Glossary

A

ACL: ACL is an audit and data analysis tool. ACL provides powerful internal controls that identify and mitigate risk, protect profits, and accelerate performance.

AGILE: In this method of system development, the focus is to "Build Short and Build Often", i.e. each development effort is kept small.

Analytical CRM: Customer relationship management applications dealing with the analysis of customer data to provide information for improving business performance.

Application Program Interface (API): How one computer process (software) communicates with another. APIs may be standardized by industry agreement or government fiat, or proprietary to a specific application or vendor. The scope of the term API can vary based on its usage. It may refer to a single "call" by which one application can request information for another, the set of such calls for an application or the collection of all such application APIs used by an organization. In cloud environments, this is sometimes referred to as "Web API."

Application Server: A server that is used for storing applications. Users can access and use these server applications instead of loading the applications on their client machines. The application that the client runs is stored on the client. Requests are sent to the server for processing, and the results are returned to the client. In this way, little information is processed by the client, and nearly everything is done by the server.

Application Software Package: A set of prewritten, pre-coded application software programs that are commercially available for sale or lease.

Artificial Intelligence (AI): The efforts to develop computer based systems that can behave like humans, with the ability to learn languages, accomplish physical tasks, use a perceptual apparatus, and emulate human expertise and decision making.

Assurance Services: An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization. Examples may include financial, performance, compliance, system security, and due diligence engagements.

Asynchronous Transfer Mode (ATM): A networking technology that parcels information into 8-byte cells, allowing data to be transmitted between computers from different vendors at any speed.

Audit Hooks: Audit hooks are audit routines that flag suspicious transactions.

Audit Trail (or **audit log**): A security-relevant chronological record, set of records, or destination and source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event.

Authentication: The process of verifying the identity of a person or process within the

© The Institute of Chartered Accountants of India

guidelines of a specific authorization policy.

Automated Control: Controls implemented in a manner that they can work without any manual intervention.

B

Back-Office Processes: Supporting business functions such as accounting, finance, payroll, employee benefits, and IT that provide infrastructure for an organization's vision and create a platform for growth. Back-office processes are also referred to as "non-core" processes.

Bandwidth: The capacity of a communications channel as measured by the difference between the highest and lowest frequencies that can be transmitted by that channel.

BCP: A plan used by an enterprise to respond to disruption of critical business processes.

Blocking: A process preventing the transfer of a specified amount of funds or a specified quantity of a security.

Boundary Control: Controls implemented to restrict access to a system.

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).

Bugs: A software bug is an error, flaw, failure, or fault in a computer program or system that produces an incorrect or unexpected result, or causes it to behave in unintended ways.

Business Intelligence (BI): It refers to applications and technologies that are used to collect, provide access and analyze data and information about companies operations.

Business Process Management: Methodology for revising the enterprise's business processes to use business processes as fundamental building blocks of corporate information systems.

Business Process Modeling: Business process design means a structured task list / process list for a business

Business Process Outsourcing (BPO): A process of delegating the back-office processes or non-core business functions to a third-party service provider.

Business Process Reengineering: The radical redesign of business processes, combining steps to cut waste and eliminating repetitive, paper-intensive tasks in order to improve cost, quality, and service, and to maximize the benefits of information technology.

Business Processes: The unique ways in which enterprises coordinate and organize work activities, information, and knowledge to produce a product or service.

C

Cipher Text: Information generated by an encryption algorithm to protect the plaintext and that is unintelligible to the unauthorized reader.

© The Institute of Chartered Accountants of India

CIS: Continuous Intermittent Simulation is a module that is embedded in a data base management system, which examines all transactions that update the DBMS.

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

Compliance: Adherence to policies, plans, procedures, laws, regulations, contracts, or other requirements. Compliance refers to the systems and processes that ensure conformity with business rules, policy and regulations.

Computer Database: A representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network.

Computer Source Code: The listing of programs, computer commands, design and layout and program analysis of computer resource in any form.

Computer Virus: Any computer instruction, information, data or program that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a program, data or instruction is executed or some other event takes place in that computer resource.

Consulting Services: Advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve an organization's governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, and training.

Control Environment: The attitude and actions of the board and management regarding the importance of control within the organization. The control environment provides the discipline and structure for the achievement of the primary objectives of the system of internal control. The control environment includes the following elements: Integrity and ethical values, Management's philosophy and operating style, Organizational structure, Assignment of authority and responsibility, Human resource policies and practices and competence of personnel.

Control Processes: The policies, procedures (both manual and automated), and activities that are part of a control framework, designed and operated to ensure that risks are contained within the level that an organization is willing to accept.

Control: Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved. Control refers to the policies, procedures, practices and organization structure which are designed to provide reasonable

© The Institute of Chartered Accountants of India

assurance that business objectives are achieved and undesired events are prevented or detected and corrected.

Corporate Governance: The systems and processes, by which enterprises are directed, controlled and monitored.

Cryptography: The art of protecting information by transforming it (*encrypting* it) into an unreadable format, called cipher text. Only those who possess a secret *key* can decipher (or *decrypt*) the message into plain text.

Customer Relationship Management Systems: Information systems that track all the ways in which a company interacts with its customers and analyze these interactions to optimize revenue, profitability, customer satisfaction, and customer retention.

Customization: The modification of a software package to meet an enterprise's unique requirements without destroying the package software's integrity.

Cyber Forensic: An investigation method gathering digital evidences to be produced in court of law.

D

Dada Diddling: Changing data with malicious intent before or during input into the system.

Damage: To destroy, alter, delete, add, modify or re-arrange any computer resource by any means.

Data Mining: A process where data in a data warehouse is identified to discover key business trends and factors. It basically finds hidden patterns from data.

Data: These are the facts that are used by programs to produce useful information.

Database: This is a collection of logically related records or files.

DBA: A Database Administrator (short form DBA) is a person responsible for the installation, configuration, upgrade, administration, monitoring and maintenance of databases in an organization.

Development Tools: These are CASE tools. They are used to enhance the quality of system development efforts.

Digital Signature: Means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions.

E

E-business: It is the use of the internet and other networks and information technologies to support electronic commerce, enterprise communications and collaborations and web-enabled business processes both within an internetworked enterprise, and with its customers and business partners.

© The Institute of Chartered Accountants of India

E-commerce: The processes by which enterprises conduct business electronically with their customers and/or public at large using the Internet as the enabling technology.

EDI: Electronic Data Interchange (EDI) promotes a more efficient paperless environment.

Encryption: The process of taking an unencrypted message (plaintext), applying a mathematical function to it (Encryption algorithm with a key) and producing an cipher text.

End user: Anyone who uses an information system or the information it produces.

Enterprise Software: Set of integrated modules for applications such as sales and distribution, financial accounting, investment management, materials management, production planning, plant maintenance, and human resources that allow data to be used by multiple functions and business processes.

Enterprise Systems: Integrated enterprise-wide information systems that coordinate key internal processes of the firm.

Expert System: It is a knowledge-intensive program that solves a problem by capturing the expertise of a human in limited domains of knowledge and experience.

F

Firewall: A system or combination of systems that enforces a boundary between two or more networks, typically forming a barrier between a secure and an open environment such as the Internet.

Framework: Set of controls and/or guidance organized in categories, focused on a particular topic. It is a structure upon which to build strategy, achieve objectives and monitor performance.

Fraud: Any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage.

G

Governance of Enterprise IT (GEIT): Concerned with IT value delivery to the business and the mitigation of IT-related risks. This is enabled by the availability and management of adequate resources and the measurement of performance to monitor progress towards the desired goals.

Governance: The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives. Governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives. In most enterprises, overall

© The Institute of Chartered Accountants of India

governance is the responsibility of the board of directors under the leadership of the chairperson. Specific governance responsibilities may be delegated to special organizational structures at an appropriate level, particularly in larger, complex enterprises.

Grid Computing: Where workstations on the same network have their resources pooled in order to complete computing tasks to address a single problem. Grid is sometimes used synonymously with cloud computing.

H

Hash Total: A sum obtained by adding together numbers having different meanings; the sole purpose is to ensure the correct number of data have been read by the computer.

I

IDEA: IDEA is a generalized audit software.

Information System: It is considered as an arrangement of a number of elements that provides effective information for decision-making and/or control of some functionalities of an organization.

Information Technology Controls: Controls that support business management and governance as well as provide general and technical controls over information technology infrastructures such as applications, information, infrastructure, and people.

Information Technology Governance: Consists of the leadership, organizational structures, and processes that ensure that the enterprise's information technology supports the organization's strategies and objectives.

Information: It is data that have been put into a meaningful and useful content.

Input: It is the data flowing into the system from outside.

Internal Audit Activity: A department, division, team of consultants, or other practitioner(s) that provides independent, objective assurance and consulting services designed to add value and improve an organization's operations. The internal audit activity helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management and control processes.

Internet: It is a network of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies.

Intranet: It refers to a network inside an organization that uses internet technologies such as web browsers, servers etc. to provide an internet-like environment within enterprise for information sharing, communications, collaboration and the support of business processes.

ISMS: An **Information Security Management System** (ISMS) is a set of policies concerned with information security management or IT related risks. The main objective of information security management is to implement the appropriate measurements in order to eliminate or

© The Institute of Chartered Accountants of India

minimize the impact that various security related threats and vulnerabilities might have on an organization.

ITF(Integrated Test Facilities): A testing methodology in which test data are processed in production systems.

K

Key Pair: In an a symmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key.

Knowledge Management: The set of processes developed in an enterprise to create, gather, store, maintain, and disseminate the firm's knowledge.

M

Middleware: Software that sits between applications and operating systems, consisting of a set of services that enable interoperability in support of distributed architectures by passing data between applications. So, for example, the data in one database can be accessed through another database.

O

Output: It is the information flowing out of a system.

Operational Level or Lower Level Management: It is the lowest level in managerial hierarchy wherein the managers coordinate the work of others who are not themselves mangers.

P

Phishing: Phishing is an attack launched to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading/impersonification as a trustworthy entity in an electronic communication.

Piggybacking: Piggybacking refers to when a person tags along with another person who is authorized to gain entry into a restricted area, or pass a certain checkpoint. The act may be legal or illegal, authorized or unauthorized, depending on the circumstances.

Private Key: The key of a key pair used to create a digital signature;

Processing: It is the action of manipulating the input into a more useful form.

Program: It is a set of instructions that directs a computer to perform a particular task.

Public Key: The key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;

© The Institute of Chartered Accountants of India

R

RAD: Rapid Application Development is a method of system development. The key consideration is rapidity of development.

Return on Investment: This defines the return an entity shall earn on a particular investment (capital expenditure)

Risk Appetite: The level of risk that an organization is willing to accept.

Risk Management: A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives. It refers to the culture, processes and structures that are directed to the effective management of potential opportunities and adverse effects.

Risk: The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood. Risk is the potential for an event to occur that could have an effect on the Enterprise objectives or operations.

Routing: The method of routing traffic through split cable facilities or duplicate cable facilities.

S

SCARF: System Control Audit Review File is a special audit technique which uses embedded audit modules to continuously monitor transaction activity and collect data on transactions with special audit significance.

SDLC: A method of system development. The same also referred to as linear, waterfall, traditional approach to system development.

Service Level Agreement (SLA): SLAs define providers' technical performance standards in terms of service agreements. In the case of cloud computing, SLAs generally address the quality of service and security protections that providers offer. According to NIST's "Draft Cloud Computing Synopsis and Recommendations," most providers assure consumers of certain standards regarding service avail ability, remedies for failure to perform, data preservation, and legal care of subscriber information, but renounce obligation for scheduled outages, force majeure events, and unauthorized modification or disclosure of subscriber data, including service in interruptions caused by malicious activity. Typically, providers also reserve the right to change the terms and pricing of their SLAs with limited advanced notice. Subscribers are typically obligated to accept certain use policies, conform to software license terms, and provide timely payments.

Spoofing: Spoofing is the creation of TCP/IP packets using somebody else's IP address. Routers use the "destination IP" address in order to forward packets through the Internet, but ignore the "source IP" address. That address is only used by the destination machine when it responds back to the source.

SRS: System Requirements Specification Document; this document is like the religious book for SDLC. This document is the output of 'Requirements Analysis' phase.

© The Institute of Chartered Accountants of India

Steering Committee: An advisory committee usually made up of high level stakeholders and /or experts who provide guidance on key issues such as company policy and objectives, budgetary control, marketing strategy, resource allocation, and decision involving large expenditures.

Strategic level or Top level management: It is concerned with the developing of organizational mission, objectives and strategies.

Structured Query Language(SQL): The SQL used by both application programmers and end users in accessing relational Databases.

Subsystem: A subsystem is a part of a larger system.

System: A system is defined as an orderly arrangement of a set of interrelated and independent elements that operate collectively to accomplish some common purpose or goal.

T

Tactical level or middle level management: It lies in middle of management hierarchy where managers plan, organize, lead and control the activities of other managers.

Tally: It is an accounting Software, very user friendly even a person having the basic knowledge of accounts and computers can easily learn this package on his own.

V

Vandalism: To destroy or damage.

Virtual Enterprise: Enterprise using networks to link people, assets and ideas to create and distribute products and services without being limited to traditional enterprise boundaries or physical location.

Virtualisation: A way of making better use of available hardware resources by running multiple operating systems on one server as “virtual machines", and managing the virtualized software layer separately from the hardware. With its emphasis on decoupling software from hardware, virtualization is a step on the way to cloud computing. Virtualization cannot be thought of as true cloud computing, however, because it does not offer elastic scaling of resources or automated provisioning of new virtual machine instances.

VPN (Virtual Private Network): A secure private network that uses the public telecommunications infrastructure to transmit data.

© The Institute of Chartered Accountants of India