CGEIT® Glossary

Term	Definition
Accountability	The ability to map a given activity or event back to the responsible party
Architecture	Description of the fundamental underlying design of the components of the business system, or of one element of the business system (e.g., technology), the relationships among them, and the manner in which they support enterprise objectives
Asset	Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation
Assurance	Pursuant to an accountable relationship between two or more parties, an IT audit and assurance professional is engaged to issue a written communication expressing a conclusion about the subject matters for which the accountable party is responsible. Assurance refers to a number of related activities designed to provide the reader or user of the report with a level of assurance or comfort over the subject matter. Scope Note: Assurance engagements could include support for audited financial statements, reviews of controls, compliance with required standards and practices, and compliance with agreements, licenses, legislation and regulation.
Balanced scorecard (BSC)	Developed by Robert S. Kaplan and David P. Norton as a coherent set of performance measures organized into four categories that includes traditional financial measures, but adds customer, internal business process, and learning and growth perspectives
Benchmarking	A systematic approach to comparing enterprise performance against peers and competitors in an effort to learn the best ways of conducting business Scope Note: Examples include benchmarking of quality, logistic efficiency and various other metrics.
Benefit	In business, an outcome whose nature and value (expressed in various ways) are considered advantageous by an enterprise
Budget	Estimated cost and revenue amounts for a given range of periods and set of books Scope Note: There can be multiple budget versions for the same set of books.
Business balanced scorecard	A tool for managing organizational strategy that uses weighted measures for the areas of financial performance (lag) indicators, internal operations, customer measurements, learning and growth (lead) indicators, combined to rate the enterprise
Business case	Documentation of the rationale for making a business investment, used both to support a business decision on whether to proceed with the investment and as an operational tool to support management of the investment through its full economic life cycle
Business control	The policies, procedures, practices and organizational structures designed to provide reasonable assurance that the business objectives will be achieved and undesired events will be prevented or detected

Term	Definition
Business dependency assessment	A process of identifying resources critical to the operation of a business process
Business process	An inter-related set of cross-functional activities or events that result in the delivery of a specific product or service to a customer
Business process reengineering (BPR)	The thorough analysis and significant redesign of business processes and management systems to establish a better performing structure, more responsive to the customer base and market conditions, while yielding material cost savings
Business sponsor	The individual accountable for delivering the benefits and value of an IT-enabled business investment program to the enterprise
Capability	An aptitude, competency or resource that an enterprise may possess or require at an enterprise, business function or individual level that has the potential, or is required, to contribute to a business outcome and to create value
Capability Maturity Model (CMM)	1. Contains the essential elements of effective processes for one or more disciplines It also describes an evolutionary improvement path from ad hoc, immature processes to disciplined, mature processes with improved quality and effectiveness. 2. CMM for software, from the Software Engineering Institute (SEI), is a model used by many enterprises to identify best practices useful in helping them assess and increase the maturity of their software development processes Scope Note: CMM ranks software development enterprises according to a hierarchy of five process maturity levels. Each level ranks the development environment according to its capability of producing quality software. A set of standards is associated with each of the five levels. The standards for level one describe the most immature or chaotic processes and the standards for level five describe the most mature or quality processes. A maturity model that indicates the degree of reliability or dependency the business can place on a process achieving the desired goals or objectives A collection of instructions that an enterprise can follow to gain better control over its software development process
Capital expenditure/expense (CAPEX)	An expenditure that is recorded as an asset because it is expected to benefit more than the current period. The asset is then depreciated or amortized over the expected useful life of the asset.
Change management	A holistic and proactive approach to managing the transition from a current to a desired organizational state, focusing specifically on the critical human or "soft" elements of change Scope Note: Includes activities such as culture change (values, beliefs and attitudes), development of reward systems (measures and appropriate incentives), organizational design, stakeholder management, human resources (HR) policies and procedures, executive coaching, change leadership training, team building and communication planning and execution
Chief executive officer (CEO)	The highest ranking individual in an enterprise
Chief financial officer (CFO)	The individual primarily responsible for managing the financial risk of an enterprise

Term	Definition
Chief information officer (CIO)	The most senior official of the enterprise who is accountable for IT advocacy, aligning IT and business strategies, and planning, resourcing and managing the delivery of IT services, information and the deployment of associated human resources Scope Note: In some cases, the CIO role has been expanded to become the chief knowledge officer (CKO) who deals in knowledge, not just information. Also see chief technology officer (CTO).
Chief technology officer (CTO)	The individual who focuses on technical issues in an enterprise Scope Note: Often viewed as synonymous with chief information officer (CIO)
Combined Code on Corporate Governance	The consolidation in 1998 of the "Cadbury," "Greenbury" and "Hampel" Reports Scope Note: Named after the Committee Chairs, these reports were sponsored by the UK Financial Reporting Council, the London Stock Exchange, the Confederation of British Industry, the Institute of Directors, the Consultative Committee of Accountancy Bodies, the National Association of Pension Funds and the Association of British Insurers to address the financial aspects of corporate governance, directors' remuneration and the implementation of the Cadbury and Greenbury recommendations.
Competencies	The strengths of an enterprise or what it does well Scope Note: Can refer to the knowledge, skills and abilities of the assurance team or individuals conducting the work.
Contingency planning	Process of developing advance arrangements and procedures that enable an enterprise to respond to an event that could occur by chance or unforeseen circumstances.
Continuous improvement	The goals of continuous improvement (Kaizen) include the elimination of waste, defined as "activities that add cost, but do not add value;" just-in-time (JIT) delivery; production load leveling of amounts and types; standardized work; paced moving lines; and right-sized equipment Scope Note: A closer definition of the Japanese usage of Kaizen is "to take it apart and put it back together in a better way." What is taken apart is usually a process, system, product or service. Kaizen is a daily activity whose purpose goes beyond improvement. It is also a process that, when done correctly, humanizes the workplace, eliminates hard work (both mental and physical), and teaches people how to do rapid experiments using the scientific method and how to learn to see and eliminate waste in business processes.
Control framework	A set of fundamental controls that facilitates the discharge of business process owner responsibilities to prevent financial or information loss in an enterprise
Control Objectives for Enterprise Governance	A discussion document that sets out an "enterprise governance model" focusing strongly on both the enterprise business goals and the information technology enablers that facilitate good enterprise governance, published by the Information Systems Audit and Control Foundation in 1999.
Control risk	The risk that a material error exists that would not be prevented or detected on a timely basis by the system of internal controls (See Inherent risk)

Term	Definition
Corporate governance	The system by which enterprises are directed and controlled. The board of directors is responsible for the governance of their enterprise. It consists of the leadership and organizational structures and processes that ensure the enterprise sustains and extends strategies and objectives.
Critical success factor (CSF)	The most important issue or action for management to achieve control over and within its IT processes
Dashboard	A tool for setting expectations for an enterprise at each level of responsibility and continuous monitoring of the performance against set targets
Disaster recovery	Activities and programs designed to return the enterprise to an acceptable condition The ability to respond to an interruption in services by implementing a disaster recovery plan (DRP) to restore an enterprise's critical business functions
Disaster recovery plan (DRP)	A set of human, physical, technical and procedural resources to recover, within a defined time and cost, an activity interrupted by an emergency or disaster
Due diligence	The performance of those actions that are generally regarded as prudent, responsible and necessary to conduct a thorough and objective investigation, review and/or analysis
Enterprise	A group of individuals working together for a common purpose, typically within the context of an organizational form such as a corporation, public agency, charity or trust
Enterprise architecture (EA)	Description of the fundamental underlying design of the components of the business system, or of one element of the business system (e.g., technology), the relationships among them, and the manner in which they support the enterprise’s objectives
Enterprise architecture (EA) for IT	Description of the fundamental underlying design of the IT components of the business, the relationships among them, and the manner in which they support the enterprise’s objectives
Enterprise governance	A set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risk is managed appropriately and verifying that the enterprise’s resources are used responsibly
Good practice	A proven activity or process that has been successfully used by multiple enterprises and has been shown to produce reliable results
Impact analysis	A study to prioritize the criticality of information resources for the enterprise based on costs (or consequences) of adverse events In an impact analysis, threats to assets are identified and potential business losses determined for different time periods. This assessment is used to justify the extent of safeguards that are required and recovery time frames. This analysis is the basis for establishing the recovery strategy.
Impact assessment	A review of the possible consequences of a risk Scope Note: See also Impact analysis.
Information security	Ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity), and non-access when required (availability)

Term	Definition
Information security governance	The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risk is managed appropriately and verifying that the enterprise's resources are used responsibly
Information systems (IS)	The combination of strategic, managerial and operational activities involved in gathering, processing, storing, distributing and using information and its related technologies Scope Note: Information systems are distinct from information technology (IT) in that an information system has an IT component that interacts with the process components.
Information technology (IT)	The hardware, software, communication and other facilities used to input, store, process, transmit and output data in whatever form
IT governance	The responsibility of executives and the board of directors; consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the enterprise's strategies and objectives
IT governance framework	A model that integrates a set of guidelines, policies and methods that represent the organizational approach to IT governance Scope Note: Per COBIT, IT governance is the responsibility of the board of directors and executive management. It is an integral part of institutional governance and consists of the leadership and organizational structures and processes that ensure that the enterprise's IT sustains and extends the enterprise's strategy and objectives.
IT investment dashboard	A tool for setting expectations for an enterprise at each level and continuous monitoring of the performance against set targets for expenditures on, and returns from, IT-enabled investment projects in terms of business values
IT steering committee	An executive-management-level committee that assists in the delivery of the IT strategy, oversees day-to-day management of IT service delivery and IT projects, and focuses on implementation aspects
IT strategic plan	A long-term plan (i.e., three- to five-year horizon) in which business and IT management cooperatively describe how IT resources will contribute to the enterprise's strategic objectives (goals)
IT strategy committee	A committee at the level of the board of directors to ensure that the board is involved in major IT matters and decisions Scope Note: The committee is primarily accountable for managing the portfolios of IT-enabled investments, IT services and other IT resources. The committee is the owner of the portfolio.
IT tactical plan	A medium-term plan (i.e., six- to 18-month horizon) that translates the IT strategic plan direction into required initiatives, resource requirements and ways in which resources and benefits will be monitored and managed
Key goal indicator (KGI)	A measure that tells management, after the fact, whether an IT process has achieved its business requirements; usually expressed in terms of information criteria
Key management practice	Management practices that are required to successfully execute business processes
Key performance indicator (KPI)	A measure that determines how well the process is performing in enabling the goal to be reached Scope Note: A lead indicator of whether a goal will likely be reached, and a good indicator of capabilities, practices and skills. It measures an activity goal, which is an action that the process owner must take to achieve effective process performance.

Term	Definition
Key risk indicator (KRI)	A subset of risk indicators that are highly relevant and possess a high probability of predicting or indicating important risk Scope Note: See also Risk Indicator.
Maturity	In business, indicates the degree of reliability or dependency that the business can place on a process achieving the desired goals or objectives
Maturity model	 Scope Note: See Capability Maturity Model (CMM).
Metric	A quantifiable entity that allows the measurement of the achievement of a process goal Scope Note: Metrics should be SMART--specific, measurable, actionable, relevant and timely. Complete metric guidance defines the unit used, measurement frequency, ideal target value (if appropriate) and also the procedure to carry out the measurement and the procedure for the interpretation of the assessment.
Net present value (NPV)	Calculated by using an after-tax discount rate of an investment and a series of expected incremental cash outflows (the initial investment and operational costs) and cash inflows (cost savings or revenues) that occur at regular periods during the life cycle of the investment Scope Note: To arrive at a fair NPV calculation, cash inflows accrued by the business up to about five years after project deployment also should be taken into account.
Net return	The revenue that a project or business makes after tax and other deductions; often also classified as net profit
Outcome measure	Represents the consequences of actions previously taken; often referred to as a lag indicator Scope Note: Outcome measure frequently focuses on results at the end of a time period and characterize historic performance. They are also referred to as a key goal indicator (KGI) and used to indicate whether goals have been met. These can be measured only after the fact and, therefore, are called "lag indicators."
Payback period	The length of time needed to recoup the cost of capital investment Scope Note: Financial amounts in the payback formula are not discounted. Note that the payback period does not take into account cash flows after the payback period and therefore is not a measure of the profitability of an investment project. The scope of the internal rate of return (IRR), net present value (NPV) and payback period is the useful economic life of the project up to a maximum of five years.
Performance	In IT, the actual implementation or achievement of a process

Term	Definition
Performance driver	A measure that is considered the "driver" of a lag indicator It can be measured before the outcome is clear and, therefore, is called a "lead indicator." Scope Note: There is an assumed relationship between the two that suggests that improved performance in a leading indicator will drive better performance in the lagging indicator. They are also referred to as key performance indicators (KPIs) and are used to indicate whether goals are likely to be met.
Performance indicators	A set of metrics designed to measure the extent to which performance objectives are being achieved on an on-going basis Scope Note: Performance indicators can include service level agreements (SLAs), critical success factors (CSFs), customer satisfaction ratings, internal or external benchmarks, industry best practices and international standards.
Performance management	In IT, the ability to manage any type of measurement, including employee, team, process, operational or financial measurements The term connotes closed-loop control and regular monitoring of the measurement.
Performance testing	Comparing the system's performance to other equivalent systems, using well-defined benchmarks
Portfolio	A grouping of "objects of interest" (investment programs, IT services, IT projects, other IT assets or resources) managed and monitored to optimize business value (The investment portfolio is of primary interest to Val IT. IT service, project, asset and other resource portfolios are of primary interest to COBIT.)
Program	A structured grouping of interdependent projects that is both necessary and sufficient to achieve a desired business outcome and create value These projects could include, but are not limited to, changes in the nature of the business, business processes and the work performed by people as well as the competencies required to carry out the work, the enabling technology, and the organizational structure.
Project	A structured set of activities concerned with delivering a defined capability (that is necessary but not sufficient, to achieve a required business outcome) to the enterprise based on an agreed-on schedule and budget
Project portfolio	The set of projects owned by a company Scope Note: It usually includes the main guidelines relative to each project, including objectives, costs, time lines and other information specific to the project.
Quality assurance (QA)	A planned and systematic pattern of all actions necessary to provide adequate confidence that an item or product conforms to established technical requirements. (ISO/IEC 24765)
RACI chart	Illustrates who is Responsible, Accountable, Consulted and Informed within an organizational framework

Term	Definition
Reengineering	A process involving the extraction of components from existing systems and restructuring these components to develop new systems or to enhance the efficiency of existing systems Scope Note: Existing software systems can be modernized to prolong their functionality. An example is a software code translator that can take an existing hierarchical database system and transpose it to a relational database system. Computer-aided software engineering (CASE) includes a source code reengineering feature.
Reputation risk	The current and prospective effect on earnings and capital arising from negative public opinion Scope Note: Reputation risk affects a bank's ability to establish new relationships or services, or to continue servicing existing relationships. It may expose the bank to litigation, financial loss or a decline in its customer base. A bank's reputation can be damaged by Internet banking services that are executed poorly or otherwise alienate customers and the public. An Internet bank has a greater reputation risk as compared to a traditional brick-and-mortar bank, because it is easier for its customers to leave and go to a different Internet bank and since it cannot discuss any problems in person with the customer.
Return on investment (ROI)	A measure of operating performance and efficiency, computed in its simplest form by dividing net income by the total investment over the period being considered
Risk	The combination of the probability of an event and its consequence. (ISO/IEC 73)
Risk analysis	1. A process by which frequency and magnitude of IT risk scenarios are estimated 2. The initial steps of risk management: analyzing the value of assets to the business, identifying threats to those assets and evaluating how vulnerable each asset is to those threats Scope Note: It often involves an evaluation of the probable frequency of a particular event, as well as the probable impact of that event.
Risk appetite	The amount of risk, on a broad level, that an entity is willing to accept in pursuit of its mission
Risk assessment	A process used to identify and evaluate risk and its potential effects Scope Note: Risk assessments are used to identify those items or areas that present the highest risk, vulnerability or exposure to the enterprise for inclusion in the IS annual audit plan. Risk assessments are also used to manage the project delivery and project benefit risk.

Term	Definition
Risk management	1. The coordinated activities to direct and control an enterprise with regard to risk Scope Note: In the International Standard, the term "control" is used as a synonym for "measure." (ISO/IEC Guide 73:2002) 2. One of the governance objectives. Entails recognizing risk; assessing the impact and likelihood of that risk; and developing strategies, such as avoiding the risk, reducing the negative effect of the risk and/or transferring the risk, to manage it within the context of the enterprise's risk appetite. Scope Note: COBIT 5 perspective
Risk mitigation	The management of risk through the use of countermeasures and controls
Risk tolerance	The acceptable level of variation that management is willing to allow for any particular risk as the enterprise pursues its objectives
Risk transfer	The process of assigning risk to another enterprise, usually through the purchase of an insurance policy or by outsourcing the service Scope Note: Also known as risk sharing
Risk treatment	The process of selection and implementation of measures to modify risk (ISO/IEC Guide 73:2002)
Segregation/separation of duties (SoD)	A basic internal control that prevents or detects errors and irregularities by assigning to separate individuals the responsibility for initiating and recording transactions and for the custody of assets Scope Note: Segregation/separation of duties is commonly used in large IT organizations so that no single person is in a position to introduce fraudulent or malicious code without detection.
Service level agreement (SLA)	An agreement, preferably documented, between a service provider and the customer(s)/user(s) that defines minimum performance targets for a service and how they will be measured
Standard	A mandatory requirement, code of practice or specification approved by a recognized external standards organization, such as International Organization for Standardization (ISO)
Strategic planning	The process of deciding on the enterprise's objectives, on changes in these objectives, and the policies to govern their acquisition and use
Strengths, weaknesses, opportunities and threats (SWOT)	A combination of an organizational audit listing the enterprise's strengths and weaknesses and an environmental scan or analysis of external opportunities and threats
Threat	Anything (e.g., object, substance, human) that is capable of acting against an asset in a manner that can result in harm Scope Note: A potential cause of an unwanted incident (ISO/IEC 13335)
Threat event	Any event during which a threat element/actor acts against an asset in a manner that has the potential to directly result in harm

Term	Definition
Transparency	Refers to an enterprise's openness about its activities and is based on the following concepts: - How the mechanism functions is clear to those who are affected by or want to challenge governance decisions. - A common vocabulary has been established. - Relevant information is readily available. Scope Note: Transparency and stakeholder trust are directly related; the more transparency in the governance process, the more confidence in the governance.
Value	The relative worth or importance of an investment for an enterprise, as perceived by its key stakeholders, expressed as total life cycle benefits net of related costs, adjusted for risk and (in the case of financial value) the time value of money
Vulnerability	A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events
Vulnerability analysis	A process of identifying and classifying vulnerabilities