Table of Contents

Definition of Terms

1. ***Administration/Administrators, Types of***

1.1. Application Administrator

2. ***Application administrators are responsible for installing, updating, configuring, loading tuning, upgrading, diagnosing, monitoring and keeping the package up and running for internal and third-party applications. The applications they support can also include DevOps***

"DevOps" is an emerging set of principles, methods, and practices for communication, collaboration and integration between software development (application/software engineering) and IT operations (systems administration/infrastructure) professionals. Source: Department of Defense Cloud Computing Strategy

DevOps is an agile relationship between development and IT operations. The goal of DevOps is to change and improve the relationship by advocating better communications and collaboration between development and operations.

Enterprise Resource Planning (ERP) Systems or applications to support the Internet of "Things" (IoT).

2.1. Database Administrators (DBAs)

Database Administrators (DBAs)/Database Administration includes the creating, maintaining, backing up, querying, tuning, and assigning user rights controlling access of an application or Information System (IS) databases.

2.2. Interface Administrator

Interface Administrators are responsible for creating, monitoring, updating, and maintaining application/IS interfaces and ensuring the interfaces exchange data properly.

2.3. System Administrator (SysAdmin)

For this contract, a SysAdmin does not administer the infrastructure or servers supporting an IS which runs in a computing facility (such as the Global Combat Support System-Air Force (GCSS-AF) or Defense Information Systems Agency (DISA)) – those services are provided under the Air Force NetCents NetOps and Infrastructure Solutions Full and Open Contract.

A SysAdmin administers and manages systems, specifically, either the servers that support an Information System (IS) or the servers in a development and test environment. The SysAdmin is responsible for installing, updating (server software), configuring, tuning, upgrading, diagnosing, monitoring and generally keeping the server operational and in compliance with security mandates. SysAdmins are also responsible for backing up, managing and restoring data as well as providing technical support to the server users.

3. Application Software

Application software is the software installed onto an Operating System. Applications are written to run under the various Operating Systems. Applications include things like word processing programs, spread sheets, email software, etc.

4. Approved Products List (APL)

4.1. Department of Defense Information Network Approved Products List (DODIN APL)

The DODIN APL is established in accordance with the Unified Capabilities Requirements (UCR 2013) document and mandated by the DOD Instruction (DODI) 8100.04, *Unified Capabilities*. Its purpose is to maintain a single consolidated list of products that have completed Interoperability (IO) and Cybersecurity certification. Use of the DODIN APL allows DOD Components to purchase and operate systems over all DOD network infrastructures. This is the link for the DODIN APL: https://aplits.disa.mil/processAPList.action Common Access Card (CAC) with Personal Identification Number (PIN) is required.

4.2. Air Force Evaluated/Approved Products Listing (AF E/APL)

The AF E/APL is established in accordance with Air Force Manual (AFMAN) 17-1203, *Information Technology (IT) Asset Management (ITAM)*. All software products for use on Air Force networks must be evaluated and certified/assessed by the appropriate Security Control Assessor (SCA), formerly known as the Certification Authority according to AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT)*. The list of evaluated products can be found at https://cs2.eis.af.mil/sites/10336/lists/cotsgots%20software/epl.aspx

5. Architecture

The structure of components, their relationships, and the principles and guidelines governing their design and evolution over time.

5.1. Architecture Models and Views and Architectural Description

The Department of Defense Architecture Framework (DoDAF) enables architectural content that is "Fit-for-Purpose" as an architectural description consistent with specific project or mission objectives.

Visualizing architectural data is accomplished through models. Models can be documents, spreadsheets, dashboards, or other graphical representations and serve as a template for organizing and displaying data in a more easily understood format. When data is collected and presented as a "filled-in" model, the result is called a view. Organized collections of views (often representing processes, systems, services, standards, etc.) are referred to as viewpoints, and with appropriate definitions are collectively called the Architectural Description.

5.2. Enterprise Architecture

The explicit description and documentation of the current and desired relationships among business and management processes and Information Technology (IT).

5.3. Integrated Architecture

An architecture consisting of multiples views or perspectives facilitating integration and promoting interoperability across capabilities and among integrated architectures". The term integrated means that data required in more than one instance in architectural views is commonly understood across those views.

6. Automatic Identification Technology (AIT)

A suite of technologies enabling the automatic capture of data, thereby enhancing the ability to identify, track, document, and control assets (e.g., materiel), and deploying and redeploying forces, equipment, personnel, and cargo. AIT encompasses a variety of data storage or carrier technologies such as linear bar codes, two-dimensional symbols, magnetic strips, integrated circuit cards, or satellite tracking transponders and Radio Frequency Identification (RFID) tags used for marking or tagging individual items, equipment, air pallets, or containers. AIT is also referred to commercially as automatic identification data capture.

7. Build

(noun) A version of software that meets a specified subset of the requirements that the completed software will meet or the period of time during which such a version is developed. Note: It may take several builds to reach a releasable version.

(verb) The process by which source code is converted into a stand-alone form that can be run on a computer or to the form itself. One of the most important steps of a software build is the compilation process, where source code files are converted into executable code.

8. Business Analysis

Business analysis is the practice of enabling change in an enterprise by defining needs and recommending solutions that deliver value to stakeholders. Business analysis enables an enterprise to articulate needs and the rationale for change, and to design and describe solutions that can deliver value.

Business analysis is performed on a variety of initiatives within an enterprise. Initiatives may be strategic, tactical, or operational. Business analysis may be performed within the boundaries of a project or throughout enterprise evolution and continuous improvement. It can be used to understand the current state, to define the future state, and to determine the activities required to move from the current to the future state.

Business analysis can be performed from a diverse array of perspectives. The Guide to the Business Analysis Body of Knowledge (BABOK® Guide) describes several of these perspectives: agile, business intelligence, information technology, business architecture, and business process management. One or many perspectives may apply to an initiative.

9. Business Process

A business process refers to a wide range of structured, often chained, activities or tasks conducted by people or equipment to produce a specific service or product for a particular user or consumer. Business processes are implemented to accomplish a predetermined organizational goal. Business processes occur at all organizational levels; some are visible to customers, while others are not.

The term business process may also refer to the cumulative effects of all steps progressing toward a business goal. This sequence of steps can be most clearly depicted using a flowchart.

10. Business Use Case

A business use-case model is a model that describes the processes of a business and their interactions with external parties like customers and partners.

11. Capability

The ability to achieve a desired effect under specified [performance] standards and conditions through combinations of ways and means [activities and resources] to perform a set of activities.

12. Cloud Terminology

12.1. Cloud Computing

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

12.2. Cloud Service Provider (CSP)

An organization, commercial or Private, that offers/provides Cloud Services. Unqualified use of the term refers to any or all Cloud Service Providers, DoD or non-DoD.

12.2.1. Commercial CSP

Refers to a Non-DoD Non-Federal Government organization offering cloud services to the public and/or government customers as part of a business venture, typically for a fee with the intent to make a profit.

12.2.2. DoD CSP

Refers to a DoD organization offering Cloud Services which may be owned and operated by DoD or a contractor for the benefit of the Department (e.g., milCloud). Such services will typically be offered under a cost recovery model. A DoD CSP may offer cloud services to non-DoD mission partners

12.2.3. Non-DoD CSP

Refers to a commercial or Federal Government owned and operated CSP.

12.3. Deployment Methods

12.3.1. Private Cloud

The 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.

12.3.2. DoD Private Cloud

A DoD Community Cloud provides services for the exclusive use of one or more DoD customer organizations; supporting multiple DoD tenants or DoD sponsored tenants in the same cloud. The DoD maintains ultimate authority over the usage of the cloud services, and any non-DoD use of services must be authorized and sponsored through the DoD. Resources providing the cloud services must be dedicated to DoD use and have physical separation from resources not dedicated to DoD use. MilCloud is the DoD private cloud built and operated by the Defense Information Systems Agency (DISA).

12.3.3. Community Cloud

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

12.3.4. Federal Government Community Cloud

A community cloud offered for use by multiple Federal Government organizations (which include the DoD). Resources providing the cloud services must be dedicated to Federal Government use and require physical separation from non-Federal customers.

12.3.5. Public Cloud

The 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.

12.3.6. Hybrid cloud

The cloud infrastructure is a 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 (e.g., cloud bursting for load balancing between clouds).

12.4. Essential Characteristics

12.4.1. On-demand self-service

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

12.4.2. Broad network access

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

12.4.3. Resource pooling

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

12.4.4. Rapid elasticity

Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

12.4.5. Measured service

Cloud systems automatically control and optimize resource use by leveraging a metering capability1 at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

12.5. Service Models

12.5.1. Software as a Service (SaaS)

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure2. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

12.5.2. Platform as a Service (PaaS)

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.3 The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

12.5.3. Infrastructure as a Service (IaaS)

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

13. Commercial Item

Any item, other than real property, that is of a type customarily used by the general public or by non-governmental entities for purposes other than governmental purposes, and--

a. Has been sold, leased, or licensed to the general public; or,
b. Has been offered for sale, lease, or license to the general public

14. Commercial Off-The-Shelf (COTS)

Any item of supply that is

a. A commercial item (reference commercial item definition)
b. Sold in substantial quantities in the commercial marketplace and
c. Offered to the government, under a contract or subcontract at any tier, without modification, in the same form in which it is sold in the commercial marketplace.

15. Cybersecurity

Measures that protect and defend DoD information and information technology (IT) from damage, and restoring the computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities. DoD information includes information that is entered, processed, transmitted, stored, retrieved, displayed, or destroyed.

15.1. Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

15.2. Integrity

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

15.3. Availability

Ensuring timely and reliable access to and use of information.

15.4. Authentication

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

15.5. Authorization

Access privileges granted to a user, program, or process or the act of granting those privileges.

15.6. Accountability (Nonrepudiation)

A security service that provides protection against false denial of involvement in a communication. A method of guaranteeing message transmission between parties via digital signature and/or encryption.

16. Data

Representation of information in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Examples could be whole models, packages, entities, attributes, classes, domain values, enumeration values, records, tables, rows, columns, and fields.

17. Data Store

A data store is a repository for persistently storing collections of data, such as a database, a file system or a directory. The data stored can be any type rendered in digital format and placed in electronic media. Examples include text, image, video files and audio files.

18. Database

A collection of related data stored in one or more computerized files in a manner that is accessible by users or computer programs via a database management system.

19. Database Conversion

Database conversion deals with changes required to move or convert data from one physical environment format to that of another, like moving data from one electronic medium or database product onto another format.

20. Database Management System

An integrated set of computer programs that provides the capabilities needed to establish, modify, make available, and maintain the integrity of a database.

21. Decommission Planning and Execution

Decommission planning and execution of a legacy system must be performed in a way that preserves data and application logic, appropriately notifies and coordinated with affected parties, and disposes of hardware and software in compliance with established federal guidelines. The following identify key elements of a decommission plan.

21.1. Software Archive

This section describes the plan for archiving the software library files and related documentation in the system being decommissioned, including which software will be archived, and in which format. The intent of the software archive is to provide sufficient stored software so that the system could be re-initiated if necessary. Software associated with decommissioned systems should be archived based on the records disposition schedules.

21.2. Documentation Archive

This section describes the plan for archiving the hard copy and soft copy user documentation for the system(s) being decommissioned, including which documentation will be archived and in which format. The intent of the documentation storage is to provide sufficient archived documentation so that the system could be re-initiated and used if necessary.

Documentation associated with decommissioned systems should be archived based on the records disposition schedules.

21.3. Data Archive

This section describes the plan for archiving data files and related documentation of the system being decommissioned. Any data that has not been migrated to the receiving/target system should be archived based on Air Force policy for records retention.

This section includes an outline on which data will migrate, which data will be archived, and data formats.

21.4. Security Archive

This section describes the system security and access rights associated with the legacy system in order to provide the necessary security information in the decommission plan so that the system could be reconstituted with the same security considerations, if necessary. The inclusion of the legacy system's security overview ensures that the applicable security considerations become part of the archive.

This section also identifies the impacts to the enterprise security posture caused by the decommissioning of the system and the rationale for changes to the authorization boundaries that are impacted by the decommissioning of the system. Identify and address impacts to

common controls provided by the legacy system and the systems that rely upon those common controls.

22. Department of Defense Architecture Framework (DoDAF)

The Department of Defense Architecture Framework (DoDAF) is the overarching, comprehensive framework and conceptual model enabling the development of architectures to facilitate the ability of Department of Defense (DoD) managers at all levels to make key decisions more effectively. The DoDAF serves as one of the principal pillars supporting the DoD Chief Information Officer (CIO) in his responsibilities for development and maintenance of architectures required under the Clinger-Cohen Act. DoDAF is prescribed for the use and development of Architectural Descriptions in the Department. It also provides extensive guidance on the development of architectures supporting the adoption and execution of Net-centric services within the Department.

DoD Components are expected to conform to DoDAF to the maximum extent possible in development of architectures within the Department. Conformance ensures that reuse of information, architecture artifacts, models, and viewpoints can be shared with common understanding.

Model	Description
Operational Views (OV)	
OV-1: High-Level Operational Concept Graphic	The high-level graphical/textual description of the operational concept.
OV-2: Operational Resource Flow Description	A description of the Resource Flows exchanged between operational activities.
OV-3: Operational Resource Flow Matrix	A description of the resources exchanged and the relevant attributes of the exchanges.
OV-4: Organizational Relationships Chart	The organizational context, role or other relationships among organizations.
OV-5a: Operational Activity Decomposition Tree	The capabilities and activities (operational activities) organized in a hierarchal structure.
OV-5b: Operational Activity Model	The context of capabilities and activities (operational activities) and their relationships among activities, inputs, and outputs; Additional data can show cost, performers, or other pertinent information.
OV-6a: Operational Rules Model	One of three models used to describe activity (operational activity). It identifies business rules that constrain operations.
OV-6b: State Transition Description	One of three models used to describe operational activity (activity). It identifies

Model	Description
	business process (activity) responses to events (usually, very short activities).
OV-6c: Event-Trace Description	One of three models used to describe activity (operational activity). It traces actions in a scenario or sequence of events.
System Views (SV)	
SV-1 Systems Interface Description	The identification of systems, system items, and their interconnections.
SV-2 Systems Resource Flow Description	A description of Resource Flows exchanged between systems.
SV-3 Systems-Systems Matrix	The relationships among systems in a given Architectural Description. It can be designed to show relationships of interest, (e.g., system-type interfaces, planned vs. existing interfaces).
SV-4 Systems Functionality Description	The functions (activities) performed by systems and the system data flows among system functions (activities).
SV-5a Operational Activity to Systems Function Traceability Matrix	A mapping of system functions (activities) back to operational activities (activities).
SV-5b Operational Activity to Systems Traceability Matrix	A mapping of systems back to capabilities or operational activities (activities).
SV-6 Systems Resource Flow Matrix	Provides details of system resource flow elements being exchanged between systems and the attributes of that exchange.
SV-7 Systems Measures Matrix	
SV-8 Systems Evolution Description	The planned incremental steps toward migrating a suite of systems to a more efficient suite, or toward evolving a current system to a future implementation.
SV-9 Systems Technology & Skills Forecast	The emerging technologies, software/hardware products, and skills that are expected to be available in a given set of time frames and that will affect future system development.
SV-10a Systems Rules Model	One of three models used to describe system functionality. It identifies constraints that are imposed on systems functionality due to some aspect of system design or implementation.

Model	Description
SV-10b Systems State Transition Description	One of three models used to describe system functionality. It identifies responses of systems to events.
SV-10c Systems Event-Trace Description	One of three models used to describe system functionality. It identifies system-specific refinements of critical sequences of events described in the Operational Viewpoint.

23. Design, Software

The process of implementing software solutions to one or more sets of problems. One of the main components of software design is the software requirements analysis (SRA). SRA is a part of the software development process that lists specifications used in software engineering. Design includes but is not limited to: system design dataflow diagrams/documentation, data modeling, and preliminary design reviews (PDR) and critical design reviews (CDR).

24. Deployment

The relocation of materiel (to include software deployment) to desired operational areas. Deployment encompasses all activities from origin through destination.

A deployment either introduces a new release into the production environment or expands the user base of existing functionality. Deployment includes training and information systems (IS) operations activities such as service desk support.

25. Development

The process of working out and extending the theoretical, practical, and useful applications of a basic design or idea. Design, building, modification, or improvement of the software prototype as determined by the basic idea or concept. Includes all efforts directed toward programs engineered for service use but which have not yet been approved for operation, and all efforts directed toward development engineering and test of systems, and support programs that have been approved for production and service deployment.

25.1. ***Software Development***

Software development is the process of computer programming (using a Programming Language), documenting, testing, and bug fixing involved in creating and maintaining applications, information systems (ISs) and frameworks resulting in a software product. Software development is a process of writing and maintaining the source code, but in a broader sense, it includes all that is involved between the conception of the desired software through to the final manifestation of the software. Therefore, software development may include research, new development, prototyping, modification, reuse, re-engineering, maintenance, or any other activities that result in software products.

26. DevOps

"DevOps" is an emerging set of principles, methods, and practices for communication, collaboration and integration between software development (application/software engineering) and IT operations (systems administration/infrastructure) professionals. Source: Department of Defense Cloud Computing Strategy

DevOps is an agile relationship between development and IT operations. The goal of DevOps is to change and improve the relationship by advocating better communications and collaboration between development and operations.

27. Enterprise Resource Planning (ERP) Systems

A configurable, packaged, commercial software package designed to enable an organization to integrate and manage the efficient and effective use of resources by providing a total, integrated solution for the organization information-processing needs. Consider a supply chain system which tracks information from procurement and inventory to automatically raise purchase orders for approval; and is capable of generating multiple reports on a single click. ERP systems are capable of accessing data from all the modules and run it as an enterprise-wide system. ERPs tend to be very large, involve a multitude of stakeholders, and take a long time and considerable cost to implement.

27.1. ERP Commercially Available Off-the-Shelf (COTS)

Packages available commercially for purchase. Organizations adopt these packages for many benefits such as outsourced system maintenance, system improvements and error corrections.

27.2. Implementation and support of ERP solutions

The ERP implementation process includes identifying the mismatch between COTS product selected and the organizational goals, recruiting an implementation team in-house or selecting a contractor for the transition of legacy onto the new system fall under the implementation phase. Other activities included in this phase are: ERP set-ups, development effort for customizations required, data transfer from legacy to ERP, training of end-users and deployment.

27.3. ERP Support

The maintenance/support phase refers to addressing problems post deployment. Any updates in the ERP package or issues encountered by the end users are corrected with the help of the implementation contractor or ERP vendor; based on the contract terms identified during the acquisition and implementation phases.

28. Enterprise Service

Any capability provided for broad use across the Department of Defense (DoD) that enables awareness of, access to, or delivers information across DoD networks.

a. Enterprise services may be provided by any source within the DoD or any trusted partners.

b. Enterprise services providing data or information must be authoritative and, therefore, trusted as being accurate, complete, and having assured integrity. Authoritative information has a pedigree that can be traced to a trusted source.
c. Enterprise services include environments that are composed of multiple service layers such as the infrastructure, infrastructure services, platform services, common user services, enterprise service management, and mission assurance services.

29. Environment

Aggregate of external procedures, conditions, and objects affecting the development, operation, and maintenance of an information system (IS).

30. Framework

A framework, or software framework, is a platform for developing software. It provides a foundation on which software developers can build programs for a specific platform. For example, a framework may include predefined classes and functions that can be used to process input, manage hardware devices, and interact with system software. This streamlines the development process since programmers don't need to reinvent the wheel each time they develop new software.

A framework is similar to an application programming interface (API), though technically a framework includes an API. As the name suggests, a framework serves as a foundation for programming, while an API provides access to the elements supported by the framework. A framework may also include code libraries, a compiler, and other programs used in the software development process.

31. Free and Open Source Software (FOSS)

FOSS is software licensed to users under an open source license, which generally allows users the freedom to access and use the software source code for any purpose, to study and modify the software, and to redistribute copies of the original and modified software without payment of royalties. This is the DoD website for sharing Government/DoD FOSS: http://forge.mil/

Open source software is allowed in DoD systems, as long as it passes all the certification testing required of COTS, GOTS, and newly developed software. To check for the latest policy on open source software check the DoD Chief Information Office website: http://www.defenselink.mil/cio-nii/

32. Form, Fit, Function, and Interface (F3I)

A concept used for the update or upgrade of a system whereby only a portion or subsystem of the entire system is replaced. The updated item is said to be Form/Fit/Function and interface compatible when it can be inserted into the existing system without impacting system operation.

33. Functional Business Area Expert (FBAE)

Recognized for strong expertise in industry issues and trends. Utilizes functional area expertise gained through direct industry experience to assess the operational and functional baseline of an

Information System (IS) and the functional business process. Identifies information technology inadequacies or deficiencies affecting the functional area's ability to support or meet stakeholder requirements.

34. Government Off the Shelf (GOTS)

Government-off-the-Shelf (GOTS) refers to software and hardware products that are developed and owned by a government entity and ready-to-use to meet unique government requirements.

Typically GOTS are developed by the technical staff of the government agency for which it is created. It is sometimes developed by an external entity, but with funding and specification from the agency. Because agencies can directly control all aspects of GOTS products, these are sometimes preferred for government purposes.

GOTS software solutions can normally be shared among government agencies without additional cost to the government. GOTS hardware solutions are typically provided at cost (meaning research and development costs are not recouped).

35. Implementation

Planning; coordinating; scheduling; deploying/installing (or providing all needed technical assistance to deploy/install) and transitioning a technical solution (e.g. information system) into the operational environment. Implementation services also include performing data conversion before loading data into the system and training appropriate personnel on the operation and use of the technical solution.

36. Information Assurance (IA)

DoDI 8500.01 *Cybersecurity*, 24 March 2014 adopts the term "cybersecurity" as it is defined in National Security Presidential Directive (NSPD)-54/Homeland Security Presidential Directive (HSPD)-23 to be used throughout DoD instead of the term "information assurance (IA)" Refer to Cybersecurity.

37. Information Display Solutions and Services

37.1. Dashboard

A dashboard is a data visualization tool that displays the current status of metrics and key performance indicators (KPIs) for an enterprise. Dashboards consolidate and arrange numbers, metrics and sometimes performance scorecards on a single screen.

37.2. Mashup

A mashup is a Web page or application that integrates complementary elements from two or more sources. Mash-ups are often defined by the type of content that they aggregate. A content mash-up, for example, brings together various types of content for presentation through an interface. That content could include -- among other things -- text, data feeds, video and social updates. An enterprise mash-up typically combines internal corporate data and applications with externally sourced data, SaaS (software as a service) and Web content. Business mash-ups

might also provide integration with the business computing environment, data governance, business intelligence (BI)/ business analytics (BA), more sophisticated programming tools and more stringent security measures.

37.3. Portal

A portal is a specially-designed web site that brings information together from diverse sources in a uniform way. Usually, each information source gets its dedicated area on the page for displaying information (a portlet); often, the user can configure which ones to display.

37.4. Rich Internet Application (RIA)

A web-based application that has some characteristics of graphical desktop applications. A typical Rich Internet Application is decomposed into three layers: the presentation layer, business layer, and data layer. RIA frameworks include: Curl, Adobe Flash/Adobe Flex/AIR, Java/JavaFX, uniPaaS, and Microsoft Silverlight.

38. Information System (IS)

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. IS can include as constituent components, a range of diverse computing platforms from high-end supercomputers to personal digital assistants and cellular telephones. IS can also include very specialized systems and devices (e.g., telecommunications systems, industrial/process control systems, testing and calibration devices, weapons systems, command and control systems, and environmental control systems).

38.1. Federal Information System

A federal information system is an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

39. Information Technology (IT)

Includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.

40. Information Technology (IT) Service Desk

As the single primary point of contact, the Service Desk is the interface between the user and the service. If there is an issue whether it is an unclear Event or Alert message, an Incident or Problem, or an Access issue, the user is going to contact the Service Desk for assistance if the issue cannot be resolved through self-help methods.

The purpose of the Service Desk is to:

a. Be primary contact point for all calls, questions, service requests, complaints, and remarks
b. Be primary provider of ongoing monitoring and management of mission partner satisfaction through appropriate communication channels
c. Manage the incident lifecycle

40.1. Access Management

The process of granting authorized users the right to use a service while preventing access to non-authorized users. The process provides the ability to control and track who has access to data and services ("who" may be another system, service, or process, as well as an individual). It contributes to achieving the appropriate confidentiality, availability, and integrity of the command's data and includes levels of access to the service catalog for requesting services, access to data, and access to facilities.

40.2. Event Management

The process of identifying and prioritizing all events that occur throughout the IT infrastructure and establish the appropriate response to those events. Event Management monitors, filters, and notifies of actions and occurrences that have an effect on the services provided. This process is proactive and reactive. Proactively, Operations is notified of events that may cause service degradation and outages enabling operations to take steps necessary to avert any service level agreement (SLA) breach. Reactively, Event Management interfaces with Operations, Incident, Problem and Change Management to provide information and corrective actions for those events.

40.3. Incident Management

The process of restoring normal service operation as quickly as possible, minimizing the adverse impact on mission partner operations, thus ensuring that the best possible levels of service quality, security, and availability are maintained. The focus is on reducing the duration and consequences of service outages from a mission partner perspective; not on finding the root cause of the incident.

40.4. Problem Management

The process of preventing problems and incidents from happening, eliminate recurring incidents and minimizing the impact of incidents that cannot be prevented. Problem Management includes the activities required to diagnose the root cause of incidents, determining the resolution to those problems and providing workarounds to Incident Management.

40.5. Request Management

The process of fulfilling requests from users and routing each request to the appropriate process owner for handling within accepted service levels. Request Fulfillment is responsible for the entire lifecycle of the request.

41. Information Technology (IT) Services

The performance of any work related to IT and the operation of IT, including National Security Systems (NSS). This includes outsourced IT-based business processes, outsourced IT, and outsourced (e.g. contractor) information functions.

42. Internet of "Things" (IoT)

The IoT consists of two foundational aspects—1) the Internet itself and, 2) semi-autonomous devices (the "things") that leverage inexpensive computing, networking, sensing, and actuation capabilities to sense the physical world and act on it. Such devices have the capability to connect to the Internet—being Internet Protocol (IP) based—but may also be deployed in stand-alone IP networks not connected to the Internet.

The IoT scenario allows objects, animals or people unique identifiers and the ability to transfer data over a network with requiring human-to-human or human-to-machine interaction.

Examples of "things" in the IoT are a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile with built-in sensors to alert the driver when tire pressure is low -- or any other natural or man-made object that can be assigned an IP address and provided with the ability to transfer data over a network.

43. Legacy System

A system or application in which an organization has already invested considerable time and money.

44. Life-Cycle Services

The scope of activities associated with a system, encompassing the system's initiation, development, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.

45. Maintainability

The capability of an item to be retained in or restored to a specified condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures and routines, at each prescribed level of maintenance and repair.

46. Migration

The process of moving from the use of one operating environment to another operating environment. Migration can involve upgrading to new hardware, new software or both.

46.1. Data Migration

Data migration is the process of transferring data between data storage systems, data formats or computer systems. A data migration project is usually undertaken to replace or upgrade servers or storage equipment, for a website consolidation, to conduct server maintenance or to relocate a data center.

46.2. System Migration

System migration involves moving a set of instructions or programs from one platform to another. Migration of systems may involve downtime, while the old system is replaced with a new one. Migration can be from a mainframe computer to more open systems such as Cloud Computing platforms.

A system migration may be performed using tools that automatically convert data from one form to another or using tools that convert code from one platform to another. A system migration my also involve using software than can run the code from the old system on the new system.

47. Mobile Application Development

The act or process by which application software is developed for mobile devices, such as personal digital assistants, enterprise digital assistants or mobile phones.

48. Mobile Information Technology (IT) Programming Services

Mobile IT is the ability to deliver IT services to employees working on mobile devices. Smart phones, tablets and other mobile devices are rapidly becoming the vehicle for doing business. Mobile IT is more than implementing a "bring your own device" (BYOD) program. Programming services for Mobile IT includes creating new applications or redesigning legacy systems to work -- and to work securely – with or on mobile devices.

49. Modernization

Software modernization means the conversion and rewriting of a legacy system, software libraries and protocols to a modern computer programming language and porting the new IS to a new hardware platform.

50. Modification

A configuration change to the Form, Fit, Function, and Interface (F3I) of an in-service, configuration-managed or produced Configuration Item (CI). Modifications are primarily defined by their purpose. A capability modification alters the F3I of an asset in a manner that requires a change to the existing system, performance, or technical specification of the asset. Such modifications are generally accomplished to add a new capability or function to a system or component, or to enhance the existing technical performance or **Error! Reference source not found.** (OE) of the asset. Some modification alter the F3I of an asset in a manner that does not change the existing system, performance, or technical specification of the asset. Such modifications are generally accomplished to correct product quality deficiencies, or to bring the asset in compliance with, or to maintain the established technical or performance specification(s) associated with the asset. Modifications may also include efforts with the primary purpose of improving the reliability, availability, maintainability, or supportability of an asset, or to reduce its ownership costs.

51. National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology (NIST) was founded in 1901 and is now part of the U.S. Department of Commerce. NIST in partnership with the Department of Defense

(DoD), the Office of the Director of National Intelligence (ODNI), and the Committee on National Security Systems (CNSS), has developed a common information security framework for the federal government and its contractors. The intent of this common framework is to improve information security, strengthen risk management processes, and encourage reciprocity among federal agencies.

From the smart electric power grid and electronic health records to atomic clocks, advanced nanomaterials, and computer chips, innumerable products and services rely in some way on technology, measurement, and standards provided by the National Institute of Standards and Technology.

NIST is working with many public and private sector entities to establish mappings and relationships between the security standards and guidelines developed by NIST and the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC).

51.1. Federal Information Processing Standards (FIPS)

Federal Information Processing Standards (FIPS) are approved by the Secretary of Commerce and issued by NIST in accordance with the Federal Information Security Management Act (FISMA). FIPS are compulsory and binding for federal agencies. FISMA requires that federal agencies comply with these standards, and therefore, agencies may not waive their use.

51.2. Special Publications (SPs)

Special Publications (SPs) are developed and issued by NIST as recommendations and guidance documents. For other than national security programs and systems, federal agencies must follow those NIST Special Publications mandated in a Federal Information Processing Standard. FIPS 200 mandates the use of Special Publication 800-53, as amended. In addition, Office of Management and Budget (OMB) policies (including OMB Reporting Instructions for FISMA and Agency Privacy Management) state that for other than national security programs and systems, federal agencies must follow certain specific NIST Special Publications.

52. National Security System (NSS)

The term “national security system” means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

a. the function, operation, or use of which—
   (1) involves intelligence activities;
   (2) involves cryptologic activities related to national security;
   (3) involves command and control of military forces;
   (4) involves equipment that is an integral part of a weapon or weapons system; or
   (5) may be critical to the direct fulfillment of military or intelligence missions; or

b. is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

53. Net-Centric

Relating to or representing the attributes of a robust, globally interconnected network environment (including infrastructure, systems, processes, and people) in which data are shared timely and seamlessly among users, applications, and platforms.

54. Operating System (OS)

Operating System is the System Software that makes a computer work. An Operating System (OS) is software that acts as an interface between the user and the hardware. OS examples are Windows or Linux.

55. Patch

An update to an operating system, application, or other software issued specifically to correct particular problems with the software.

56. Performance Tuning

The process of making an application, system, database, or interface work effectively as possible to deliver data faster. Performance tuning includes optimizing the configuration of the application and database servers to remove bottlenecks or increase throughput, tuning structured query language (SQL) queries or modifying code to improve efficiency.

57. Platform, Computer

A computer platform generally refers to the operating system and computer hardware ***only***. The platform conforms to a set of standards that enable software developers to develop software applications for the platform. These same standards allow owners and managers to purchase appropriate applications and hardware.

58. Programming

Modifying code (includes but is not limited to removing cloned or dead code); adding new code; unit testing; documenting code.

58.1. Cloned Code

Redundant code caused by the common programming practice of replicating (or cloning) existing code and then customizing it to handle new demands on an application. An IT organization consequently spends corresponding amounts of its budget redundantly maintaining this code; a bug in one code fragment is also a bug in all of its hidden clones.

58.2. Dead Code

Unnecessary, inoperative code that can be removed without affecting the program functionality. Dead code includes functions and sub-programs that are never called, properties that are never

read or written, and constants and enumerations that are never referenced. Variables should be both read and written to. User-defined types can also be dead and a project may contain redundant application program interface (API) declarations. Even entire modules and classes can be completely redundant. The opposite of dead code is live, operational code. There are also several types of semi dead code, that is, live-looking code and controls that are not actually required at run-time.

59. Programming Language

In computer technology, a set of conventions in which instructions for the machine are written. An artificial language used to write instructions that can be translated into machine language and then executed by a computer. A compiled language is a language in which the set of instructions (or code) written by the programmer is converted into machine language by special software called a compiler prior to being executed. An interpreted language is a language in which the set of instructions (or code) written by the programmer is converted into machine language by special software called a compiler prior to being executed.

60. Radio Frequency Identification (RFID)

RFID is:

a. A means of identifying a unique object or person using a radio frequency transmission

b. Tags (or transponders) that store information, which can be transmitted wirelessly in an automated fashion

c. Readers (or interrogators) both stationary and hand-held read/write information from/to tags

60.1. Active RFID Tag

A radio frequency tag device that has the ability to produce its own radio signal not derived from an external radio source. Active RFID tags may hold relatively large amounts of data, are continuously powered, and are normally used when a longer tag read distance is desired.

60.2. Passive RFID Tag

A passive radio frequency tag that reflects energy from the reader or interrogator, or that receives and temporarily stores a small amount of energy from the reader and interrogator signal to generate the tag response.

61. Re-Engineering

Software Re-engineering is the examination and alteration of a system to reconstitute it in a new form. This process encompasses a combination of sub-processes such as reverse engineering, restructuring, recreating or updating documentation, forward engineering and retargeting.

62. Reliability

Reliability measures the probability that the system will perform without failure over a specified interval under specified conditions. Reliability must be sufficient to support the warfighting

capability needed in its expected operating environment. Considerations of reliability must support both availability metrics.

63. Requirements Analysis

The process of transforming stakeholder expectations into unique, quantitative, and measurable software requirements that can be used for defining a design solution for the software end products and related enabling products. This process also includes validation of the requirements to ensure that the requirements are well formed (clear and unambiguous), complete (agrees with customer and stakeholder needs and expectations), consistent (conflict free), and individually verifiable and traceable to a higher level requirement.

64. Risk Management Framework (RMF)

The six-step RMF includes security categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. The RMF promotes the concept of near real-time risk management and ongoing information system authorization through the implementation of robust continuous monitoring processes, provides senior leaders the necessary information to make cost-effective, risk-based decisions with regard to the organizational information systems supporting their core missions and business functions, and integrates information security into the enterprise architecture and system development life cycle. Applying the RMF within enterprises links risk management processes at the information system level to risk management processes at the organization level through a risk executive (function) and establishes lines of responsibility and accountability for security controls deployed within organizational information systems and inherited by those systems (i.e., common controls).

64.1. Security Requirements Guides (SRGs)

SRGs are collections of requirements applicable to a given technology family. SRGs represent an intermediate step between Control Correlation Identifiers (CCIs) and Security Technical Implementation Guides (STIGs). CCIs represent discrete, measurable, and actionable items sourced from Information Assurance (IA) controls defined in a policy, such as the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. STIGs provide product-specific information for validating and attaining compliance with requirements defined in the SRG for that product’s technology area.

There are four core SRGs: Application, Network, Operating System, and Policy. Each addresses the applicable CCIs in the context of the technology family. Subordinate to the core SRGs, there are Technology SRGs developed to address the technologies at a more granular level.

64.2. Security Technical Implementation Guides (STIGs)

The configuration standards for DoD IA and IA-enabled devices/systems. The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack. Implementation guide geared to a specific product and version. Contains all requirements that have been flagged as applicable for the product which have been selected on a DoD baseline.

65. Server Support Services

Server support services include: setting up and maintaining servers for ongoing operations, calibrating the server environment and addressing many of the technical questions around the server systems.

66. Software Assurance

Software assurance is the level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software, throughout the life cycle.

67. Software Development Methodologies

Methodologies developed through software engineering to manage the complexity of system development. Development methodologies include software engineering aids and high-level design analysis tools.

67.1. Agile Software Development (ASD)

Agile is a group of software development methodologies based on iterative and incremental development where requirements and solutions evolve through highly collaborative, self-organizing, cross-functional teams. Agile development relies on close cooperation and collaboration between all team members and stakeholders. Agile development principles include keeping requirements and documentation lightweight, and acknowledging that change is a normal and acceptable reality in software development.

Agile is an iterative development approach that focuses on mature technologies, continuous testing, test-driven development, continuous user involvement and requirements definition, and rapid early fielding of working functionality.

Agile methods emphasize real-time communication, preferably face-to-face, over written documents. Agile methods also emphasize working software as the primary measure of progress. There are a number of agile software development methodologies e.g. Crystal Methods, Dynamic Systems Development Model (DSDM), and Scrum.

67.2. Crystal Methods

Alistair Cockburn developed the Crystal Methods approach. His focus is on the people, interaction, community, skills, talents, and communications with the belief that these are what have the first-order effect on performance. Process, he says, is important, but secondary.

Cockburn's philosophy translates into a recognition that each team has a different set of talents and skills. Therefore each team should use a process uniquely tailored to it, and that process should be minimized - barely significant.

67.3. Extreme Programming (XP) Methodology

XP is a methodology for creating software within a very unstable environment. It allows flexibility within the modelling process.

The main goal of XP is to lower the cost of change in software requirements. With traditional system development methodologies, like the Waterfall Methodology, the requirements for the system are determined and often “frozen” at the beginning of the development project. This means that the cost of changing the requirements at a later stage in the project - something that is very common in the real-world can be very high.

67.4. Feature-Driven Development (FDD)

Feature-driven development is a client-centric, architecture-centric, and pragmatic software development process. In feature-driven development clients are the project stakeholders. As the name implies, FDD is centered on features. All aspects of the software development process are planned, managed, and tracked at that level, so at the level of features. A feature is a small client-valued function expressed in the form action, result, and object. So for example, calculate the total of a shopping cart. Features are to FDD as use cases are to the Rational Unified Process (RUP) and user stories are to Scrum - they're a primary source of requirements and the primary input into your planning efforts.

67.5. Incremental Development

Incremental development, also known as Evolutionary Acquisition in DoDI 5000.02, *Operation of the Defense Acquisition System*, involves dividing a system up into multiple "builds" or releases and developing the system one release at a time. A project performs project planning and requirements analysis one time only, and then repeats the design, construction, and testing processes multiple times to develop each build of the system. The first build of the system incorporates a subset of the planned capabilities; the next build adds another subset of the planned capabilities, and so on, until the system is complete.

67.6. Lean Software Development

Lean Development (LD) focuses on the creation of change-tolerant software. This methodology embodies the notion of dynamic stability which can be thought of as similar to how Scrum embraces controlled chaos.

67.7. Scrum

Scrum is a process framework that has been used to manage complex product development since the early 1990s. Scrum is not a process or a technique for building products; rather, it is a framework within which you can employ various processes and techniques. Scrum makes clear the relative efficacy of your product management and development practices so you can improve. The Scrum framework consists of Scrum Teams and their associated roles, events, artifacts, and rules. Each component within the framework serves a specific purpose and is essential to Scrum’s success and usage.

67.8. Waterfall

The waterfall methodology arose during the early 1970s as a remedy to the undisciplined “code and fix” method of software development. It is a "once-through, do-each-step once" methodology. In grand design, each phase is performed in sequence, and each phase is completed before proceeding to the next phase in the sequence.

68. Standard

A formal agreement documenting generally accepted specifications or criteria for products, processes, procedures, policies, systems, and/or personnel.

69. Support Services

The activity required for successful execution of a product, program or process. Support services typically include troubleshooting, installation assistance and basic usability assistance, installation of product updates, and support for custom application or infrastructure software.

70. Technology Refresh

The periodic replacement of Commercial Off-The-Shelf (COTS) components; e.g. processors, displays, computer operating systems, commercially available software within larger DoD systems to assure continued supportability of that system through an indefinite service life.

71. Technical Standard

Technical standards document specific technical methodologies and practices to design and implement.

72. Test and Evaluation (T&E)

T&E is a process by which a system or components are tested and results analyzed to provide performance related information. This information has many uses, including risk identification and mitigation as well as providing empirical data to validate models and simulations. T&E enables an assessment of the attainment of technical performance, specifications, and system maturity to determine whether systems are operationally effective, suitable, and survivable for their intended use.

72.1. Automated Testing and Tools

Automated software testing is a process in which software tools execute pre-scripted tests on software before it is released into production.

Automated testing tools are capable of executing tests, reporting outcomes and comparing results with earlier test runs. Tests carried out with automated tools can be run repeatedly, at any time of day.

72.2. Common T&E Database

A common database for all T&E information for the system under test. A properly validated common T&E database affords more continuity and uniformity in the T&E data. Multi-

disciplinary teams looking at the same T&E data will be more innovative at solving problems than separate organizations working alone. The common T&E database will help reduce duplication of effort, fill voids, remove unnecessary barriers, promote the efficient continuum of testing among integrated test teams, and identify better solutions earlier.

72.3. Evaluation (Evaluate)

Evaluation denotes the process whereby data are logically assembled, analyzed, and compared to expected performance to aid in systematic decision making. It may involve review and analysis of qualitative or quantitative data obtained from design reviews, hardware inspections, modeling and simulation (M&S), hardware and software testing, metrics review, and operational usage of equipment.

72.4. Integration Testing

Integrated Testing is a process intended to result in resource efficiencies (time, money, people, and assets) and an enhanced data set for separate evaluations. The goal of integrated testing is to conduct a seamless test program that produces credible qualitative and quantitative data useful to all evaluators, and to address developmental, life-cycle, and Critical Operational Issues (COI). Integrated testing allows for the collaborative planning of test events, where a single test point or mission can provide data to satisfy multiple objectives, without compromising the test objectives of participating test organizations. Integrated testing focuses the entire test program (contractor test, Government Developmental Test & Evaluation and Operational Test & Evaluation) on designing, developing, and producing a comprehensive plan that coordinates all test activities to support evaluation results for decision makers at required decision reviews.

Integrated testing must be embedded in the Test and Evaluation (T&E) Strategy. There is no single implementation of integrated testing that will be optimum for all programs, but planning and conducting the test program in a collaborative manner will result in a more effective and efficient test effort.

72.5. Test

Test denotes any program or procedure designed to obtain, verify, or provide data for the evaluation of any of the following:

a. Progress in accomplishing developmental objectives;
b. The performance, operational capability, and suitability of systems, subsystems, components, and equipment items; and
c. The vulnerability and lethality of systems, subsystems, components, and equipment items.

72.6. Testable

The attribute of being measurable and repeatable with available test instrumentation and resources. Note: Testability is a broader concept indicating whether T&E infrastructure capabilities are available and capable of measuring the parameter. The difference between testable and measurable may indicate a test limitation. Some requirements may be measurable

but not testable due to T&E infrastructure shortfalls, insufficient funding, safety, or statutory or regulatory prohibitions.

72.7. Validation

The process of evaluating a system or software component during, or at the end of, the development process to determine whether it satisfies specified requirements.

72.8. Verification

Confirms that a system element meets design-to or build-to specifications. Throughout the system's life cycle, design solutions at all levels of the physical architecture are verified through a cost-effective combination of analysis, examination, demonstration, and testing, all of which can be aided by modeling and simulation.

73. Tools

73.1. Quality Category

Quality analysis tools may be used to flag violations of programming rules, duplicated code and provide information about possible source code defects such as buffer overruns, logic errors, un-initialized memory, null pointer references or memory and resource leaks.

73.2. Security Category

Source code analysis tools, also referred to as Static Application Security Testing (SAST) Tools, are designed to analyze source code and/or compiled versions of code to help find security flaws. Such tools serve as aids for an analyst to help zero in on security-relevant portions of code so they can find flaws more efficiently.

73.3. Testing Category

Automated testing tools are capable of executing tests, reporting outcomes and comparing results with earlier test runs. Tests carried out with these tools can be run repeatedly, at any time of day. The method or process being used to implement automation is called a test automation framework.

74. Upgrade

(n) Something that improves the performance or quality of something else (such as computer hardware or software); something that has better performance or qualities than the existing item (hardware or software)

75. User Story

User stories originated with Extreme Programming (XP). Expressed in template form: As an (actor or role) I need to (action or function) so as to (result or benefit) and is verified when (acceptance criteria).

76. Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

77. Web Services

A request/response mechanism that allows a client to remotely access and modify data. Web services describes a standardized way of integrating web-based applications over an internet protocol backbone. Web services share business logic, data and processes through a programmatic interface across a network. Web services allow different applications from different sources to communicate with each other without time-consuming custom coding. Web services are not tied to any one operating system or programming language.