

Information Security Glossary

1. Purpose

The purpose of this document is to provide a general glossary of terms used in information security documentation.

2. Glossary

Term	Definition
2FA	Two-Factor Authentication; a particular and common form of Multi-Factor Authentication (MFA) based on exactly two pieces of evidence (or factors) for authentication; (see also MFA)
ANPR	Automatic Number-Plate Recognition
ANSI	American National Standards Institute; a private non-profit organisation that oversees the development of voluntary consensus standards for products, services, processes, systems, and personnel in the United States
AoC	Attestation of Compliance; a form used by merchants and service providers to attest to the results of a PCI DSS assessment
AP	Access Point; a networking hardware device that allows other Wi-Fi devices to connect to a wired network; also known as wireless access point (WAP)
ASCII	American Standard Code for Information Interchange; a character encoding standard for electronic communication
ASV	Approved Scanning Vendor; an organisation with a set of security services and tools to conduct external vulnerability scanning services to validate adherence with the external scanning requirements of PCI DSS
Bastion host	A special-purpose computer on a network specifically designed and configured to withstand attacks
BC	Business Continuity
BCP	Business Continuity Plan
BDK	Base Derivation Key; in DUKPT, the single, fixed key from which all unique keys used for transactions are derived
BI	Business Intelligence
BSIMM	Build Security in Maturity Model; a software security measurement framework that helps organisations compare their software security to other organisations
BYOD	Bring Your Own Device; it refers to being allowed to use one's personally owned device, rather than being required to use an officially provided device
CA	Certification Authority; an entity that issues digital certificates

Term	Definition
CAB	Change Advisory Board; a designated body with overall responsibility for the assessment and approval or rejection of changes; it includes representatives from all areas within IT as permanent members, but representatives from other business units can be incorporated as temporary members when required
Cardholder data	Any personally identifiable information associated with a person who has a personal card; it includes the PAN, the cardholder name, the service code and the expiration date; in a broad sense, cardholder data is considered to also include sensitive authentication data; (see sensitive authentication data)
CCM	Cloud Controls Matrix; a cyber security control framework for cloud computing, created and maintained by CSA
CCTV	Closed-circuit Television
CD	Compact Disc
CDE	Cardholder Data Environment
CEF	Common Event Format; a standard for the interoperability of event or log-generating devices and applications
CHD	Cardholder Data
Cloud	Metaphor for a global network of remote servers that operates as a single ecosystem, commonly associated with the Internet
Cloud computing	The on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user
Cloud forensics	Investigations that are focused on incidents primarily involving the cloud
CMMI	Capability Maturity Model Integration; a process level improvement training and appraisal program, developed by the Carnegie Mellon University
COM	Communications port; the original, yet still common, name of the serial port interface on PCs; it can refer not only to physical ports, but also to emulated ports, such as ports created by Bluetooth or USB-to-serial adapters
Containerisation	Operating system-level virtualisation or application-level virtualisation over multiple network resources so that software applications can run in isolated user spaces (called containers) in any cloud or non-cloud environment
Controller	Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; (see also processor)
CPU	Central Processing Unit; the electronic circuitry within a computer that executes instructions that make up a computer program
CR	Change Request; the formal request for a change to be made; each CR will have a unique identifier for reference

Term	Definition
Cryptography	The practice and study of techniques for secure communication in the presence of third parties; more generally, cryptography is about constructing and analysing protocols that prevent third parties or the public from reading private messages
CSA	Cloud Security Alliance; a not-for-profit organisation with the mission to promote the use of best practices for providing security assurance within cloud computing, and to provide education on the uses of cloud computing to help secure all other forms of computing
CSC (1)	Card Security Code; also known by other designations, including Card Verification Code (CVC) and Card Verification Value (CVV)
CSC (2)	Cloud Service Customer (or cloud service consumer)
CSP	Cloud Service Provider
CSSRA	Countries to which Special Security Regulations Apply; a list, maintained by the UK Government, of countries that pose an increased threat to information security
CV	Curriculum Vitae
CVC	Card Verification Code; see CSC (1)
CVE	Common Vulnerabilities and Exposures, a reference method for publicly known information-security vulnerabilities and exposures
CVV	Card Verification Value; see CSC (1)
CWE	Common Weakness Enumeration; a category system for software weaknesses and vulnerabilities, sustained by a community project with the goals of understanding flaws in software and creating automated tools that can be used to identify, fix, and prevent those flaws
DBS	Disclosure and Barring Service
DDoS	Distributed Denial-of-Service; a type of denial-of-service attack where the incoming traffic flooding the victim originates from many different sources; (see also DoS)
DHCP	Dynamic Host Configuration Protocol; a network management protocol used on Internet Protocol networks whereby a server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks
DLP	Data Loss Prevention
DMZ	Demilitarised Zone; a physical or logical subnetwork that contains and exposes an organisation's external-facing services to an untrusted, usually larger, network such as the Internet
DNS	Domain Name System; a hierarchical and decentralised naming system for computers, services, or other resources connected to the Internet or a private network

Term	Definition
DoS	Denial-of-Service; a type of cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet; (see also DDoS)
DPA (2018)	Data Protection Act (2018); a United Kingdom Act of Parliament which updates data protection laws in the UK; it is a national law which complements the EU's GDPR and updates the Data Protection Act 1998
DPIA	Data Protection Impact Assessment; a kind of privacy impact assessment, under the EU's GDPR
DPO	Data Protection Officer; a corporate officer responsible for data protection under the EU's GDPR
DR	Disaster Recovery
DRP	Disaster Recovery Plan
DTMF	Dual-Tone Multi-Frequency signalling; a telecommunication signalling system using the voice-frequency band over telephone lines between telephone equipment and other communications devices and switching centres
DUKPT	Derived Unique Key Per Transaction; a key management scheme in which, for every transaction, a unique key is used which is derived from a single, fixed key – the Base Derivation Key (BDK)
DVD	Digital Versatile Disc
EAP	Extensible Authentication Protocol; an authentication framework frequently used in network and internet connections
E-discovery	Electronic discovery; discovery in legal proceedings (such as litigation or government investigations) where the information sought is in electronic format
EEA	European Economic Area
Encryption	The process of encoding information by the use of cryptographic algorithms, converting the original representation of the information ('plaintext') into an alternative, encoded form ('ciphertext')
ERM	Enterprise rRsk Management
ETL	Extract, Transform, Load; a three-phase process where data is extracted, transformed (cleaned, sanitised, scrubbed) and loaded into an output data container
EU	European Union
FIM	File Integrity Monitoring; a process that performs the act of validating the integrity of operating system and application software files using a verification method between the current file state and a known, good baseline
FTP	File Transfer Protocol; a standard network protocol used for the transfer of computer files between a client and server on a computer network

Term	Definition
GDPR	General Data Protection Regulation; a regulation in EU law on data protection and privacy in the EU and the EEA
GPS	Global Positioning System; a satellite-based radio-navigation system
Hard delete	A delete operation that permanently deletes data from a database, rather than only marking it as deleted and rendering it invisible to (normal) users; the opposite of soft delete
HIDS	Host-based Intrusion Detection System; an intrusion detection system that is capable of monitoring and analysing the internals of a computing system as well as the network packets on its network interfaces; (see also IDS)
HIPS	Host-based Intrusion Prevention System; an installed software package which monitors a single host for suspicious activity by analysing events occurring within that host; (see also IPS)
HLD	High-Level Design; commonly used in the context of software design
HRA	Human Rights Act
HSM	Hardware Security Module; a physical computing device that safeguards and manages digital keys for strong authentication and provides crypto processing
HTTP	Hypertext Transfer Protocol; an application protocol for distributed, collaborative, hypermedia information systems
Hypervisor	A type of computer software, firmware or hardware that creates and runs virtual machines
IaaS	Infrastructure as a Service; a cloud computing service model where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications
IAM	Identity and Access Management (IAM); see IdM
ICMP	Internet Control Message Protocol; a supporting protocol in the Internet protocol suite
ICO	Information Commissioner's Office; the independent national data protection authority in the UK; it is a non-departmental public body which reports directly to the UK Parliament
ID	Identity / identifier
IdM	Identity Management; a framework of policies and technologies for ensuring that the proper people in an enterprise have the appropriate access to technology resources; also known as Identity and Access Management (IAM)
IDPS	Intrusion Detection and Prevention System; see IPS
IDS	Intrusion Detection System; a device or software application that monitors a network or systems for malicious activity or policy violations
IEC	International Electrotechnical Commission; an international standards organisation

Term	Definition
IEEE	Institute of Electrical and Electronics Engineers; a professional association for electronic engineering and electrical engineering (and associated disciplines) in the United States
IETF	Internet Engineering Task Force; an open standards organisation, which develops and promotes voluntary Internet standards, in particular the standards that comprise the Internet protocol suite
IM	Instant Messaging; real-time text transmission over the Internet
IMAP	Internet Message Access Protocol; an Internet standard protocol used by email clients to retrieve email messages from a mail server over a TCP/IP connection
Internet protocol suite	The conceptual model and set of communications protocols used on the Internet and similar computer networks; commonly known as TCP/IP because the foundational protocols in the suite are TCP and IP
Interoperability	The capability of different applications/systems to exchange data via a common set of exchange formats, to read and write the same file formats, and to use the same protocols
IoT	Internet of Things; a system of interrelated computing devices, mechanical and digital machines provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction
IP	Internet Protocol; the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries; its routing function enables internetworking, and essentially establishes the Internet
IPR	Intellectual Property Rights
IPS	Intrusion Prevention System; a device or software application that monitors a network or systems for malicious activity or policy violations; also known as Intrusion Detection and Prevention System (IDPS)
IPsec	Internet Protocol Security; a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an IP network; it is used in VPNs
IPv4	Internet Protocol version 4; the fourth version of the IP; it uses a 32-bit address space, which limits the number of unique hosts to 4,294,967,296
IPv6	Internet Protocol version 6; the most recent version of the IP, intended to replace IPv4; it uses a 128-bit address, theoretically allowing approximately 3.4×10^{38} addresses
ISA	Internal Security Assessor; a designation given by the PCI SSC to eligible internal security audit professionals working for a qualifying organisation
ISB	Information Security Board

Term	Definition
ISMS	Information Security Management System
ISO	International Organisation for Standardisation; an international standard-setting body composed of representatives from various national standards organisations
ISO 27001	An information security standard, part of the ISO/IEC 27000 family of standards
IT	Information Technology
IVR	Interactive Voice Response; a technology that allows a computer to interact with humans through the use of voice and DTMF tones input via a keypad
Jailbreaking	Removing, through privilege escalation, software restrictions imposed by the mobile operating system on a mobile device, thereby enabling root access to the operating system; a device in which this has occurred is said to be “jailbroken”
Jump box	A system on a network used to access and manage devices in a separate security zone
KIF	Key Injection Facility; a controlled facility where electronic payment terminals are customised by loading security keys through dedicated tools, in accordance with strictly defined operating procedures
LAN	Local Area Network; a computer network that interconnects computers within a limited area such as an office building
LDAP	Lightweight Directory Access Protocol; an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an IP network
LLD	Low-Level Design; commonly used in the context of software design
MAC address	Media Access Control address; a unique identifier assigned to a network interface controller for use as a network address in communications within a network segment
MAM	Mobile Application Management; software and services responsible for provisioning and controlling access to internally developed and commercially available mobile apps used in business settings on both company-provided and “bring your own” smartphones and tablet computers
MDM	Mobile Device Management; administration of mobile devices, such as smartphones, tablet computers and laptops; usually implemented with the use of a third-party product that has management features for particular vendors of mobile devices

Term	Definition
MFA	Multi-Factor Authentication; an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something the user and only the user knows), possession (something the user and only the user has), and inherence (something the user and only the user is)
MIME	Multipurpose Internet Mail Extensions; an Internet standard that extends the format of email messages to support text in character sets other than ASCII, as well as attachments of audio, video, images, and application programs
MoSCoW	A prioritisation technique used in requirements management; the term is an acronym derived from the first letter of each of four prioritisation categories: M = Must have, S = Should have, C = Could have, W = Won't have
MS	Microsoft
MSP	Managed Service Provider
MSSP	Managed Security Service Provider
NAC	Network Access Control; an approach to computer security that attempts to unify endpoint security technology (such as anti-malware, host intrusion prevention, and vulnerability assessment), user or system authentication and network security enforcement
NAT	Network Address Translation; a method of remapping one IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device
NCSC	National Cyber Security Centre; an organisation of the United Kingdom Government that provides advice and support for the public and private sector in how to avoid computer security threats
NIST	National Institute of Standards and Technology; a physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce; its mission is to promote innovation and industrial competitiveness
NIST CSF	NIST Cybersecurity Framework; a set of guidelines for mitigating organisational cybersecurity risks, published by the NIST
Non-repudiation	Inability to deny
NTP	Network Time Protocol; a networking protocol for clock synchronisation between computer systems over packet-switched, variable-latency data networks
OS	Operating system
OWASP	Open Web Application Security Project; an online community that produces freely available articles, methodologies, documentation, tools, and technologies in the field of web application security

Term	Definition
OWASP Top 10	A list, published and maintained by OWASP, of the top 10 most critical application security risks facing organisations
P2PE	Point to Point Encryption; an encryption standard established by the PCI SSC
PaaS	Platform as a Service; a cloud computing service model where the consumer is able to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider
PACE	Police and Criminal Evidence Act 1984; an Act of Parliament which instituted a legislative framework for the powers of police officers in England and Wales to combat crime
PAM	Privileged Access Management; the cybersecurity strategies and technologies for exerting control over the elevated (“privileged”) access and permissions for users, accounts, processes, and systems across an IT environment
PAN	Primary Account Number; the full number of a credit card
PC	Personal Computer
PCI	Payment Card Industry; all the organisations which store, process and transmit cardholder data, most notably for debit cards and credit cards
PCI DSS	Payment Card Industry Data Security Standard; an information security standard for organisations that handle branded personal cards from the major card schemes
PCI SSC	Payment Card Industry Security Standards Council; the council responsible for managing the evolution of PCI DSS
PDCA	Plan-Do-Check-Act; an iterative four-step management method used in business for the control and continuous improvement of processes and products
PED	PIN Entry Device; an electronic device used in a debit, credit or smart card-based transaction to accept and encrypt the cardholder's Personal Identification Number (PIN); also referred to as PIN pad
Personal card	A card issued by a financial institution to a customer that enables its owner (the cardholder) to access the funds in designated bank accounts, or through a credit account and make payments by electronic funds transfer and access automated teller machines; the most common types are credit cards and debit cards
PGP	Pretty Good Privacy; an encryption program that provides cryptographic privacy and authentication for data communication
Phishing	A type of social engineering where an attacker sends a fraudulent message designed to trick a person into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure.

Term	Definition
PIM	P2PE Instruction Manual; an instruction manual prepared by a P2PE solution provider in accordance with the P2PE standard
PIN	Personal Identification Number
PIN block	In a personal card, the block used to transport a new PIN; it also contains an authentication code, and optionally the "current" PIN value, enabling the personal card to further ensure receipt of a valid PIN value
PIN pad	See PED
PIR	Post Implementation Review
PKI	Public Key Infrastructure; a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption
PoFA	Protection of Freedoms Act
POI	Point of Interaction; a (hardware and/or software) component in POS equipment (e.g. a magnetic card reader) that enables a consumer to use a credit card to make a purchase at a retailer
POP	Post Office Protocol; an application-layer Internet standard protocol used by e-mail clients to retrieve e-mail from a mail server
POS	Point-of-Sale; the time and place where a retail transaction is completed; a POS terminal is a device that enables the completion of retail transactions
Processor	Natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller; (see also controller)
PSP	Payment Service Provider; an organisation that offers shops online services for accepting electronic payments by a variety of payment methods including credit card, bank-based payments such as direct debit, bank transfer, and real-time bank transfer based on online banking
PTS	PIN Transaction Security; technical and operational requirements set to protect cardholder data; applicable to all organisations that store, process or transmit cardholder data
QSA	Qualified Security Assessor; a person who has been certified by the PCI SSC to audit merchants for PCI DSS compliance
RACI matrix	A matrix that describes the participation by various roles in completing tasks or deliverables for a project or business process; RACI is an acronym derived from the four key responsibilities most typically used: responsible, accountable, consulted and informed
RASIC matrix	A matrix that describes the participation by various roles in completing tasks or deliverables for a project or business process; RASIC is an acronym derived from the five key responsibilities most typically used: responsible, accountable, supporter, informed and consulted; (the variant RASCI is sometimes used with the same meaning)

Term	Definition
RBAC	Role Based Access Control; an approach to restricting system access to authorised users; it is a policy-neutral access-control mechanism defined around roles and privileges
RFID	Radio Frequency Identification; the use of electromagnetic fields to automatically identify and track tags attached to objects
RoC	Report on Compliance; a report documenting detailed results from a PCI DSS assessment
RPO	Recovery Point Objective; the maximum targeted period in which data (transactions) might be lost from an IT service due to a disaster
RTO	Recovery Time Objective; the targeted duration of time and a service level within which a business process must be restored after a disaster
SaaS	Software as a Service; a cloud computing service model where the consumer is able to use the provider's applications running on a cloud infrastructure
SAD	Sensitive Authentication Data
SAML	Security Assertion Markup Language; an open standard for exchanging authentication and authorisation data between parties, in particular, between an identity provider and a service provider
SAQ	Self-Assessment Questionnaire; a merchant's statement of PCI DSS compliance; it includes a series of yes-or-no questions for each applicable requirement
SCD	Secure Cryptographic Device; a device that is used either for the acceptance and encryption of account data at the POS or for cryptographic key management functions and/or the decryption of account data. SCDs used for acceptance or encryption of account data at the POS are also referred to as POIs. SCDs used for cryptographic key management functions and/or the decryption of account data are typically HSMs
SDLC	Systems Development Life Cycle; also used for Software Development Life Cycle
Sensitive authentication data	Data used by the issuers of personal cards to authorise transactions; it includes but is not limited to the full magnetic data stripe, the CSC, the PIN and the PIN block; in a broad sense, sensitive authentication data is considered to be part of cardholder data; (see cardholder data)
Service code	In a payment card, the three- or four- digit value that follows the expiration date of the card; it is used for various things such as defining service attributes, differentiating between international and national interchange, or identifying usage restrictions
SIEM	Security Information and Event Management
SLA	Service Level Agreement
S/MIME	Secure/Multipurpose Internet Mail Extensions; a standard for public key encryption and signing of MIME data

Term	Definition
SMS	Short Message Service; a text messaging service component of most telephone, Internet, and mobile device systems
SMTP	Simple Mail Transfer Protocol; a communication protocol for electronic mail transmission
SNMP	Simple Network Management Protocol; an Internet Standard protocol for collecting and organising information about managed devices on IP networks and for modifying that information to change device behaviour
Soft delete	A delete operation that does not permanently delete data, but only marks it as deleted and renders it invisible to (normal) users, while remaining stored in the database; the opposite of hard delete
Special categories of personal data	Personal data that refers to or reveals any of the following: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetic data • Biometric data for the purpose of uniquely identifying a natural person • Health data • Data concerning a natural person's sex life or sexual orientation
Spoofing attack	A situation in which a person or program successfully identifies as another by falsifying data, to gain an illegitimate advantage
Spyware	Software that is installed and used in an unauthorised way to capture information (e.g. keystrokes, bank details, credit cards and passwords)
SRED	Secure Read and Exchange of Data; in PCI DSS, a module that ensures that cardholder account data is protected at the point of acceptance, which will assist in meeting the required security considerations of the wider point-to-point security process
SSID	Service Set Identifier; an identifier used for a group of network devices; it serves as a "network name" and typically consists of a natural language label
SSL	Secure Sockets Layer; a cryptographic protocol used for network traffic, deprecated in 2011
SSRM	Shared Security Responsibility Model; a model that defines the responsibilities of cloud service providers and customers for the security of the cloud environment
Structured data (or information)	Data that is aligned to a predefined data model and accordingly contained in well-identified data fields or columns; typical examples include data stored in relational databases or in spreadsheets (with well-identified columns)

Term	Definition
TCP	Transmission Control Protocol; one of the main protocols of the Internet protocol suite; It originated in the initial network implementation in which it complemented the IP
TCP/IP	Transmission Control Protocol/Internet Protocol; see Internet protocol suite
TLS	Transport Layer Security; a cryptographic protocol designed to provide communications security over a computer network; it replaced the now-deprecated SSL
UAT	User Acceptance Testing; a process of verifying that a solution works for the user
UDP	User Datagram Protocol; one of the core members of the Internet protocol suite; it enables computer applications to send messages, in this case referred to as datagrams, to other hosts on an IP network
UEM	Unified Endpoint Management; a class of software tools that provide a single management interface for mobile, PC and other devices; it can also be used to refer more generally to the management of all types of endpoint devices (typically using such tools)
UID	Unique Identifier
Unstructured data (or information)	Data that is not aligned to a predefined data model; typical examples include data contained in text documents, presentations, e-mails, images, audio files and video files
UPS	Uninterruptible Power Supply; an electrical apparatus that provides emergency power to a load when the input power source or mains power fails
UPT	Unattended Payment Terminal; a cardholder-operated payment terminal that reads, captures and transmits card information in conjunction with an unattended self-service device
URL	Uniform Resource Locator; a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it; colloquially termed a web address
USB	Universal Serial Bus; an industry standard that establishes specifications for cables and connectors and protocols for connection, communication and power supply between computers, peripheral devices and other computers
UTC	Coordinated Universal Time; the primary time standard by which the world regulates clocks and time
UTM	Unified Threat Management; an approach to information security where a single hardware or software installation provides multiple security functions
Virtualisation	The act of creating a virtual (rather than actual) version of something at the same abstraction level, including virtual computer hardware platforms, storage devices, and computer network resources

Term	Definition
VLAN	Virtual Local Area Network; any broadcast domain that is partitioned and isolated in a computer network at the data link layer; it can keep network applications separate despite being connected to the same physical network, and without requiring multiple sets of cabling and networking devices to be deployed
VoIP	Voice over IP; a method and group of technologies for the delivery of voice communications and multimedia sessions over IP networks; also referred to as IP telephony
VPN	Virtual Private Network; an extension of a private network across a public network, enabling users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network
VRF	Virtual Routing and Forwarding; a technology that allows multiple instances of a routing table to co-exist within the same router at the same time
WAN	Wide Area Network; a telecommunications network that extends over a large geographical area for the primary purpose of computer networking
WAP	Wireless Access Point; see AP
WLAN	Wireless Local Area Network; a wireless computer network that links two or more devices using wireless communication to form a LAN within a limited area such as an office building
WPA	Wi-Fi Protected Access; a security and security certification program developed by the Wi-Fi Alliance to secure wireless computer networks; WPA2 and WPA3 refer to more recent versions which have introduced increased security
WPA2	See WPA
WPA3	See WPA
XML	Extensible Markup Language; a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable