

## CGEIT GLOSSARY 1 June 2008

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 the organization's objectives.
Asset	Something of either tangible or intangible value worth protecting including people, systems, infrastructure, finances and reputation.
Assurance	An objective examination of evidence for the purpose of providing an assessment on risk management, control or governance processes for the organization.  Scope Note: Examples may include financial, performance, compliance and system security engagements.
Balanced Scorecard	The balanced scorecard, developed by Robert S. Kaplan and David P. Norton, is a coherent set of performance measures organized into four categories. It includes traditional financial measures, but adds customer, internal business process, and learning and growth perspectives.
Benchmarking	A systematic approach to comparing an organization's performance against peers and competitors in an effort to learn the best ways of conducting business.  Scope Note: Examples include: benchmarking of quality, logistical efficiency and various other metrics.
Benefit	In business, an outcome whose nature and value (expressed in various ways) are considered advantageous by an organization.
Best Practice	A proven activity or process that has been successfully used by multiple organizations.
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 which uses weighted measures for the areas of financial performance (lag) indicators, internal operations, customer measurements, learning and growth (lead) indicators combined to rate the organization.
Business Case	Documentation of the rationale for making a business investment, used both to support a business decision on whether to proceed or not with the investment and as an operational tool to support management of the investment through its full economic life cycle.
Business Controls	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.
Business Dependency Assessment	A process of identifying resources critical to the operation of a business process.

Term	Definition
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 organization.
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 creating value.
Capability Maturity Model (CMM)	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.
Capital Expenditure	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.
Capital Expense	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	<p>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.</p> <p>Scope Note: Change management includes activities such as culture change (values, beliefs and attitudes), development of reward systems (measures and appropriate incentives), organizational design, stakeholder management, human resource policies and procedures, executive coaching, change leadership training, team building and communications planning and execution.</p>
Chief Executive Officer (CEO)	Chief executive officer is the highest ranking individual in an organization.
Chief Financial Officer (CFO)	Chief financial officer is the individual primarily responsible for managing the financial risks of an organization.
Chief Technology Officer (CTO)	<p>The individual who focuses on technical issues in an organization.</p> <p>Scope Note: The title CTO is often viewed as synonymous with Chief Information Officer.</p>
Combined Code on Corporate Governance	<p>The consolidation in 1998 of the "Cadbury," "Greenbury" and "Hampel" Reports.</p> <p>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.</p>
Competencies	The strengths of an organization, what it does well.
Contingency Planning	Process of developing advance arrangements and procedures that enable an organization to respond to an event that could occur by chance or unforeseen circumstances.

Term	Definition
Continuous Improvement	<p>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 delivery; production load leveling of amounts and types; standardized work; paced moving lines; right-sized equipment.</p> <p>Scope Note: A closer definition of the Japanese usage of Kaizen is "to take it apart and put 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.</p>
Control Framework	A set of fundamental controls that facilitates the discharge of business process owner responsibilities to prevent financial or information loss in an organization.
Control Objectives for Enterprise Governance	A discussion document which sets out an "Enterprise Governance Model" focusing strongly on both the enterprise business goals and the information technology enablers which 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 also Inherent Risk)
Corporate Security Officer (CSO)	Responsible for coordinating the planning, development, implementation, maintenance and monitoring of the information security program.
Critical Success Factors (CSFs)	Critical success factor; the most important issues or actions for management to achieve control over and within its IT processes.
Dashboard	A tool for setting expectations for an organization at each level of responsibility and continuous monitoring of the performance against set targets.
Disaster Recovery	Activities and programs designed to return the organization to an acceptable condition. The ability to respond to an interruption in services by implementing a disaster recovery plan to restore an organization's critical business functions.
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	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 organization's objectives.
Enterprise Architecture 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 organization's objectives.
Impact Analysis	An impact analysis is a study to prioritize the criticality of information resources for the organization 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.

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 risks are managed appropriately and verifying that the enterprise's resources are used responsibly.
Information Technology (IT)	The hardware, software, communications and other facilities used to input, store, process, transmit and output data in whatever form.
IT Governance Framework	<p>A model that integrates a set of guidelines, policies and methods that represent the organizational approach to the IT governance.</p> <p>Scope Note: Per COBIT 4.0, 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 organization's IT sustains and extends the organization's strategy and objectives.</p>
IT Investment Dashboard	A tool for setting expectations for an organization 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 the executive 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	<p>Committee at the level of the board of directors to ensure the board is involved in major IT matters/decisions.</p> <p>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.</p>
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 Indicators (KGIs)	Key goal indicator; measures that tell management, after the fact, whether an IT process has achieved its business requirements, usually expressed in terms of information criteria.
Key Management Practices	Those management practices required to successfully execute business processes.
Key Performance Indicators (KPIs)	<p>Measures that determine how well the process is performing in enabling the goal to be reached.</p> <p>Scope Note: KPIs are lead indicators of whether a goal will likely be reached, and are good indicators of capabilities, practices and skills. They measure the activity goals, which are the actions the process owner must take to achieve effective process performance.</p>
Maturity	In business, indicates the degree of reliability or dependency the business can place on a process achieving the desired goals or objectives.

Term	Definition
Maturity Model	<p>The Capability Maturity Model (CMM) for Software (CMM), from the Software Engineering Institute (SEI), is a model used by many organizations to identify best practices useful in helping them assess and increase the maturity of their software development processes.</p> <p>Scope Note: The CMM ranks software development organizations 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. 1) A model that indicates the degree of reliability or dependency the business can place on a process achieving the desired goals or objectives (2) A collection of instructions an organization can follow to gain better control over its software development process.</p>
Metric	<p>Specific descriptions of how a quantitative and periodic assessment of performance is to be measured.</p> <p>Scope Note: A complete metric defines the unit used, frequency, ideal target value, the procedure to carry out the measurement and the procedure for the interpretation of the assessment.</p>
Net Present Value (NPV)	<p>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.</p> <p>Scope Note: To arrive at a fair NPV calculation, cash inflows accrued by the business up to about five years after project deployment should be taken into account as well.</p>
Net Return	<p>The revenue after tax and other deductions that a project or business makes. Often also classified as net profit.</p>
Outcome Measures	<p>Represent the consequences of actions previously taken and are often referred to as lag indicators.</p> <p>Scope Note: Outcome measures frequently focus on results at the end of a time period and characterize historical performance. They are also referred to as key goal indicators (KGIs) and are used to indicate whether goals have been met. These can be measured only after the fact and, therefore, are called 'lag indicators'.</p>
Payback Period	<p>The length of time needed to recoup the cost of capital investment.</p> <p>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 is therefore not a measure of the profitability of an investment project. The scope of the IRR, NPV and payback period is the useful economic life of the project up to a maximum of five years.</p>
Performance	<p>In IT, the actual implementation or achievement of a process.</p>
Performance Drivers	<p>Measures that are considered the 'drivers' of lag indicators. They can be measured before the outcome is clear and, therefore, are called 'lead indicators'.</p> <p>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.</p>

Term	Definition
Performance Indicators	<p>A set of metrics designed to measure the extent to which performance objectives are being achieved on an on-going basis.</p> <p>Scope Note: Performance indicators can include service level agreements, critical success factors, customer satisfaction ratings, internal or external benchmarks, industry best practices and international standards.</p>
Performance Management	<p>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.</p>
Performance Testing	<p>Comparing the system's performance to other equivalent systems using well defined benchmarks.</p>
Portfolio	<p>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. T service, project, asset and other resource portfolios are of primary interest to COBIT).</p>
Program	<p>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 not be limited to, changes in the nature of the business, business processes, the work performed by people, as well as the competencies required to carry out the work, enabling technology, and organizational structure.</p>
Project	<p>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-upon schedule and budget.</p>
Project Portfolio	<p>The set of projects owned by a company.</p> <p>Scope Note: A project portfolio usually includes the main guidelines relative to each project including objectives, costs, timelines and other information specific to the project.</p>
Quality Assurance (QA)	<p>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)</p>
RACI Chart	<p>Illustrates who is responsible, accountable, consulted and informed within an organizational framework.</p>
Reengineering	<p>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.</p> <p>Scope Note: Existing software systems can be modernized to prolong their functionality. An example of this is a software code translator that can take an existing hierarchical database system and transpose it to a relational database system. CASE includes a source code reengineering feature.</p>
Reputation Risk	<p>The current and prospective effect on earnings and capital arising from negative public opinion.</p> <p>Scope Note: Reputation risk affects the bank's ability to establish new relationships or services, or 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, since it is easier for its customers to leave and go to a different Internet bank and since it cannot discuss any problems with the customer in person.</p>

Term	Definition
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/IEC73)
Risk Analysis	<p>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.</p> <p>Scope Note: Risk analysis often involves an evaluation of the probable frequency of a particular event, as well as the probable impact of such event.</p>
Risk Assessment	<p>A process used to identify and evaluate risks and their potential effects.</p> <p>Scope Note: Risk assessment includes assessing the critical functions necessary for an organization to continue business operations, defining the controls in place to reduce organization exposure and evaluating the cost for such controls. Risk analysis often involves an evaluation of the probabilities of a particular event.</p>
Risk Mitigation	The management of risk through the use of countermeasures and controls.
Risk Transfer	The process of assigning risk to another organization, usually through the purchase of an insurance policy or outsourcing the service.
Risk Treatment	The process of selection and implementation of measures to modify risk [ISO/IEC Guide 73:2002].
Segregation/Separation of Duties	<p>A basic internal control that prevents or detects errors and irregularities by assigning to separate individuals responsibility for initiating and recording transactions and custody of assets to separate individuals.</p> <p>Scope Note: Segregation and 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.</p>
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 ISO.
Strategic Planning	The process of deciding on the organization'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 organization's strengths and weaknesses and an environmental scan or analysis of external opportunities and threats.
Value	The relative worth or importance of an investment for an organization, 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 Analysis	Process of identifying and classifying vulnerabilities.