-secure/
IT Risk Management	Information risk management is the act of aligning exposure to risk and capability of managing it with the risk tolerance of the data owner. It is the primary means of decision support for information technology resources designed to protect the confidentiality, integrity, and availability of information assets. Ensures that risk of all types are identified, understood, communicated, and either accepted, remediated, transferred or avoided. IT Risk Management can look at the output of Compliance Management activities to assist the organization in evaluating the overall security posture and aligning with the defined risk objectives. Source: Enterprise Architecture Reference Guide v2 : CSA: Security and Risk Management (SRM) Domain
Identity	An attribute or set of attributes that uniquely describe a subject within a given context. Source: https://csrc.nist.gov/glossary/term/identity

© Copyright 2024, Cloud Security Alliance. All rights reserved.

Identity and Access Management (IAM)	Identity and Access Management (IAM) refers to the policies, technologies, and processes that enable organizations to manage and control user identities, access, and privileges to systems and applications. IAM solutions typically include user provisioning, authentication, authorization, and auditing capabilities. IAM helps organizations to ensure that only authorized users can access sensitive data and applications and that access is granted based on the principle of least privilege. IAM also enables organizations to streamline user management processes and reduce the risk of insider threats. Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-203.pdf
Incident Response (IR)	The systematic process of managing and addressing security incidents, including detecting, responding to, and mitigating the impact of incidents.
Incident Response Plan	A clear set of instructions that helps an organization prepare, detect, analyze and recover from an incident. Source: Cloud Penetration Testing : CSA
Indicators of Compromise (IoC)	Serve as forensic evidence of potential intrusions on a host system or network. These artifacts enable information security professionals and system administrators to detect intrusion attempts or other malicious activities. Security researchers use IOCs to better analyze a particular malware's techniques and behaviors. IOCs also provide actionable threat intelligence that can be shared within the community to further improve an organization's incident response and remediation strategies. Source: TrendMicro: Indicators of compromise
Intrusion Detection System	Network security tool that monitors network traffic and devices for known malicious activity, suspicious activity or security policy violations. Source: IBM: What is an intrusion detection system (IDS)?
Malware	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code. Source: https://csrc.nist.gov/glossary/term/malware

© Copyright 2024, Cloud Security Alliance. All rights reserved.

Master Data Management (MDM)	is a technology-enabled discipline in which business and IT work together to ensure the uniformity, accuracy, stewardship, semantic consistency and accountability of the enterprise's official shared master data assets. Source: https://www.gartner.com/en/information-technology/glossary/master-data-management-mdm
Metadata	The information that describes and explains data. It provides context with details such as the source, type, owner, and relationships to other data sets. So, it can help you understand the relevance of a particular data set and guide you on how to use it. In a nutshell: Metadata is a cornerstone of a modern enterprise data stack.
Multi Factor Authentication (MFA)	A form of authentication that relies on two or more 'factors' where a factor is 'something you have' such as a smartcard, 'something you know' such as a password or pin, and 'something you are' such as a physical fingerprint or a behavioral keyboard cadence. Source: Enterprise Architecture Reference Guide v2 : CSA: Security and Risk Management (SRM) Domain
Network Segmentation	A network security technique that divides a network into smaller, distinct sub-networks that enable network teams to compartmentalize the sub-networks and deliver unique security controls and services to each sub-network. Source: VMware: What is network segmentation?
Non-Human Identity	A non-human identity refers to an identity that is not associated with a human user. This could include an identity associated with an automated process or service, such as a script or an application. Non-human identities are often used to perform tasks that are not performed by human users, such as running a scheduled task or accessing a web service. They also can be used in cases like Internet of Things devices or other machines that can interact with systems with certain permissions. Source: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63a.pdf
Password	A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization. Source: https://csrc.nist.gov/glossary/term/password#:~:text=memorized%20

© Copyright 2024, Cloud Security Alliance. All rights reserved.

Password Management	The process to specify multiple password policies, define password composition constraints, maintain password history, restrict passwords, configure password validity period, create password rules, etc. Source: Enterprise Architecture Reference Guide v2 : CSA: Security and Risk Management (SRM) Domain
Penetration Testing	A method of testing where testers target individual binary components or the application as a whole to determine whether intra or intercomponent vulnerabilities can be exploited to compromise the application, its data, or its environment resources. Source: https://csrc.nist.gov/glossary/term/penetration_testing
Personally identifiable information (PII)	Information that can be used to distinguish or trace an individual's identity—such as name, social security number, biometric data records—either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.). Source: https://csrc.nist.gov/glossary/term/personally_identifiable_information
Phishing	A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person. Source: https://csrc.nist.gov/glossary/term/phishing
Phishing Simulation	A cybersecurity exercise that tests an organization's ability to recognize and respond to a phishing attack. Source: IBM: What is a phishing simulation?
Policy Management	A process or platform for centralized policy creation, repository and management. Policy management strives to maintain an organization structure and process that supports the creation, implementation, exception handling, and frameworks that represent business requirements. Source: Enterprise Architecture Reference Guide v2 : CSA: Security and Risk Management (SRM) Domain

© Copyright 2024, Cloud Security Alliance. All rights reserved.

Principal Data Management	The capability for the management of all attributes regarding the subjects of access control decisions. These principals can be users, machines, or services. Authorization decisions may need to consider many attributes about the principals, including role, location, relationships to accounts, other principals, etc. Source: Enterprise Architecture Reference Guide v2 : CSA: Security and Risk Management (SRM) Domain
Quality of Service (QoS)	The ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. Source: https://www.iso.org/obp/ui#iso:std:iso:20205:ed-1:v1:en:term:1.6.3
Ransomware	Ransomware is malicious software that gains access to an organization's systems and data and then encrypts these systems and data rendering them inaccessible without the encryption key. The attacker supplies the decrypt key only if the victim pays a fee (ransom). Ransomware can gain access to systems through such avenues as users interacting with phishing emails or infected websites. Source: Disaster Recovery as a Service : CSA
Ransomware-as-a-Service (RaaS)	A business model that involves selling or renting ransomware to buyers, called affiliates. RaaS can be credited as one of the primary reasons for the rapid proliferation of ransomware attacks, as it has made it easier for a variety of threat actors , even those who have little technical knowledge, to deploy ransomware against targets. Source: TrendMicro: Ransomware as a Service
Real Time Filtering	A control to track use patterns and information like what sites are visited and blocked some in real-time based on policies. Source: Enterprise Architecture Reference Guide v2 : CSA: Security and Risk Management (SRM) Domain
Recovery Plans	Recovery plans describe the processes and procedures required to restore service delivery after interruption or disaster. The plans will often include steps to gradually restore the service while monitoring the performance and system health of every reached milestone. Source: Enterprise Architecture Reference Guide v2 : CSA: Technology Solution Services (TSS) Domain - Information Services

© Copyright 2024, Cloud Security Alliance. All rights reserved.

Reporting Services	Reporting services provide the ability to present data in various ways going from a top-level aggregated dashboard, drilling down to raw data. Reporting services also offer the ability to mine and analyze data and provide business intelligence to decision-makers Source: Enterprise Architecture Reference Guide v2 : CSA: Technology Solution Services (TSS) Domain - Information Services
Resource Data Management	Authorization plays a key role in data management by simultaneously providing access and protection to application information resources. Source: Enterprise Architecture Reference Guide v2 : CSA: Security and Risk Management (SRM) Domain
Risk	A subset of "business risks" and, as such, should be talked about in business terms. Instead of defining risk in technical terms, cybersecurity professionals—when speaking to executives—can adopt the definition of risk used by almost every business manager and board of directors: the potential for monetary loss. In this context, "risk" is the possibility that an event will lead to reduced profitability. Therefore, a cyber event causing damage to an organization's brand or reputation can be quantified. Source: Information Technology Governance, Risk and Compliance in Healthcare : CSA
Risk Assessments	Risk Assessments measure the maturity of the organization's controls from a reference framework perspective (i.e., COBIT, ISO27001), regulatory perspective (i.e., SOX, PCI). Source: Enterprise Architecture Reference Guide v2 : CSA: Technology Solution Services (TSS) Domain - Information Services
Rootkit	A set of tools used by an attacker after gaining root-level access to a host to conceal the attacker's activities on the host and permit the attacker to maintain root-level access to the host through covert means. Source: https://csrc.nist.gov/glossary/term/rootkit
Rules for Data Retention	This capability manages the policies, procedures, or requirements associated with keeping data (transactions information, email, document images, card swipes, online browsing history) as long as required to do so from the business and regulatory perspective, then secured disposal. Source: Enterprise Architecture Reference Guide v2 : CSA: Business Operation Support Services (BOSS) Domain

© Copyright 2024, Cloud Security Alliance. All rights reserved.

Secure Data Enclave (SDE)	a secure, centralized service for faculty and researchers that work with sensitive research data. The SDE meets the high water mark of security policy to ensure that restricted information is protected per local, federal, and international laws. Source: https://securedata.uchicago.edu/
Secure Disposal of Data	Ensure that data is destroyed appropriately to preclude its recovery (e.g., through digital forensic techniques).Documentation of such destruction should be in place and should be included in information lifecycle management processes. Source: Enterprise Architecture Reference Guide v2 : CSA: Business Operation Support Services (BOSS) Domain
Secure Sockets Layer (SSL)	A security protocol providing privacy and data integrity between two communicating applications. The protocol is composed of two layers: the TLS record protocol and the TLS handshake protocol. Source: https://csrc.nist.gov/glossary/term/secure_sockets_layer
Security Audit	Independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures. Source: https://csrc.nist.gov/glossary/term/security_audit
Security Incident	n occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Source: https://csrc.nist.gov/glossary/term/security_incident
Security Patch	An update that often comes from a security developer to any device that needs the update. Delayed patch updates often come because a vulnerability or hole isn't known or discovered before the software is released initially or before a big update is rolled out. Source: CyberDB: What is a Patch in Cybersecurity?

© Copyright 2024, Cloud Security Alliance. All rights reserved.

Security Token	A security token is a physical device that users must possess to access a system. Authentication data must flow between both the user and the system to validate identities and access. A security token is the conduit for this data. Source: Okta: What Is a Security Token?
Security Token Service (STS)	A component that issues, validates, renews, and cancels security tokens for trusted systems, users, and resources requesting access within a federation. Source: Radiant Logic: Secure Token Service
Sensitive Data Scanning	is the process of identifying sensitive data stored in various formats, such as Documents, Databases, and Other digital files. The primary purpose of sensitive data scanning is to identify all PII-related data within an organization, determine the quantity and location of such data, and assess the security of the data. Scanning data might go by similar names such as sensitive data discovery tools, PII scanning tools and confidential data scanning. Data scanning is done using tools that have different features, such as detecting sensitive data as it is stored or transferred. Some others can also evaluate the vulnerability of every piece of data and its importance regarding data security standards. Source: https://www.splunk.com/en_us/blog/learn/data-scanning.html
Single Sign-On (SSO)	Provides the capability to authenticate once, and be subsequently and automatically authenticated when accessing various target systems. It eliminates the need to separately authenticate and sign on to individual applications and systems, essentially serving as a user surrogate between client workstations and target systems. Source: https://www.gartner.com/en/information-technology/glossary/sso-single-sign-on
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Source: https://www.niap-ccevs.org/Ref/CNSSI_4009.pdf (March 2, 2022, Page 200)

© Copyright 2024, Cloud Security Alliance. All rights reserved.

Third Party Providers	Service providers, integrators, vendors, telecommunications, and infrastructure support that are external to the organization that operates the manufacturing system. Source: Third-party Providers - Glossary | CSRC (nist.gov)
Threat Intelligence	Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes. Source: https://csrc.nist.gov/glossary/term/threat_intelligence
Threat & Vulnerability Management	This discipline deals with core security, such as vulnerability management, threat management, compliance testing, and penetration testing. Vulnerability management is a complex endeavor in which enterprises track their assets, monitor, scan for known/emerging vulnerabilities, and take action by patching the software, changing configurations, or deploying other controls to reduce the attack surface at the resource layer. Threat modeling and security testing are also part of activities to identify the vulnerabilities effectively. This discipline aims to proactively inspect the infrastructure that runs the cloud to address new security threats using vulnerability scanning, virtual patching, and other aspects of security testing and response. Source: Enterprise Architecture Reference Guide v2 : CSA: Security and Risk Management (SRM) Domain
Tokenization	is a technique to protect highly sensitive information by removing it from the database and substituting an equivalent, nonsensitive element into the database. This non-sensitive element is referred to as a token. The sensitive data is placed into a highly secured, encrypted vault. Source: https://www.ibm.com/cloud/architecture/architectures/security-data-tokenization-solution/
Transport Layer Security (TLS)	A cryptographic protocol, successor to SSL, that provides security for communications over a computer or IP network. Source: https://csrc.nist.gov/glossary/term/transport_layer_security
TTPs (Tactics, Techniques, and Procedures)	The behavior of an actor. A tactic is the highest-level description of this behavior, while techniques give a more detailed description of behavior in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique. Source: https://csrc.nist.gov/glossary/term/tactics_techniques_and_procedures

Virtual Private Network (VPN)	A virtual network built on top of existing physical networks that can provide a secure communications mechanism for data and IP information transmitted between networks or between different nodes on the same network. Source: https://csrc.nist.gov/glossary/term/virtual_private_network
Vulnerability	A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation exploitable by a threat source. Source: Special Publication 800-30 Revision 1 Guide for Conducting Risk Assessments, National Institute of Standards and Technology
Web Application Firewall (WAF)	Application firewall that monitors, alerts, and blocks attacks by inspecting HTTP traffic. Source: The Six Pillars of DevSecOps: Automation : CSA
Whitelisting	An approach where only pre-approved entities are allowed access to a specific service or environment, while all others are automatically denied by default. Source: What is Whitelist and How Does It Work
Zero-day exploit	A zero-day exploit is a cyberattack vector or technique that takes advantage of an unknown or unaddressed security flaw in computer software, hardware or firmware. 'Zero day' refers to the fact that the software or device vendor has zero days, or no time, to fix the flaw, because malicious actors can already use it to gain access to vulnerable systems. Source: IBM: What is a zero-day exploit
Zero-Day Vulnerability	A vulnerability in a system or device that has been disclosed but is not yet patched. Because they were discovered before security researchers and software developers became aware of them, and before they can issue a patch, zero-day vulnerabilities pose a higher risk to users as cybercriminals race to exploit these vulnerabilities to cash in on their schemes. Vulnerable systems are exposed until a patch is issued by the vendor. Source: Trend Micro: What is a zero-day vulnerability?

© Copyright 2024, Cloud Security Alliance. All rights reserved.

Zero Knowledge Proof (ZKP)	Zero Trust is a cybersecurity strategy premised on the idea that no user or asset is to be implicitly trusted. It assumes that a breach has already occurred or will occur, and therefore, a user should not be granted access to sensitive information by a single verification done at the enterprise perimeter. Instead, each user, device, application, and transaction must be continually verified. Source: https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Zero%20Trust%20and%20Trusted%20Identity%20Management.pdf
Zero Trust (ZT)	A cybersecurity strategy premised on the idea that no user or asset is to be implicitly trusted. It assumes that a breach has already occurred or will occur, and therefore, a user should not be granted access to sensitive information by a single verification done at the enterprise perimeter. Instead, each user, device, application, and transaction must be continually verified. Source: https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Zero%20Trust%20and%20Trusted%20Identity%20Management.pdf

© Copyright 2024, Cloud Security Alliance. All rights reserved.