Glossary of Terms and Definitions
Supporting Policies, Standards and Guidelines
For
Information Technology and Information Security

REFRENCES:

1. This glossary and list of acronyms includes ITIL® terminology that may be freely downloaded. ITIL® is a Registered Trade Mark, and a Registered Community Trade Mark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office. ITIL® Glossaries/Acronyms © Crown Copyright Office of Government Commerce. Reproduced with the permission of the Controller of HMSO and the Office of Government Commerce. See http://www.get-best-practice.co.uk/glossaries.aspx
2. "*A Guide to the Project Management Body of Knowledge (PMBOK Guide)"*, Bolles, Dennis and Fahrenkrog, Steve. 2004. Third Edition. Newtown Square, PA: Project Management Institute. (ISBN: 1-930699-45-X). *www.pmi.org.*
3. "*Information Technology Resource Management Standard (Technology Management Glossary)*". Virginia Information Technologies Agency (VITA). 1/22/2008. State of Virginia. (Gov 2003-02.3). http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/GlossaryStandard.pdf
4. Software Engineering Institute (SEI), http://www.sei.cmu.edu/str/indexes/
5. General Accounting Office (GAO), http://www.gao.gov/special.pubs/bprag/bprgloss.htmand http://www.gao.gov/aac/auditingorganizations.htm
6. National Aeronautics and Space Administration (NASA), http://www.nasa.gov/centers/ivv/about/visionmission.html
7. The Cambridge International Dictionary of English, http://dictionary.cambridge.org/default.asp?dict=a
8. "*Enterprise Performance Life Cycle Management*", a Guideline published by GTAs Enterprise Project Management Office
9. TechTerms.com

Revision: January 2014

A

Access Control - The rules and deployment mechanisms which control physical and logical access to information systems

Access Management - The process responsible for allowing users to make use of IT Services, data or other assets. Access Management helps to protect the confidentiality, integrity and availability of assets by ensuring that only authorized Users are able to access or modify the assets. Access Management is sometimes referred to as Rights Management or Identity Management. (ITIL® V3, Service Operation)

Acceptance - Formal agreement that an IT Service, Process, Plan, or other Deliverable is complete, accurate, Reliable and meets its specified Requirements. Acceptance is usually preceded by Evaluation or Testing and is often required before proceeding to the next stage of a Project or Process.
See Service Acceptance Criteria

Acceptance Criteria (Project) – Those criteria, including performance requirements and essential conditions, which must be met before project deliverables are accepted (PMBOK 3RD EDITION)

Active Monitoring - Monitoring of a configuration item or an IT Service that uses automated regular checks to discover the current status. (ITIL® V3, Service Operation)

Activity
(1) (Project) An element of work performed during the course of a project. An activity normally has an expected duration, expected cost, and expected resource requirements. Activities are often subdivided into tasks
(2) (Service Operation) - A set of actions designed to achieve a particular result. Activities are usually defined as part of processes or plans, and are documented in procedures

Agency – Every state department, agency, board, bureau, commission, and authority including the judicial branch of Georgia's State government and the University System of Georgia

Agency Impact Rating - The level of risk that an agency poses to the State's enterprise and/or their constituency. Agencies are categorized based on the highest impact rating (high water mark) assigned to any operational/production system which should also be equal to the highest impact rating assigned to any application running on that system

Agency Project Request (APR) –
(1) A Project Concept Document (PCD) that is referred to as an Agency Project Request (APR) at State of Georgia Agencies. The APR specifies what the project should accomplish; it contains the business problem that initiated the project, and a preliminary cost structure to be used to solicit funding
(2) An approved APR begins the first process in the project life cycle, *Project Initiation,* at State of Georgia Agencies

Agreed Service Time - A synonym for Service Hours, commonly used in formal calculations of availability (ITIL® V3, Service Design)

Agreement - A document that describes a formal understanding between two or more parties. An Agreement is not legally binding, unless it forms part of a contract. (ITIL® V3)

Alert - A warning that a threshold has been reached, something has changed, or a failure has occurred. Alerts are often created and managed by system management tools and are managed by the Event Management Process. (ITIL® V3, Service Operation)

Analytical Modeling - A technique that uses mathematical models to predict the behavior of a configuration item or IT Service. Analytical models are commonly used in Capacity Management and Availability Management. (ITIL® V3**,** Service Strategy, Service Design, Continual Service Improvement)

Application or Application Software - Software that allows the business to achieve operational goals and is designed to help people perform a certain type of work. An application thus differs from an operating system (which runs a computer), a utility (which performs maintenance or general-purpose chores), a programming language (with which computer programs are created) or a general purpose off the shelf software package which can be employed to perform a wide variety of functions (Microsoft Office). An application is often more than just the computer program but also includes the aggregation of the supporting components, such as component software (such as browsers, database software, printing software, etc), implementation, maintenance, support, training and manuals

Application FTE - Application FTE is an estimate of labor computed from "application" roles such as system admins, application developers/testers/trainers, database admins, user/floor help and people who support application processes like Quality Assurance

Application Management - The function responsible for managing applications throughout their lifecycle (ITIL® V3, Service Design, Service Operation)

Application Portfolio - A database or structured document used to manage applications throughout their lifecycle. The Application Portfolio contains key attributes of all applications. The Application Portfolio is sometimes implemented as part of the Service Portfolio, or as part of the Configuration Management System (ITIL® V3**,** Service Design)

Application Portfolio Management - Inventory applications, assessed by using a variety of criteria such as, 1) agreement with agency business strategies, initiatives or governmental priorities, 2) benefits and value to agency missions or business processes, 3) costs to maintain and operate, 4) ability to meet current and future agency business requirements, and 4) operational performance, technical status, and risks. Assets should be retired when they no longer are cost-justified or risk-acceptable

Application Program - Any data entry, update, query or report program that processes data for the user. It includes the generic productivity software (spreadsheets, word processors, database programs, etc.) as well as custom and packaged programs for payroll, billing, inventory and other accounting purposes

Application Program Interface - A formalized set of software calls and routines that can be referenced by an application program in order to access supporting system or network services (SEI)

Application Risk Categories - There are three risk categories for applications:
1) Critical - Agency goals would not be met if application did not function.
2) Important - Agency could operate and meet most goals if the application did not function.
3) Supportive - Application supports only basic agency functions and is not necessary to achieve agency goals.

Application Security Plan - An application security plan is an application specific section of the system security plan

Application Service Provider (ASP) -
A computer-based service to customers over a network. The principle component for an ASP is that it separates the management and operations of an application system from the business function(s) which depend on it for their software system needs. Typically, multiple customers share the same application, running on the same operating system, on the same hardware, with the same data-storage mechanism. ASPs can allocate costs across multiple customers, within certain limits, starting with the computing platform, software licensing, support costs and leveraging common processes

One type of ASP is an Enterprise ASP which provides a range of business functions, such as an Enterprise Resource Planning (ERP) system. The advantages to this approach include:

- Software integration issues are easier to manage.
- Key software systems are kept up to date, available, and managed for performance.
- Improved regulatory compliance, reliability, availability, scalability and security of internal IT systems.
- A provider's service level agreement guarantees a certain level of service.
- Access to product and technology experts dedicated to available products.
- Reduction of internal IT costs to a predictable annual or monthly fee.
- Redeploying IT staff and tools to focus on strategic technology projects that impact the enterprise's bottom line.

Some inherent disadvantages include:

- There is less flexibility and adaptability across multiple customers creating a need to agree on common and standard processes and procedures.
- The client may rely on the provider to provide a critical business function, thus limiting their control of that function and instead relying on the provider.

Application Sizing - The activity responsible for understanding the resource requirements needed to support a new application, or a major change to an existing application. Application sizing helps to ensure that the IT Service can meet its agreed Service Level Targets for Capacity and Performance (ITIL® V3, Service Design)

Approve - To accept as satisfactory. Approval implies that the item approved has the endorsement of the approving entity. The approval may still require confirmation by another party as in levels of approval. In management use, the important distinction is between approved and authorized. See authorization.

Approval / Authority to Operate - An authorization granted by a responsible executive (Agency Head, CIO, Business Owner or other) to put an information system into production based on his/her acknowledgement and acceptance of system risks

Architecture - The structure of a system or IT Service, including the relationships of components to each other and to the environment they are in. Architecture also includes the standards and guidelines which guide the design and evolution of the system. (ITIL® V3, Service Design)

Architectural design (Hardware and Software) - The process of defining a collection of hardware and software components and their interfaces to establish the framework for the development of a computer system (SEI)

Assembly - A configuration item that is made up from a number of other CIs. For example a server CI may contain CIs for CPUs, disks, memory etc.; an IT Service CI may contain many hardware, software and other CIs. (ITIL® V3, Service Transition)

Asset - Any resource or capability. Assets of a service provider include anything that could contribute to the delivery of a service. Assets can be one of the following types: Management, Organization, Process, Knowledge, People, Information, Applications, Infrastructure, and Financial Capital. (ITIL® V3, Service Strategy)

Asset Management - Asset Management is the process responsible for tracking and reporting the value and ownership of financial assets throughout their lifecycle. Asset Management is part of an overall Service Asset and Configuration Management Process (ITIL® V3, Service Transition)

Assumptions – Factors that, for planning purposes, are considered to be true, real, or certain without proof or demonstration

Attribute - A piece of information about a Configuration Item. Examples are name, location, Version number, and Cost. Attributes of CIs are recorded in the Configuration Management Database (CMDB). (ITIL® V3, Service Transition)

Automatic Call Distribution (ACD) - Use of information technology to direct an incoming telephone call to the most appropriate person in the shortest possible time. ACD is sometimes called Automated Call Distribution. (ITIL® V3, Service Operation)

Authorization and need-to-know is above and beyond the administrative approval needed to access sensitive information. In addition to having the formal approval to access information, individuals must also have system authorization and a need, based on their job functions or role to access the information. (Example: GTA system administrators have administrative approval for privileged access to the GTA intranet, however, based on their job functions they are not authorized nor do they have a need-to-know the information contained in personnel files)

Authorization –

(1) The power granted by management to specified individuals allowing them to approve transactions, procedures, or total systems.
(2) The formal administrative approval required for an individual to gain access to a facility, system, or other information asset.

Authentication

(1) A process that establishes origin of information or determines an entity's identity.
(2) A process of attempting to verify the digital identity of system users or processes.
(3) Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system [FIPS 200 and NIST Special Publications 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations"]. Electronic authentication is the process of establishing confidence in user identities electronically presented to an information system [NIST Special Publication 800-63, "Electronic Authentication Guideline"]

Availability - Ability of a configuration item or IT Service to perform its agreed function when required. Availability is determined by Reliability, Maintainability, Serviceability, Performance, and Security. Availability is usually calculated as a percentage. This calculation is often based on Agreed Service Time and Downtime. It is best practice to calculate Availability using measurements of the business output of the IT Service (ITIL® V3, Service Design

Availability Management - The process responsible for defining, analyzing, planning, measuring and improving all aspects of the availability of IT Services. Availability Management is responsible for ensuring that Infrastructure, processes, tools, roles etc. are appropriate for the agreed Service Level Targets for Availability (ITIL® V3, Service Design)

Availability Management Information System (AMIS) - A virtual repository of all Availability Management data, usually stored in multiple physical locations (ITIL® V3, Service Design)

Availability Plan - A plan to ensure that existing and future availability requirements for IT Services can be provided cost effectively (ITIL® V3, Service Design)

B

Back Out Plan- Plan that specifies the processes required to restore a system to its original or earlier state, in the event of failed or aborted implementation. The plan includes detailed steps and techniques for uninstalling a new system, as well as reversing coding changes

Backup - Copying data to protect against loss of integrity or availability of the original (ITIL® V3, Service Design)

Balanced Scorecard - A management tool developed by Drs. Robert Kaplan (Harvard Business School) and David Norton. A Balanced Scorecard enables a strategy to be broken down into Key Performance Indicators. Performance against the KPIs is used to demonstrate how well the strategy is being achieved. A Balanced Scorecard has 4 major areas, each of which has a small number of KPIs. The same 4 areas are considered at different levels of detail throughout the organization (ITIL® V3**,** Continual Service Improvement)

Bar Chart - A graphic display of schedule-related information. In the typical bar chart, schedule activities or work breakdown structure components are listed down the left side of the chart, dates are shown across the top, and activity durations are shown as date-placed horizontal bars. (PMBOK 3RD EDITION)

Baseline -
(1) The approved time phased plan (for a project, a work breakdown structure component, a work package, or a schedule activity), plus or minus approved project scope, cost, schedule, and technical changes. Generally refers to the current baseline, but may refer to the original or some other baseline. Usually used with a modifier (e.g., cost baseline, schedule baseline, performance measurement baseline, technical baseline). (PMBOK 3RD EDITION)
(2) A Benchmark used as a reference point (ITIL® V3, Continual Service Improvement). For example:

- An IT Service Management Baseline can be used as a starting point to measure the effect of a Service Improvement Plan
- A Performance Baseline can be used to measure changes in performance over the lifetime of an IT Service
- A Configuration Management Baseline can be used to enable the IT Infrastructure to be restored to a known configuration if a change or release fails

Basis of Estimate (BOE) –
(1) A statement of the assumptions underlying the costs, activity durations, or other forecast items used for planning.
(2) A forecast budget that includes such statements.
(3) Factual information and objective factors upon which the estimate was found

Benchmark - The recorded state of something at a specific point in time. A Benchmark can be created for a configuration, a process, or any other set of data (ITIL® V3**,** Continual Service Improvement). For example, a benchmark can be used in:

- Continual Service Improvement, to establish the current state for managing improvements.
- Capacity Management, to document performance characteristics during normal operations.

Benchmarking - Comparing a benchmark with a baseline or with best practice. The term Benchmarking is also used to mean creating a series of benchmarks over time, and comparing the results to measure progress or improvement (ITIL® V3, Continual Service Improvement)

Best Practices - The processes, practices, or systems identified in public and private organizations that performed exceptionally well and are widely recognized as improving an organization's performance and efficiency in specific areas. Successfully identifying and applying best practices can reduce business expenses and improve organizational efficiency. ITIL is an example of Best Practice

Boundary Protection (or perimeter defense) – Tools and techniques used to manage, control and protect the security objectives of information stored, processed and transmitted within and between network boundaries; such as but not limited to controlled interfaces, intrusion detection, anti-virus, network forensic analysis, log monitoring

Budget - When unqualified, refers to an estimate of funds planned to cover a project or specified period

Budget At Completion (BAC) - The sum of all the budget values established for the work to be performed on a project or a work breakdown structure component or a schedule activity. (PMBOK 3RD EDITION)

Build –
(1) The activity of assembling a number of configuration items to create part of an IT Service.
(2) Refer to a release that is authorized for distribution - for example server build or laptop build.
(3) A major step in the EPLC. (ITIL® V3, Service Transition, and "Enterprise Performance Life Cycle Management" Guideline, published by GTAs Enterprise Project management Office)

Build Environment - A controlled environment where applications, IT Services and other Builds are assembled prior to being moved into a Test or Live Environment (ITIL® V3, Service Transition)

Business - An overall corporate entity or organization formed of a number of business units. In the context of IT Service Management, the term Business includes public sector and not-for-profit organizations, as well as companies. An IT Service Provider provides IT Services to a customer within a Business. The IT Service Provider may be part of the same Business as their Customer (Internal Service Provider), or part of another Business (External Service Provider). (ITIL® V3, Service Strategy)

Business Analyst- Someone who analyzes the existing or ideal organization and design of systems, including businesses, departments, and organizations. BA's will assess business models and their integration with technology

Business Capacity Management (BCM) - In the context of IT Service Management, Business Capacity Management is the activity responsible for understanding future business requirements for use in the Capacity Plan (ITIL® V3, Service Design)

Business Case - A structured proposal for business improvement that functions as a decision package for organizational decision-makers. A business case includes an analysis of business process performance and associated needs or problems, proposed alternative solutions, assumptions, constraints, and a risk-adjusted cost-benefit analysis. (GAO)

Business Continuity Management (BCM)
(1) The business process responsible for managing risks that could seriously impact the business. BCM safeguards the interests of key stakeholders, reputation, brand and value creating activities. The BCM Process involves reducing risks to an acceptable level and planning for the recovery of business processes should a disruption to the business occur. BCM sets the Objectives, Scope and Requirements for IT Service Continuity Management (ITIL® V3, Service Design)
(2) The act of anticipating incidents which will affect critical functions and processes for the organization and ensuring that the organization responds to any incident in a planned and rehearsed manner.

Business Continuity Plan (BCP)
(1) A plan defining and documenting the arrangements and procedures required to respond to an event that lasts for an unacceptable period of time and return to performing its critical business functions after an interruption.
(2) The documentation of a predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption.

Business Continuity Planner - A Business Continuity Planner is an individual in an agency with responsibilities within the Business Continuity Management program to coordinate the planning for and the implementation of recovery from unplanned business interruptions

Business Impact Analysis (BIA) - BIA is the activity in Business Continuity Management that identifies vital business functions and their dependencies. These dependencies may include suppliers, people, other Business Processes, IT Services etc. BIA defines the recovery requirements for IT Services. These requirements include Recovery Time Objectives, Recovery Point Objectives and minimum Service Level Targets for each IT Service (**ITIL® V3,** Service Strategy)

Business Objective - The objective of a business process, or of the business as a whole. Business objectives support the business vision, provide guidance for the IT Strategy, and are often supported by IT Services (ITIL® V3, Service Strategy)

Business Operations - The day-to-day execution, monitoring and management of business processes (ITIL® V3, Service Strategy)

Business Owner – The executive in charge of an organization, who serves as the primary customer and advocate for an IT project. The Business Owner is responsible for identifying the business needs and performance measures to be satisfied by an IT project; providing funding for the IT project; establishing and approving changes to cost, schedule and performance goals; and validating that the IT project initially meets business requirements and continues to meet business requirements. The Business Owner is responsible and accountable for ensuring the technology investment meets the business and regulatory requirements. The Stage Gate Review process is the Business Owner's mechanism to ensure the viability of the investment and the compliance with agency, state and federal laws and regulations.

Business Perspective - An understanding of the service provider and IT Services from the point of view of the business, and an understanding of the business from the point of view of the service provider (ITIL® V3, Continual Service Improvement)

Business Process –

(1) A Business Process is a set of linked activities that take an input and transform it to create an output. Ideally, the transformation that occurs in the process should add value to the input and create an output that is more useful and effective to the recipient either upstream or downstream. (Johansson et (1993).
(2) A process that is owned and carried out by the business. A business process contributes to the delivery of a product or device to a business customer. For example, a retailer may have a purchasing process which helps to deliver services to their business customers. Many business processes rely on IT Services (ITIL® V3, Service Strategy)

Business Relationship Management - The process or function responsible for maintaining a relationship with the business. BRM usually includes:

- Managing personal relationships with business managers
- Providing input to service portfolio management
- Ensuring that the IT Service Provider is satisfying the business needs of the customers

This Process has strong links with Service Level Management (ITIL® V3**,** Service Strategy)

Business Requirements - The critical activities of an enterprise that must be performed to meet the organizational objective(s) while remaining solution independent. These requirements focus on what is required, rather than on how to achieve it, which is usually specified in the system or functional requirements.

Business Service - (ITIL® V3, Service Strategy)
(1) An IT Service that directly supports a business process, as opposed to an infrastructure service

(2) A service that is delivered to business customers by business units. For example, delivery of financial services to customers of a bank, or goods to the customers of a retail store. Successful delivery of business services often depends on one or more IT Services

Business Unit - A segment of the business which has its own plans, metrics, income and costs. Each business unit owns assets and uses these to create value for customers in the form of goods and services (ITIL® V3, Service Strategy)

Business Vision - A description of what senior management wants to achieve with the organization in the future. A business vision usually addresses a medium to long-term period and is expressed in terms of a series of objectives. (GAO)

C

Calendaring and scheduling tools are included in packages like Now Up-to-Date & Contact Novell GroupWise, Netscape Communicator, Contact Office and Microsoft Exchange. They automatically check the electronic calendar of team members for open time slots, propose alternative meeting times, schedule team meetings or appointments and notify/remind participants by email.

Calendar Unit -The smallest unit of time used in scheduling the project. Calendar units are generally in hours, days, or weeks, but can also be in quarter years, months, shifts, are even in minutes. (PMBOK 3RD EDITION)

Call Center - An organization or business unit which handles large numbers of incoming and outgoing telephone calls (ITIL® V3, Service Operation)

Call Type - A category that is used to distinguish incoming requests to a service desk. Common call types are Incident, Service Request and Complaint (ITIL® V3, Service Operation)

Capability - The ability of an organization, person, process, application, configuration item or IT Service to carry out an activity. Capabilities are intangible assets of an Organization (ITIL® V3, Service Strategy)

Capacity - The maximum throughput that a configuration item or IT Service can deliver while meeting agreed Service Level Targets (ITIL® V3, Service Design)

Capacity Management - The process responsible for ensuring that the capacity of IT Services and the IT infrastructure is able to deliver agreed Service Level Targets in a cost effective and timely manner. Capacity Management considers all resources required to deliver the IT Service, and plans for short, medium and long term business requirements (ITIL® V3, Service Design)

Capacity Management Information System (CMIS) - A virtual repository of all capacity management data, usually stored in multiple physical locations (ITIL® V3, Service Design)

Capacity Plan - Capacity Plan is used to manage the resources required to deliver IT Services. The plan contains scenarios for different predictions of business demand, and costed options to deliver the agreed Service Level Targets. (ITIL® V3, Service Design)

Capacity Planning - The activity within Capacity Management responsible for creating a Capacity Plan (ITIL® V3, Service Design)

Category - A named group of things that have something in common. Categories are used to group similar things together. For example Cost Types are used to group similar types of cost. Incident Categories are used to group similar types of incidents, CI Types are used to group similar types of configuration items. (ITIL® V3)

Change - The addition, modification or removal of anything that could have an effect on IT Services. The scope should include all IT Services, configuration items, processes, documentation etc. (ITIL® V3, Service Transition)

Change Advisory Board (CAB) - A group of people that advises the Change Manager in the assessment, prioritization and scheduling of changes. This board is usually made up of representatives from all areas within the IT Service Provider, the business, and Third Parties such as suppliers (ITIL® V3, Service Transition)

Change Case - A technique used to predict the impact of proposed changes. Change cases use specific scenarios to clarify the scope of proposed changes and to help with cost benefit analysis (ITIL® V3, Service Operation)

Change Control - Identifying, documenting, approving or rejecting, and controlling changes to the project baselines. (PMBOK 3RD EDITION)

Change History - Information about all changes made to a configuration item during its life. Change History consists of all those change records that apply to the CI (ITIL® V3, Service Transition)

Change Management –

(1) The process responsible for controlling the lifecycle of all changes. The primary objective of Change Management is to enable beneficial changes to be made, with minimum disruption to IT Services (ITIL® V3, Service Transition)
(2) Change Management can relate to the activities surrounding the transition of people to a new/ enhanced system or process.
(3) The process of controlling modifications to hardware, software, firmware, and documentation to ensure that Information Resources are protected against improper modification before, during, and after system implementation. Changes include:
    - Any implementation of new functionality (including OS upgrades)
    - Any interruption of service (scheduled or unscheduled)
    - Any repair of existing functionality (including patch, virus and security updates)
    - Any removal of existing functionality
    - Maintenance routines
    - Hardware installations/upgrades

Change Model - A repeatable way of dealing with a particular category of change. A Change Model defines specific pre-defined steps that will be followed for a change of this category. Change Models may be very simple, with no requirement for approval (e.g. Password Reset) or may be very complex with many steps that require approval (e.g. major software release). (ITIL® V3, Service Transition)

Change Record - A record containing the details of a change. Each Change Record documents the lifecycle of a single change. A Change Record is created for every Request for Change that is received, even those that are subsequently rejected. Change Records should reference the configuration items that are affected by the change. Change Records are stored in the Configuration Management System. (ITIL® V3, Service Transition)

Change Request - Synonym for Request for Change

Change Schedule - A document that lists all approved changes and their planned implementation dates. A Change Schedule is sometimes called a Forward Schedule of Change, even though it also contains information about changes that have already been implemented (ITIL® V3, Service Transition)

Change Window - A regular, agreed time when changes or releases may be implemented with minimal impact on services. Change Windows are usually documented in SLAs. (ITIL® V3, Service Transition)

Charter - See Project Charter

CIO (Chief Information Officer) - The most senior executive in an organization responsible for the information technology and computer systems that support enterprise goals. He/she holds ultimate responsibility for the technology assets and security of information assets held by the agency.

CI Type - A category that is used to classify CIs. The CI Type identifies the required attributes and relationships for a configuration record. Common CI Types include: hardware, document, user etc. (ITIL® V3, Service Transition)

Client
(1) A generic term that means a customer, the business or a business customer. For example Client Manager may be used as a synonym for Account Manager.
(2) A computer that is used directly by a user, for example a PC, handheld computer, or workstation.
(3) The part of a client-server application that the user directly interfaces with, for example, an email Client.

Closed - The final status in the lifecycle of an incident, problem, change etc. When the status is closed, no further action is taken (ITIL® V3, Service Operation)

Closure - The act of changing the status of an incident, a problem, or a change to closed (ITIL® V3, Service Operation)

Commercial off the Shelf (COTS) - Application software or middleware that can be purchased from a Third Party.

Commodity – Commodity refers to individual products that can serve as end item. For example, Fax machines, copiers, scanners, and other items that can operate in a similar manner.

Communication Management - (PMBOK 3RD EDITION)
(1) The 7th of 9 PMI standard *Knowledge Areas*. The recommended processes ensure timely and appropriate generation, collection, dissemination, storage and ultimate disposition of project information. The recommended processes are: Communications Planning, Information Distribution, Performance Reporting, and Stakeholder Management.
(2) Includes managing the processes required to ensure timely and appropriate generation, collection, distribution, storage, retrieval, and ultimate disposition of project information.

Communication Software (Software Application Projects) - Software concerned with the representation, transfer, interpretation, and processing of data among computer systems or networks. The meaning assigned to the data must be preserved during these operations.

Compliance - Ensuring that a standard or set of guidelines is followed

Component - A general term that is used to mean one part of something more complex. For example, a computer system may be a component of an IT Service, an application may be a component of a release unit. Components that need to be managed should be configuration items (ITIL® V3)

Component Capacity Management (CCM) - The process responsible for understanding the capacity, utilization, and performance of configuration items. Data is collected, recorded and analyzed for use in the Capacity Plan (ITIL® V3, Service Design, Continual Service Improvement)

Component CI - A configuration item that is part of an assembly. For example, a CPU or Memory CI may be part of a Server CI (ITIL® V3, Service Transition)

Component Failure Impact Analysis (CFIA) - A technique that helps to identify the impact of CI failure on IT Services. A matrix is created with IT Services on one edge and CIs on the other to enables the identification of critical CIs that could cause the failure of multiple IT Services and of fragile IT Services that have multiple single points of failure (ITIL® V3, Service Design)

Computer Security Log Management - The processes for generating, transmitting, storing, analyzing and disposing of computer security log data

Concept – An exploration of a set of product or system ideas submitted to the Agency Business Owner or Sponsor as an *Agency Project Request (APR)* for evaluation to make sure the 'concept' is worth pursuing further. The initial *APR* approval leads to the creation of a business case and preliminary user requirements, the 2 primary deliverables used as justification to pursue the 'concept' as a project to support funding and staffing to begin the project

The people involved in the 'concept' should balance the tradeoff between defining the project in detail and moving quickly enough to a go/no-go decision. The purpose of the initial *APR* approval is NOT to fully design the system, determine all costs, or plan the overall project. Detailed requirements definition, costing, and planning will be performed during the *Initiation Process*, once senior management has decided that the basic concept is worth pursuing further

Concept phase (Software Development Projects) - The initial phase of a software development project, in which the user needs are described and evaluated through documentation (for example, statement of needs, advance planning report, project initiation memo, feasibility studies, system definition, documentation, regulations, procedures, or policies relevant to the project) (SEI)

Conceptual Architecture. The intent of the conceptual architecture is to direct attention at an appropriate decomposition of the system without delving into the details of interface specification and type information. Moreover, it provides a useful vehicle for communicating the architecture to non-technical audiences, such as management, marketing, and many users. The conceptual architecture identifies the system components, the responsibilities of each component, and interconnections between components. The structural choices are driven by the system qualities, and the rationale section articulates and documents this connection between the architectural requirements and the structures (components and connectors or communication/co-ordination mechanisms) of the architecture

Conceptual Project Planning - The process of developing broad-scope project documentation from which the technical requirements, estimates, schedules, control procedures, and effective project management will all flow

Configuration Management Plan (CMP) - Used to define the processes and procedures set up to control the release of product. The product could be hardware, software or documentation. May be the responsibility of a specific Configuration Management team or person, or as additional responsibilities to another assigned person or team

Contingency Planning - The development of a management plan that identifies alternative strategies to be used to ensure project success if specified risk events occur

Contingency Plan - Management policy and procedures designed to maintain or restore business operations, including computer operations, in the event of emergencies, system failures, or disaster

Contract Administration - The process of managing the contract and the relationship between the buyer and seller, reviewing and documenting how a seller is performing or has performed to establish required corrective

actions and provide a basis for future relationships with the seller, managing contract related changes and, when appropriate, managing the contractual relationship with the outside buyer of the project. (PMBOK 3RD EDITION)

Controlled Interfaces - Mechanisms that facilitate the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system such as but not limited to proxies, gateways, routers, firewalls, encrypted tunnels)

Concurrency - A measure of the number of users engaged in the same operation at the same time (ITIL® V3)

Confidentiality - A security principle that requires that data should only be accessed by authorized people (ITIL® V3, Service Design)

Configuration - A generic term, used to describe a group of configuration items that work together to deliver an IT Service, or a recognizable part of an IT Service. Configuration is also used to describe the parameter settings for one or more CIs (ITIL® V3**,** Service Transition)

Configuration Baseline - A baseline of a configuration that has been formally agreed and is managed through the change management process. A configuration baseline is used as a basis for future builds, releases and changes (ITIL® V3, Service Transition)

Configuration Control - The activity responsible for ensuring that adding, modifying or removing a CI is properly managed, for example by submitting a request for change or service request (ITIL® V3, Service Transition)

Configuration Identification - The activity responsible for collecting information about configuration items and their relationships, and loading this information into the CMDB. Configuration identification is also responsible for labeling the CIs themselves, so that the corresponding configuration records can be found (ITIL® V3, Service Transition)

Configuration Item (CI) - Any component that needs to be managed in order to deliver an IT Service. Information about each CI is recorded in a configuration record within the Configuration Management System and is maintained throughout its lifecycle by Configuration Management. CIs are under the control of Change Management. CIs typically include IT Services, hardware, software, buildings, people, and formal documentation such as process documentation and SLAs (ITIL® V3, Service Transition)

Configuration Management - The process responsible for maintaining information about configuration items required to deliver an IT Service, including their relationships. This information is managed throughout the lifecycle of the CI. Configuration Management is part of an overall Service Asset and Configuration Management Process (ITIL® V3, Service Transition)

Configuration Management Database (CMDB) - A database used to store configuration records throughout their lifecycle. The Configuration Management System maintains one or more CMDBs, and each CMDB stores attributes of CIs, and relationships with other CIs (ITIL® V3, Service Transition)

Configuration Management System (CMS) - A set of tools and databases that are used to manage an IT Service Provider's configuration data. The CMS also includes information about incidents, problems, known errors, changes and releases; and may contain data about employees, suppliers, locations, business units, customers and users. The CMS includes tools for collecting, storing, managing, updating, and presenting data about all configuration items and their relationships. The CMS is maintained by Configuration Management and is used by all IT Service Management Processes (ITIL® V3, Service Transition)

Configuration Record - A record containing the details of a configuration item. Each configuration record documents the lifecycle of a single CI. Configuration records are stored in a Configuration Management Database (ITIL® V3, Service Transition)

Configuration Structure - The hierarchy and other relationships between all the configuration items that comprise a configuration (ITIL® V3, Service Transition)

Continuity of Operations Plan (COOP): A predetermined set of instructions or procedures that describe how an organization's essential functions will be sustained for up to 30 days as a result of a disaster event before returning to normal operations

Continual Service Improvement (CSI) - Continual Service Improvement is responsible for managing improvements to IT Service Management Processes and IT Services. The performance of the IT Service Provider is continually measured and improvements are made to processes, IT Services and IT infrastructure in order to increase efficiency, effectiveness, and cost effectiveness (ITIL® V3, Continual Service Improvement)

Continuous Availability - An approach or design to achieve 100% Availability. A Continuously Available IT Service has no planned or unplanned Downtime (ITIL® V3, Service Design)

Continuous Operation - An approach or design to eliminate planned downtime of an IT Service. Note that individual configuration items may be down even though the IT Service is available (ITIL® V3, Service Design)

Contract - A legally binding agreement between two or more parties

Control - (ITIL® V3)
(1) A means of managing a risk, ensuring that a business objective is achieved, or ensuring that a process is followed. Example controls include policies, procedures, roles, RAID, door-locks etc. A control is sometimes called a countermeasure or safeguard
(2) A means to manage the utilization or behavior of a configuration item, system or IT Service

Controlled Interfaces - Mechanisms that facilitate the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system such as but not limited to proxies, gateways, routers, firewalls, encrypted tunnels)

Core Processes - Processes that have clear dependencies and that require the same order on most projects. See life cycle processes: Initiation, Planning, Execution and Control, and Close. (ITIL® V3)

Core Service - An IT Service that delivers basic outcomes desired by one or more customers. (ITIL® V3**,** Service Strategy)

Cost is the sum of all anticipated expenditures over the life of the project, including but not limited to: consultant fees; salaries for new and existing employees; software license and maintenance fees; hardware and maintenance expenses; telecommunication and connectivity expenses; deployment expenses; training expenses and any other expenses associated with the project. However, cost shall not include existing, full-time state personnel tasked with the planning, implementation, and support of technology

Cost Benefit Analysis - An activity that analyses and compares the costs and the benefits involved in one or more alternative courses of action

Cost Budgeting - The process of aggregating the estimated costs of individual activities or work packages to establish a cost baseline. (PMBOK 3RD EDITION)

Cost Effectiveness - A measure of the balance between the effectiveness and cost of a service, process or activity. A cost effective process is one which achieves its objectives at minimum cost

Cost of Operation - The overall cost of operating a computer system to include the costs associated with personnel, training, and system operations

Cost Performance Index (CPI) - A measure of cost efficiency on a project. It is the ratio of earned value (EV) to actual costs (AC). CPI = EV divided by AC. A value equal to or greater than one indicates a favorable condition and a value less than one indicates an unfavorable condition. (PMBOK 3RD EDITION)

Cost Variance (CV) - A measure of cost performance on a project. It is the algebraic difference between earned value (EV) and actual cost (AC). CV=EV minus AC. A positive value indicates a favorable condition and a negative value indicates an unfavorable condition. (PMBOK 3RD EDITION)

Countermeasure - Can be used to refer to any type of control. The term Countermeasure is most often used when referring to measures that increase resilience, fault tolerance or reliability of an IT Service. (ITIL® V3)

Crisis Management - The process responsible for managing the wider implications of business continuity. A Crisis Management team is responsible for strategic issues such as managing media relations and shareholder confidence, and decides when to invoke Business Continuity Plans. (ITIL® V3)

Critical Business Application - An application that is critical to the running of the agency's work. If the application were to fail, the agency goals would not be met. See Application Risk Categories

Critical Path Method (CPM) - A schedule network analysis technique used to determine the amount of scheduling flexibility (the amount of float) on various logical network paths in the project schedule network, and to determine the minimum total project duration. Early start and finish dates are calculated by means of a forward pass using a specified start date. Late start and finish dates are calculated by means of a backward pass, starting from a specified completion date, which sometimes is the project early finish date determined during the forward pass calculation. (PMBOK 3RD EDITION)

Critical Partner - Subject matter experts in the areas of Security, Acquisition Management, Finance, Budget, and Project Assurance who have expert participation roles in the IT investment governance decision processes of EPLC to ensure compliance with policies in their respective areas and to make timely tradeoff decisions where conflicts arise during the planning and execution of an investment

Critical Projects Review Panel - A State (enterprise level) IT governance organization which has the primary objective of understanding and responding to the business implications and issues associated with critical technology projects. The Panel provides a forum for agency heads to ensure they have the commitments and resources needed to deliver on their IT initiatives successfully

Critical Success Factors -
(1) The limited number of areas of performance that are essential for a project to achieve its goals and objectives. They are the key areas of activity in which favorable results are absolutely necessary to reach goals. Critical success factors are often referred to as "CSF". (SEI)
(2) KPIs are used to measure the achievement of each CSF. For example a CSF of "protect IT Services when making changes" could be measured by KPIs such as "percentage reduction of unsuccessful changes", "percentage reduction in changes causing incidents" etc. (ITIL® V3)

Cryptography is a branch of applied mathematics concerned with encrypting and decrypting data such that the sender's identity (authentication and non-repudiation), data confidentiality or integrity can be assured.

- **Encryption** is the process of converting ordinary information (plaintext) into unintelligible character

strings (i.e., *ciphertext*)
- **Decryption** is the reverse, moving from unintelligible ciphertext to plaintext
- A **cipher** (or *cypher*) is a pair of algorithms which perform this encryption and the reversing decryption
- **Key** (or cryptographic key) - A parameter used in conjunction with a cryptographic algorithm that an entity with knowledge of the key can reproduce or reverse the operation (encrypt or decrypt) while an entity without knowledge of the key cannot

Culture - A set of values that is shared by a group of people, including expectations about how people should behave, ideas, beliefs, and practices. (ITIL® V3)

Current Finish Date -The current estimate of the point in time when a schedule activity will be completed, where the estimate reflects any reported work progress. (PMBOK 3RD EDITION)

Current Start Date -The current estimate of the point in time when a schedule activity will begin, where the estimate reflects any reported work progress. (PMBOK 3RD EDITION)

Customer – The person or organization that will use the project's product or service or results. (PMBOK 3rd Edition)

Customization- Updates or changes to software that are specially developed for some specific organization or other user. Programming Code that is not delivered by application provider

D

Dashboard - A graphical representation of overall IT Service Performance and Availability. Dashboard images may be updated in real-time, and can also be included in management reports and web pages. Dashboards can be used to support Service Level Management, Event Management or Incident Diagnosis. (ITIL® V3, Service Operation)

Data – Any representation of facts, concepts or instructions (structured, semi-structured or unstructured) in a formalized manner suitable for communication, interpretation or processing by people or by machines

Data Classification - Applying standard descriptions of characteristics to data. In the case of data sharing, this specifically refers to security, privacy, integrity and commercial value of the data

Data Custodianship is the responsibility assumed by anyone entrusted with state information for upholding the security objectives of confidentiality, integrity and availability while that information is in that person's possession either physically or digitally

Data Owner – The agency which is responsible for creating and/or maintaining specific data, and its accuracy and completeness is the data owner. The agency head will assign this responsibility to one or more individuals within the agency. These individuals shall be responsible for protecting and managing the use and sharing of the specific data

Data Steward – The specific employee or position assigned by a Data Owner to protect and manage the use of specific data

Data-sharing – Data-sharing is allowing data to be used in an agency outside of the Data Owner's agency

Database
(1) A collection of logically related data stored together in one or more computerized files. Note: Each data item is identified by one or more keys. (SEI)
(2) An electronic repository of information accessible via a query language interface. (SEI)

Database administration - The responsibility for the definition, operation, protection, performance, and recovery of a database (SEI)

Database design - The process of developing a database that will meet a user's requirements. The activity includes three separate but dependent steps: conceptual database design, logical database design, and physical database design (SEI).

Defect- An error, flaw, failure, or fault in a software application or system that produces an incorrect or unexpected result, or causes it to behave in unintended ways

Defense-in Depth – An Information Assurance (IA) "best practices" strategy for protecting networked environments where multiple layers of security defenses (policy, personnel, technology and operations) are placed throughout a network infrastructure to protect internal data, systems, networks, and users such that if one mechanism fails, another will already be in place to continue to protect the assets

Definitive Media Library (DML) - One or more locations in which the definitive and approved versions of all software configuration items are securely stored. The DML may also contain associated CIs such as licenses and documentation. The DML is a single logical storage area even if there are multiple locations. All software in the DML is under the control of change and release management and is recorded in the Configuration Management System. Only software from the DML is acceptable for use in a release. (ITIL® V3, Service Transition)

Deliverable -
(1) Any unique and verifiable product, result or capability to perform a service that must be produced to complete a process, phase, or project. Often used more narrowly in reference to an external deliverable, which is a deliverable subject to approval by the project sponsor or customer. (PMBOK 3RD EDITION)
(2) Something that must be provided to meet a commitment in a Service Level Agreement or a Contract. Deliverable is also used in a more informal way to mean a planned output of any process. (ITIL® V3**)**

Demand Management - Activities that understand and influence customer demand for devices and the provision of capacity to meet these demands. At a strategic level Demand Management can involve analysis of patterns of business activity and user profiles. At a tactical level it can involve use of differential charging to encourage customers to use IT Services at less busy times. (ITIL® V3**)**

Demilitarized Zone (DMZ) - A host or network segment inserted as a "neutral zone" between an organization's private network and the Internet

Dependency - (ITIL® V3)
(1) In a project, a relationship between two tasks, or projects, where the full or partial start or finish of one task determines the start or finish of the other
(2) In IT service operations, the direct or indirect reliance of one process or activity upon another

Deploy – The 3rd stage in the Build step of the EPLC where a project team performs comprehensive audit and testing of the requirements, design, code and documentation. ("Enterprise Performance Life Cycle Management" Guideline, published by GTAs Enterprise Project management Office) and places the results of the project into live operation

Deployment - The activity responsible for movement of new or changed hardware, software, documentation, process, etc to the live environment. Deployment is part of the Release and Deployment Management Process. (ITIL® V3, Service Transition)

Deployment Certification - This Certification is an explicit go-live decision to place a new or modified application into production and to explicitly accept the risk to agency operations (including mission, functions, image, or

reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of business, system and security requirements. The Deployment Certification should be proceduralized as an essential component of the project quality assurance lifecycle, as well as the procurement and contracting processes, and any related product or service contract should include a payment holdback provision subject to acquiring Deployment Certification. Deployment Certification is required prior to initial deployment, with updates, at least every three years or more often at each instance of change to any component of a deployed application

- **Authorizing Official** - Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets or individuals.
- **Application Owners** - For the purposes of application development and deployment certification, the individuals designated as the Project/Product Manager, the Executive Sponsor and the Technical Leader are jointly and collectively termed Application Owners.

Depreciation - A measure of the reduction in value of an asset over its life. This is based on wearing out, consumption or other reduction in the useful economic value. (ITIL® V3, Service Strategy)

Design –
(1) An activity or process that identifies requirements and then defines a solution that is able to meet these Requirements. (ITIL® V3, Service Design)
(2) The 1st stage in the Build step of the EPLC wherein a project team develops the design for development based on the business and technical requirements. ("Enterprise Performance Life Cycle Management" Guideline, published by GTAs Enterprise Project management Office)

Design Documents - Technical documents that lay out in detail the anticipated design of the project deliverable

Design phase (Software Application Projects) - The period of time in the software life cycle during which the designs for architecture, software components, interfaces, and data are created, documented, and verified to satisfy requirements (SEI)

Detailed Project Planning – Activities required for completing a detailed project plan for project execution and control as specified in the State of Georgia Agency Project Management Standard and Guideline

Detection - A stage in the Incident Lifecycle. Detection results in the incident becoming known to the service provider. Detection can be automatic, or can be the result of a user logging an incident. (ITIL® V3, Service Operation)

Developer- Individual responsible for maintaining and improving the systems used by organizations in their day-to-day operations and for serving as a go-between among different areas of an organization to resolve technology problems

Development - (ITIL® V3, Service Design)
(1) The process responsible for creating or modifying an IT Service or application
(2) The role or group that carries out development work
(3) The 2nd stage in the Build step of the EPLC wherein a project team develops code/configuration and/or capabilities required to deploy the business product/service. ("Enterprise Performance Life Cycle Management" Guideline, published by GTAs Enterprise Project management Office)

Development Environment - An environment used to create or modify IT Services or applications. Development environments are not typically subjected to the same degree of control as test environments or live environments. (ITIL® V3, Service Design)

Diagnosis - A stage in the incident and problem lifecycles. The purpose of diagnosis is to identify a workaround for an incident or the root cause of a problem. (ITIL® V3, Service Operation)

Diagnostic Script - A structured set of questions used by Service Desk staff to ensure they ask the correct questions, and to help them classify, resolve and assign incidents. Diagnostic scripts may also be made available to users to help them diagnose and resolve their own incidents. (ITIL® V3, Service Operation)

Disaster Recovery Plan
(1) An element of Business Continuity Planning to identify, prioritize and restore IT operations that support business
(2) A written plan that details how an organization's applications and/or infrastructure will be recovered or rebuilt and returned to normal operations after a major hardware or software failure or destruction of facilities
(3) A comprehensive statement of consistent actions to be taken by an organization to respond quickly to a disaster or serious interruption of service to stabilize and restore critical functions. The plan should be documented and tested to ensure its effectiveness in continuing operations or restoration and availability of critical resources in the event of a disaster

Disposition – The 2nd stage of the Run step of the EPLC wherein an IT product(s)/service(s) is deliberately and systematically decommissioned or retired. ("Enterprise Performance Life Cycle Management" Guideline, published by GTAs Enterprise Project management Office)

Documentation Management –
(1) Project deliverables management including: planning, development, processes, control, management reporting, numbering schemes and security around documents generated during the full life cycle of an Agency initiative, program or project
(2) Managing and controlling any unique and verifiable product, result or capability used to perform a service produced to complete a process, phase, or project. Often used in reference to an external deliverable, subject to approval by the project sponsor or customer

Do Nothing - A recovery option. The Service Provider formally agrees with the customer that recovery of a given IT Service will not be performed. (ITIL® V3, Service Design)

Downtime - The time when a configuration item or IT Service is not available during its Agreed Service Time. The availability of an IT Service is often calculated from Agreed Service Time and downtime. (ITIL® V3, Service Design, Service Operation)

Driver - Something that influences strategy, objectives or requirements, for example, new legislation or the actions of competitors

Due Diligence and Due Care - the degree of effort and care that a prudent person might be expected to exercise in the examination and evaluation of risks affecting a business transaction

Duration -The total number of work periods (not including holidays or other non-working periods) required to complete a schedule activity or work breakdown structure components. Usually expressed as workdays or workweeks. Sometimes incorrectly equated with elapsed time. Contrast with effort. (PMBOK 3RD EDITION)

E

E-surplus –
(1) Electronic equipment that is no longer needed by the owning agency or has exceeded its useful life.
(2) This term shall also be used to cover all forms of storage media including but not limited to: electronic, magnetic, optical or other representation of data

ESF - See Emergency Support Function

Early Life Support - Support provided for a new or changed IT Service for a period of time after it is released. During Early Life Support the IT service provider may review the KPIs, Service Levels and Monitoring Thresholds, and provide additional resources for Incident and Problem Management. (ITIL® V3, Service Transition)

Early Finish Date (EF) - In the critical path method, the earliest possible point in time on which the uncompleted portions of a schedule activity (or the project) can finish, based on the schedule network logic, the data date, and any schedule constraints. Early finish dates can change as the project progresses and as changes are made to the project management plan. (PMBOK 3RD EDITION)

Early Start Date -In the critical path method, the earliest possible point in time on which the uncompleted portions of a schedule activity (or the project) can start, based on the schedule network logic, the data date and any schedule constraints. Early start dates can change as the project progresses and changes are made to the project management plan. (PMBOK 3RD EDITION)

Earned Value (EV) - The value of completed work expressed in terms of the approved budget assigned to that work for a schedule activity or work breakdown structure component. (PMBOK 3RD EDITION)

Economies of Scale - The reduction in average cost that is possible from increasing the usage of an IT Service or asset. (ITIL® V3, Service Strategy)

Effectiveness - A measure of whether the objectives of a process, service or activity have been achieved. An effective process or activity is one that achieves its agreed objectives. (ITIL® V3, Continual Service Improvement)

Efficiency - A measure of whether the right amount of resources have been used to deliver a process, service or activity. An efficient process achieves its objectives with the minimum amount of time, money, people or other resources. (ITIL® V3, Continual Service Improvement)

Effort -The number of labor units required to complete a schedule activity or work breakdown structure component. Usually expressed as staff hours, staff days, or staff weeks. Should not be confused with duration

Electronic Data, Information and/or Record is any form of digitally recorded material generated, transmitted, received and/or stored that is designated a record by data owner or law, based on content and/or subject matter. This includes but is not limited to electronic digital interchange, email, digital/text voice messages, instant messages and text messages

Electronic Media – Any electronic equipment that uses non-volatile memory to store data. (Examples include but are not limited to: Desktop computers, laptop/notebook computers, network servers, Network Storage Devices, PDAs, Network routers and switches, Digital copiers, scanners, printers, and faxes)

Electronic Mail, abbreviated **email** or **email**, is a method of composing, sending, storing, and receiving messages over electronic communication systems or Email Systems. The term email applies both to the Internet email system based on the Simple Mail Transfer Protocol (SMTP) and to intranet systems allowing users within one company or organization to send messages to each other

Elicitation- The collecting of the requirements of a system from users, customers and other stakeholders

Email Systems are software and hardware systems that transport messages from one computer user to another. Email systems range in scope and size from a local email system that carries messages to users within an agency or

office over a local area network (LAN) or an enterprise-wide email system that carries messages to various users in various physical locations over a wide area network (WAN) email system to an email system that sends and receives messages around the world over the internet. Often the same email system serves all three functions

Email Messages are electronic documents created and sent or received by a computer via an email system. This definition applies equally to the contents of the communication, the transactional information, and any attachments associated with such communication. Email messages are similar to other forms of communicated messages, such as correspondence, memoranda and circular letters

Emergency Change - A change that must be introduced as soon as possible. For example to resolve a major incident or implement a security patch. The Change Management Process will normally have a specific procedure for handling emergency changes. (ITIL® V3, Service Transition)

Emergency Change Advisory Board (ECAB) - A sub-set of the Change Advisory Board who make decisions about high impact emergency changes. Membership of the ECAB may be decided at the time a meeting is called, and depends on the nature of the emergency change. (ITIL® V3, Service Transition)

Emergency Support Function (ESF) - Agencies are designated as having ESF in the Governor's executive order (EO) and the Georgia Emergency Operations Plan (GEOP). These agencies have primary and/or support responsibilities to provide essential services or support for those services during a man-made, natural, or environmental state emergency. Go to www.gema.gov to review the EO and the GEOP to ESF agencies

End User - The individual or group who will use the system for its intended operational use when it is deployed in its environment

Enterprise – An organization with common or unifying business interests. An enterprise may be defined at the State of Georgia level, the Sponsor level, or Business Owner level for programs and projects requiring either vertical or horizontal integration. At times within Georgia's state government, "enterprise" refers to the group of GETS agencies (those participating in the Georgia Enterprise Technology Service operated by GTA); however, for Statewide Information Technology Governance Reports the term refers to "all agencies at the state level"

Enterprise Architecture -Enterprise Architecture (EA) is a framework that is designed to coordinate the many facets of IT that comprise the state's technology infrastructure. It is a plan which supports the components that collectively comprise an enterprise's business architecture.
Components of the business architecture include aspects of business planning such as goals, visions, strategies and governance principles; aspects of business operations such as business terms, organization structures, processes and data; aspects of automation such as application systems and databases; and the enabling technological infrastructure of the business such as computers, operating systems and networks

Enterprise Application: An application that:

- Is operated by one agency (or sourced by an agency),
- Provides for, or will be able to provide upon implementation, one or more common business functions of multiple agencies, and
- Has been designated as such by the State Enterprise Application Council or by State statute.

Enterprise Application Integration (EAI) is the sharing of data, services, and business processes throughout networked applications or data sources

Enterprise Information Integration (EII) is a software infrastructure that combines various data sources at an enterprise level to support applications that present or analyze the data in new ways. EII provides a service that

allows administrators, developers, and end-users to treat a broad array of data sources as if they were one large database or data service
EAI and EII both address the problem of integration but from different perspectives. EAI deals with straightforward application connection needs, while EII is concerned with a more complex integration of the information structures that the applications process. Today, EII solutions often address both application and information integration

Enterprise Integration (EI) means EAI, EII, or both

Enterprise Operational Environment (EOE) – The IT Infrastructure and managed network services managed by Georgia Enterprise Technology Services (GETS) is the EOE for the State of Georgia.

Enterprise Performance Life Cycle (EPLC) - A methodology to organize the activities, deliverables, and governance reviews activities of project managers and all stakeholders during the life of an IT investment into ten life-cycle phases. Seven of the ten phases are traditional "project" lifecycle phases, the remaining phases are the investment phases of conception, operation and disposal of the IT investment. The phases are: 1) concept 2) initiation 3) planning 4) requirements analysis 5) design 6) development 7) test 8) transition 9) operate 10) dispose. The last step of each phase is a Stage Gate Review to ensure that the investment status may progress to the next phase

Enterprise Program Management (EPM) – An Information Technology Investment Management-based methodology to manage programs and projects of enterprise significance. EPM focuses on the management of multiple related programs and projects that individually support the same mission or ongoing activity

Enterprise Technology Program - A group of related IT projects, aggregated for management purposes that support a defined enterprise

Environment - (ITIL® V3)
(1) (Service Transition) A subset of the IT infrastructure that is used for a particular purpose. For Example: Live Environment, Test Environment, Build Environment. It is possible for multiple environments to share a configuration item, for example Test and Live Environments may use different partitions on a single mainframe computer
(2) The Physical Environment including floor space, accommodation, air conditioning, power system etc.
(3) A generic term to mean the external conditions that influence or affect something

EPLC – The Enterprise Performance Life Cycle framework or management process. A framework used by State agencies to manage their technology investments in order to achieve consistently successful outcomes. Includes the “Plan”, “Build” and “Run” processes with seven (7) embedded stages. Project Managers are required to demonstrate a project’s readiness to proceed from stage to stage via stage gate reviews. Reference GTA Enterprise Standards SM-10-006, SM-10-007 and SM-10-008. (“Enterprise Performance Life Cycle Management” Guideline, published by GTAs Enterprise Project management Office)

ERP (Enterprise Resource Planning) - A cross-functional enterprise system driven by an integrated suite of software modules that supports the basic internal business processes of an organization. ERP gives an organization an integrated real-time view of its core business processes

Error - A design flaw or malfunction that causes a failure of one or more configuration items or IT Services. A mistake made by a person or a faulty process that impacts a CI or IT Service is also an Error. (ITIL® V3, Service Operation)

Escalation - An activity that obtains additional resources when these are needed to meet Service Level Targets or customer expectations. Escalation may be needed within any IT Service Management Process, but is most

commonly associated with Incident Management, Problem Management and the management of customer complaints. There are two types of Escalation, Functional Escalation and Hierarchic Escalation. (ITIL® V3, Service Operation)

Estimate – A quantitative assessment of the likely amount or outcome. Usually applied to project costs, resources, effort, and duration and is usually preceded by a modifier (i.e.,) preliminary, conceptual, feasibility, order of-magnitude, definitive). It should always include some indication of accuracy (e.g. + percent). (PMBOK 3RD EDITION)

Estimate at Completion (EAC) - The expected total cost of a schedule activity, a work breakdown structure component, or the project when the defined scope of work will be completed. EAC is equal to the actual cost (AC) plus the estimate to complete (ETC) for all of the remaining work. EAC=AC plus ETC. The EAC may be calculated based on performance to date or estimated by the project team based on other factors, in which case it is often referred to as the latest revised estimate. (PMBOK 3RD EDITION)

Estimate to Complete (ETC) - The expected cost needed to complete all the remaining work for a schedule activity, work breakdown structure component, or the project. (PMBOK 3RD EDITION)

Estimation - The use of experience to provide an approximate value for a metric or cost. Estimation is also used in Capacity and Availability Management as the cheapest and least accurate Modeling method. (ITIL® V3)

Ethics – In the conduct of their operations, state organizations and their employees will employ information technology in a legal and ethical manner consistent with government statutes, rules, and regulations. Information technology will not be used for purposes that are unrelated to the state organization's mission or violates state or federal law. Contract provisions, including software licensing agreements, will be strictly enforced

Evaluation -
(1) (Service Transition) The process responsible for assessing a new or changed IT Service to ensure that risks have been managed and to help determine whether to proceed with the change. (ITIL® V3)
(2) Evaluation is also used to mean comparing an actual outcome with the intended outcome, or comparing one alternative with another

Event - (ITIL® V3, Service Operation)
(1) A change of state which has significance for the management of a configuration item or IT Service
(2) The term Event is also used to mean an alert or notification created by any IT Service, configuration item or monitoring tool. Events typically require IT Operations personnel to take actions, and often lead to incidents being logged

Events of Interest are questionable or suspicious activities that could threaten the security objectives for critical or sensitive data or infrastructure. They may or may not have criminal implications

Event Management - The process responsible for managing Events throughout their lifecycle. Event Management is one of the main activities of IT Operations. (ITIL® V3, Service Operation)

Expanded Incident Lifecycle - Detailed stages in the lifecycle of an incident. The stages are Detection, Diagnosis, Repair, Recovery, and Restoration. The Expanded Incident Lifecycle is used to help understand all contributions to the impact of incidents and to plan how these could be controlled or reduced. (ITIL® V3, Availability Management)

F

Facilities Management - The function responsible for managing the physical environment where the IT Infrastructure is located. Facilities Management includes all aspects of managing the physical environment, for example power and cooling, building access management, and environmental monitoring. (ITIL® V3, Service Operation)

Failure - Loss of ability to operate to specification, or to deliver the required output. The term Failure may be used when referring to IT Services, processes, activities, configuration items etc. A Failure often causes an incident. (ITIL® V3, Service Operation)

Facilities Management Plan (FMP) –
(1) At minimum, a documented statement of the intended actions a project organization will take to prepare workspaces or buildings ready for project or operational use.
(2) A comprehensive statement of all key factors guiding a management team in their pursuit of a safe, effective physical workspace.
(3) The specific document prepared as a project deliverable detailing plans for facilities management.

Fast Recovery - A recovery option which is also known as Hot Standby. Provision is made to recover the IT Service in a short period of time, typically less than 24 hours. Fast Recovery typically uses a dedicated fixed facility with computer systems, and software configured ready to run the IT Services. Immediate Recovery may take up to 24 hours if there is a need to restore data from Backups. (ITIL® V3, Service Design)

Fault - Synonym for Error

Fault Tolerance - The ability of an IT Service or configuration item to continue to operate correctly after failure of a component part. (ITIL® V3, Service Design)

"Federal work authorization program" means any of the electronic verification of work authorization programs operated by the US Department of Homeland Security (USDHS) or any equivalent federal work authorization program operated by the USDHS to verify information of newly hired employees

Financial Closure - The process of completing and terminating the financial and budgetary aspects of the project being performed. It includes both (external) contract closure and (internal) project account closure

Financial Management - The 4th of 9 PMI standard *Knowledge Areas*. The recommended processes ensure that the project is completed within the approved budget. The recommended processes are: Cost Estimating, Cost Budgeting, and Cost Control

FIPS 140-2 Validated Cryptographic Modules – cryptographic s including, but not limited to, hardware components or modules, software/firmware programs or modules or any combination thereof that employ approved security functions such as cryptographic algorithms, cryptographic key management techniques, and authentication techniques and validate through the Cryptographic Module Validation Program (CMVP)

Firewall - A combination of hardware and software designed to prevent outsiders from accessing an internal network while allowing internal customers to access outside networks

First-line Support - The first level in a hierarchy of support groups involved in the resolution of incidents. Each level contains more specialist skills, or has more time or other resources. (ITIL® V3, Service Operation)

FISMA – The Federal Information Security Management Act (FISMA) requires each [federal] agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source

FISMA-based security assessment - An assessment of a system's security controls based on the FISMA risk management framework and NIST SP800-53A

Fit for Purpose - An informal term used to describe a process, configuration item, IT Service etc. that is capable of meeting its objectives or Service Levels. Being Fit for Purpose requires suitable design, implementation, control and maintenance. (ITIL® V3)

FIT-GAP Analysis - This analysis determines if the current software/ system fit the requirements defined and identifies gaps where it does not. It is used for implementing the correct requirements and design into a project plan

Fixed price or lump sum contracts – This category of contract involves a fixed total price for a well-defined product. Fixed price contracts may also include incentives for meeting or exceeding selected project objectives such as schedule targets

Float - The amount of time that a schedule activity can be delayed without delaying the early start of any immediately following schedule activities. Also called slack, total float, free float and path float. (PMBOK 3RD EDITION)

Fulfillment - Performing activities to meet a need or requirement. For example by providing a new IT Service, or meeting a Service Request. (ITIL® V3)

Full Time Equivalent - FTE
Full-time equivalent (FTE) is a calculated figure to indicate the proportion of full time labor applied to a given task. Calculated as follows:

1) Calculate FTE for salaried positions:
   - A full-time budgeted position = 1.0 FTE
   - If 10% of a staff position is spent supporting this application the FTE would be: 1.0 x .10 = .10 FTE
   - If 5 staff positions each spend 10% supporting this application the FTE would be: 5 x .10 = .50 FTE
2) Calculate FTE for hourly positions (also use for hourly contractors/ consultants)
   - Total annual hours of time spent supporting this application divided by 2,080 (52 weeks/yr x 40 hrs/week = 2,080 hours annually = full-time)
   - If full-time hourly position spends 988 hours supporting this application during the year, the FTE calculation is: 988 divided by 2080 = .48 FTE (rounded)
   - If part-time hourly position works 500 hours annually and spends 10% of that supporting this application, the FTE calculation is: 500 x .10 divided by 2080 = .02 FTE (rounded)

Function (ITIL® V3)
(1) A team or group of people and the tools they use to carry out one or more processes or activities: for example, the Service Desk
(2) An intended purpose of a configuration item, person, team, process, or IT Service. For example one function of an Email Service may be to store and forward outgoing mails, one function of a business process may be to dispatch goods to customers
(3) To perform the intended purpose correctly, "The computer is functioning"

Functional Escalation - Transferring an incident, problem or change to a technical team with a higher level of expertise to assist in an escalation. (ITIL® V3, Service Operation)

Functional Requirements – These requirements build on Business Requirements to show how a requirement can be achieved within a specified software. Functional requirements capture the intended behavior of the system-or what the system will do. This behavior may be expressed as services, security, tasks or functions the system is

required to perform. Functional Requirements drive the application architecture of a system. These requirements should be testable

Functional testing –

(1) Testing that ignores the internal mechanism of a system or component and focuses solely on the outputs generated in response to selected inputs and execution conditions. Synonym: black-box testing. (SEI)
(2) Functions are tested by feeding them input and examining the output, and internal program structure is rarely considered (not like in white box testing). Functional Testing usually describes *what* the system does

G

Gantt Chart - See bar chart. (PMBOK 3RD EDITION)

Gap Analysis - An activity which compares two sets of data and identifies the differences. Gap Analysis is commonly used to compare a set of Requirements with actual delivery. (ITIL® V3, Continual Service Improvement)

Governance - Ensuring that policies and strategy are actually implemented, and that required processes are correctly followed. Governance includes defining roles and responsibilities, measuring and reporting, and taking actions to resolve any issues identified. (ITIL® V3)

Governing Body - The term is relative to the risk, complexity and cost of an investment. For major State investments and critical projects, the IT governing body will be the State Critical Project Panel. For delegated projects, an IT governing body organization may be designated by the Business Owner

Gradual Recovery - A recovery option which is also known as Cold Standby. Provision is made to recover the IT Service in a period of time greater than 72 hours. Gradual recovery typically uses a portable or fixed facility that has environmental support and network cabling, but no computer systems. The hardware and software are installed as part of the IT Service Continuity Plan. (ITIL® V3, Service Design)

Guidelines - Are directives and specifications, similar to standards, but advisory in nature. In essence, guidelines constitute recommendations which are not binding on agencies and institutions of higher education

H

Hardware maintenance (Project-related Operations) - The cost associated with the process of retaining, or restoring a hardware system or hardware component to a state in which it can perform its required functions

Help Desk - A point of contact for users to log incidents. A Help Desk is usually more technically focused than a Service Desk and does not provide a Single Point of Contact for all interaction. The term Help Desk is often used as a synonym for Service Desk. (ITIL® V3, Service Operation)

Hierarchic Escalation - Informing or involving increasingly more senior levels of management to respond to an event. (ITIL® V3, Service Operation)

High Availability - An approach or design that minimizes or hides the effects of configuration item failure from the users of an IT Service. High Availability solutions are designed to achieve an agreed level of availability and make use of techniques such as fault tolerance, resilience and fast recovery to reduce the number of incidents, and the impact of incidents. (ITIL® V3, Service Design)

Hot Standby - Synonym for Fast Recovery or Immediate Recovery. Provision is made to recover the IT Service with no loss of service. Immediate recovery typically uses mirroring, load balancing and split site technologies. (ITIL® V3, Service Design)

I

iCalendar – A standard (RFC2445 or RFC2445 Syntax Reference) for calendar data exchange. iCalendar allows users to send meeting requests and tasks to other users through emails. Recipients of the iCalendar email (with supported software) can respond to the sender easily or counterpropose another meeting date/time

Identified for Preliminary Planning – Projects which address an agency business need but which requires additional effort by the agency or further review at the CIO Level before authorizing the expenditure of planning funds

Identity - A unique name that is used to identify a user, person or role. The identity is used to grant rights to that user, person, or role. Example identities might be the username SmithJ or the Role "Change Manager". (ITIL® V3, Service Operation)

Identity and Access Management is a set of processes and supporting infrastructure for creating, maintaining, and using digital identities in accordance with business policies and needs

Immediate Recovery - A recovery option which is also known as Hot Standby. Provision is made to recover the IT Service with no loss of service. Immediate recovery typically uses mirroring, load balancing and split site technologies. (ITIL® V3, Service Design)

Impact - A measure of the effect of an incident, problem or change on business processes, projects, programs or enterprise. Impact is often based on how Service Levels will be affected. Impact and urgency are used to assign priority. (ITIL® V3)

Impact Statement - A cause and effect report generated at the manager level to show the impact that new projects will have on current schedules and resources as they enter the work stream

Implementation - Occurs when products that have completed testing are moved into production or into their working environment

Important Business Application - Agency could operate and meet *most* goals if the application did not function. See Application Risk Categories

Inappropriate usage includes (but is not limited to) actual or attempted misuse of information technology resources for:

- Conducting private or personal for-profit activities. This includes use for private purposes such as business transactions, private advertising of products or services, and any activity meant to foster personal gain;
- Conducting unauthorized not-for-profit business activities;
- Conducting any illegal activities as defined by federal, state, and local laws or
- regulations;
- Creation, accessing or transmitting sexually explicit, obscene, or pornographic material;
- Creation, accessing or transmitting material that could be considered discriminatory, offensive, threatening, harassing, or intimidating;
- Creation, accessing, or participation in online gambling;
- Infringement of any copyright, trademark, patent or other intellectual property rights;
- Performing any activity that could cause the loss, corruption of or prevention of rightful access to data or

the degradation of system/network performance;

- Conducting any activity or solicitation for political or religious causes;
- Unauthorized distribution of state data and information;
- Attempts to subvert the security of any state or other network or network
- resources;
- Use of another employee's access for any reason unless explicitly authorized;
- Attempts to modify or remove computer equipment, software, or peripherals without proper authorization.
- Attempts to libel or otherwise defame any person

Incident

1) An unplanned interruption to an IT Service or a reduction in the quality of an IT Service. Failure of a configuration item that has not yet impacted service is also an incident. For example failure of one disk from a mirror set. (ITIL® V3, Service Operation)
2) A violation of security policy and /or controls (FISMA)
3) A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices which may include, but are not limited to: widespread infections from virus, worms, Trojan horse or other malicious code; unauthorized use of computer accounts and computer systems; unauthorized, intentional or inadvertent disclosure or modification of sensitive/critical data or infrastructure; intentional disruption of critical system functionality; intentional or inadvertent penetration of firewall; compromise of any server, including Web server defacement; exploitation of other weaknesses; child pornography; attempts to obtain information to commit fraud or otherwise prevent critical operations or cause danger to state or national security; and violations of the State security policies or standards that threaten or compromise the security objectives of the State's data, technology or communications systems.

Incident Management

(1)The process responsible for managing the lifecycle of all incidents. The primary objective of Incident Management is to return the IT Service to users as quickly as possible. (ITIL® V3, Service Operation)
(2) The process of detecting, mitigating, and analyzing threats or violations of security policies and controls and limiting their effect
(3) A systematic approach to preventing incidents in an information security infrastructure; responding to incidents when they occur and reporting incidents to the proper escalation points

Incident Record - A record containing the details of an incident. Each incident record documents the lifecycle of a single incident. (ITIL® V3, Service Operation)

Incident Response Plan (Security) - A method for preventing, monitoring, detecting, containing, responding, recovering, reporting and escalating threats or violations of security policy and/or controls and limiting their affects to the organization.

Independent Project Oversight - A process that employs a variety of quality control, inspection, test measurement, and other observation processes to ensure that project objectives are achieved in accordance with an approved plan. Project oversight is usually done by an independent entity (separate from the project team) trained or experienced in a variety of management and technical review methods. Project oversight includes both technical and management oversight

Independent Verification and Validation (IV&V) – A review (or audit) that is performed by an organization that is technically, managerially, and financially independent of the development organization. A quality assurance process carried out by an independent third party

Information Security - The concepts, techniques, technical measures, and administrative measures used to protect information assets from deliberate or inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification, loss, or use (SEI)

Information Security Governance - Development, maintenance and enforcement of security polices, standards, guidelines, processes and procedures

Information Security Infrastructure – the interconnected elements (people, policies, processes, procedures and technology), that provide the framework to support an organizations security philosophy regarding their assets and effectively meeting their business objectives

Information Security Management (ISM) - The process that ensures the confidentiality, integrity and availability of an organization's assets, information, data and IT Services. Information Security Management usually forms part of an organizational approach to Security Management which has a wider scope than the IT service provider, and includes handling of paper, building access, phone calls etc., for the entire organization. (ITIL® V3, Service Design)

Information Security Management System (ISMS) - The framework of policy, processes, standards, guidelines and tools that ensures an organization can achieve its Information Security Management Objectives. (ITIL® V3, Service Design)

Information Security Policy - A policy that governs the organization's approach to Information Security Management. (ITIL® V3, Service Design)

Information System - The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. Information systems include non-financial, financial, and mixed systems. (GAO)

Information System Security Plan - System Security plans are living documents that are developed, reviewed and updated throughout the systems lifecycle to accurately reflect the current state of the information system.

Information Technology (IT) - The hardware and software operated by an organization to support the flow or processing of information in support of business activities, regardless of the technology involved, whether computers, telecommunications, or other. For the State of Georgia Agency projects, Information Technology means telecommunications, automated data processing, databases, the Internet, management information systems, and related information, equipment, goods, and services

Information Technology Resources or IT Resources means hardware, software, and communications equipment, including, but not limited to, personal computers, email, internet, mainframes, wide and local area networks, servers, mobile or portable computers, peripheral equipment, telephones, wireless communications, public safety radio services, facsimile machines, technology facilities (including but not limited to: data centers, dedicated training facilities, and switching facilities), and other relevant hardware and software items as well as personnel tasked with the planning, implementation, and support of technology

Infrastructure Service - An IT Service that is not directly used by the business, but is required by the IT Service provider so they can provide other IT Services. For example, directory services, naming services, or communication services. (ITIL® V3)

Initial Risk Identification - The process during the initial concept phase of identifying risks that might impact a project. The risk identification process is recommended for agencies to evaluate a project

Initiation Stage – The 1st stage in the Plan step of the EPLC. In this stage, the project identifies high level business and functional requirements that are required to develop the product(s)/services(s) and estimates the overall benefits of the proposed investment. ("Enterprise Performance Life Cycle Management" Guideline, published by GTAs Enterprise Project management Office)

Installation and Checkout Phase (Software Application Projects) - The period of time in the software life cycle during which a software product is integrated into its operational environment and tested in this environment to ensure it performs as required. (SEI)

Intangible Benefits – Benefits that are difficult to measure and quantify. Intangible benefits include such things as customer retention, employee retention, and improved customer service

Intangible Costs - Costs that are difficult to measure and quantify. Intangible costs include such things as lost performance and efficiency while the users are getting acquainted with the new system

Integration Management –
(1) This is the 1st o f 9 PMI standard *Knowledge Areas.* The recommended processes ensure that the various parts of the project are coordinated into a coherent whole. The recommended processes are: Develop Project Charter, Develop Preliminary Scope Statement, Develop Project Management Plan, Direct and Manage Project Execution, Monitor and Control Project Work, Integrated Change Control, Close Project
(2) Includes the process and activities needed to identify, define, combine, unify and coordinate the various processes and project management activities within the Project Management Process Groups. (PMBOK 3RD EDITION)

Integration Testing (Software Application Projects) –
(1) Testing in which software components, hardware components, or both are combined and tested to evaluate the interaction between them (SEI)
(2) Also includes testing with 3rd party software that interface back to an agency owned application

Integrity - A security principle that ensures data and configuration items are only modified by authorized personnel and activities. Integrity considers all possible causes of modification, including software and hardware failure, environmental events, and human intervention. (ITIL® V3, Service Design)

Interfaces Design (Software Application Projects) - The activity concerned with the interfaces of the software system contained in the software requirements and software interface requirements documentation. Consolidates the interface descriptions into a single interface description of the software system. (SEI)

Intermediate Recovery - A recovery option which is also known as Warm Standby. Provision is made to recover the IT Service in a period of time between 24 and 72 hours. Intermediate Recovery typically uses a shared portable or fixed facility that has computer systems and network components. The hardware and software will need to be configured, and data will need to be restored, as part of the IT Service Continuity Plan. (ITIL® V3, Service Design)

Internet Service Provider (ISP) - An External Service Provider that provides access to the Internet. Some ISPs also provide other IT Services such as web hosting. (ITIL® V3)

Investment - The term "investment" is meant to be all inclusive of an information technology solution in that it can consist of a single project, or of several logically related projects

Invitation for Bids (IFB) - A document, containing or incorporating by reference, the specifications or scope of work and all contractual terms and conditions that is used to solicit written bids for a specific requirement for goods or nonprofessional services. This type of solicitation is also referred to as an Invitation to Bid or Request for Proposal (RFP)

IP (Internet Protocol) - IP is the computer networking protocol used on the Internet and is used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol suite and has the task for delivering distinguished protocol data-grams (packets) from the source host to the destination host solely based on their addresses

Issue –
1) A topic of discussion, general concern, or legal dispute.
2) A condition that exists or may exist that could change the assumptions, requirements, or constraints for the project, or that could cause re-evaluation of the project's processes.
3) An item that may constrain some or all of the activities of a project.

IT Contingency Planning - The dynamic development of a coordinated recovery strategy for IT systems (major application or general support system), operations, and data after a disruption

IT Governing Body - The term is relative to the risk, complexity and cost of an investment. For major State investments and critical projects, the IT governing body will be the State Critical Project Panel. For delegated projects, an IT governing body organization may be designated by the Business Owner

IT Infrastructure - All of the hardware, software, networks, facilities etc. that are required to develop, test, deliver, monitor, control or support IT Services. The term IT Infrastructure includes all of the Information Technology but not the associated people, processes and documentation. (ITIL® V3)

IT Investment - The term "investment" is meant to be all inclusive of information technology solution in that it can consist of a single project, or of several logically related projects

IT Operations - Activities carried out by IT Operations Control, including console management, job scheduling, backup and restore, and print and output management. IT Operations is also used as a synonym for Service Operation. (ITIL® V3, Service Operation)

IT Service - A Service provided to one or more customers by an IT Service Provider. An IT Service is based on the use of Information Technology and supports the customer's business processes. An IT Service is made up from a combination of people, processes and technology and should be defined in a Service Level Agreement. (ITIL® V3)

IT Service Continuity Management (ITSCM) - The process responsible for managing risks that could seriously impact IT Services. ITSCM ensures that the IT Service Provider can always provide minimum agreed Service Levels, by reducing the risk to an acceptable level and planning for the recovery of IT Services. ITSCM should be designed to support Business Continuity Management. (ITIL® V3, Service Design)

IT Service Continuity Plan - A Plan defining the steps required to recover one or more IT Services. The plan will also identify the triggers for invocation, people to be involved, communications etc. The IT Service Continuity Plan should be part of a Business Continuity Plan. (ITIL® V3, Service Design)

IT Service Management (ITSM) - The implementation and management of quality IT Services that meet the needs of the business. IT Service Management is performed by IT Service Providers through an appropriate mix of people, process and information technology. (ITIL® V3**)**

IT Service Provider - A Service Provider that provides IT Services to internal customers or external customers. (ITIL® V3, Service Strategy)

IT System: An IT system is a discrete set of information resources (workstations, servers, applications, network, etc) working together for the collection, processing, maintenance, use, sharing, dissemination, or disposition of

information. Operational systems are those IT systems that are readily available, in use and actively supporting the business. It is also common in the industry nomenclature to call these systems "production systems".

IT as a Service: Services, which are information technology based, utilizing IT assets that are owned, delivered and managed remotely by one or more providers. Services based on common assets (code, platform, and/or infrastructure) that are consumed in a one-to-many model by all contracted customers anytime, typically on a pay-for-use basis, or as a subscription based on use metrics

ITIL - A set of best practice guidance for IT Service Management. Information Technology Infrastructure Library (ITIL) is owned by the British Office of Government Commerce and consists of a series of publications giving guidance on the provision of quality IT services, and on the processes and facilities needed to support them. (ITIL® V3)

IT Strategic Plan - A document which aligns IT strategy and investments with organizational business priorities, goals, and objectives

IT Strategic Planning (ITSP)- An Information Systems-based planning methodology that looks at IT resources and projects as capital investments and forms a foundation for the selection, control and evaluation of IT resources and projects as part of a business-driven technology portfolio

J

Job Scheduling - Planning and managing the execution of software tasks that are required as part of an IT Service. Job scheduling is carried out by IT Operations Management, and is often automated using software tools that run batch or online tasks at specific times of the day, week, month or year. (ITIL® V3, Service Operation)

K

Key Performance Indicator (KPI) - A metric that is used to help manage a process, IT Service or activity. Many metrics may be measured, but only the most important of these are defined as KPIs and used to actively manage and report on the process, IT Service or activity. KPIs should be selected to ensure that efficiency, effectiveness, and cost effectiveness are all managed. (ITIL® V3, Continual Service Improvement)

Key Stakeholders - Stakeholders are individuals with vested interests in the success of the technology investment. Certain stakeholders are considered Key Stakeholders or critical partners because of their expertise and/or roles in the reviews and governance of the investment. Their participation in a project is to ensure compliance with policies, standards, best practices, legislative requirements and environmental limitations. Their contributions are on behalf of and at the request of the Business Owner, as needed and based on their respective areas of expertise. Because organizational structures vary in the Agencies, the expertise for these roles may be fulfilled from a mixture of organizations, as appropriate. Key Stakeholder roles include:

- Strategic Planner
- Technology Architect
- Information Security Officer
- Procurement Officer
- Budget/Finance Officer
- Workforce/HR, and
- Representatives of non-agency groups such as federal authorities or Georgia's Office of Planning & Budget, Georgia Technology Authority, Department of Administrative Services, State Personnel Agency, and State Accounting Office.

Knowingly Accepted Risks - The Business Owner is ultimately responsible for ensuring appropriate confidentiality, integrity, and availability of IT systems and information needed to support the business. He/she must be fully aware of the risks associated with operating an information system or application that supports his/her business area and has taken the necessary steps to either mitigate those risks or accept them

Known Error - A problem that has a documented root cause and a workaround. Known Errors are created and managed throughout their lifecycle by Problem Management. Known Errors may also be identified by development or suppliers. (ITIL® V3, Service Operation)

Known Error Database (KEDB) - A database containing all Known Error Records. This database is created by Problem Management and used by Incident and Problem Management. The Known Error Database is part of the Service Knowledge Management System. (ITIL® V3, Service Operation)

Known Error Record - A record containing the details of a Known Error. Each Known Error Record documents the lifecycle of a Known Error, including the status, root cause and workaround. In some implementations a Known Error is documented using additional fields in a Problem Record. (ITIL® V3, Service Operation)

L

Lag - A modification of a logical relationship that directs a delay in the successor activity. For example, in a finish-to-start dependency with a 10-day lag, the successor activity cannot start until ten days after the predecessor activity has finished. (PMBOK 3RD EDITION)

LAN - A Local Area Network is a private wiring network. LANs often only serve a single agency or office

Late Finish Date (LF) - In the critical path method, the latest possible point in time that a schedule activity may be completed based upon the schedule network logic, the project completion date, and any constraints assigned to the schedule activities without violating a schedule constraint or delaying the project completion date. The late finish dates are determined during the backward pass calculation of the project schedule network. (PMBOK 3RD EDITION)

Late Start Date (LS) - In the critical path method, the latest possible point in time that a schedule activity may begin based upon the schedule network logic, the project completion date, and any constraints assigned to the schedule activities without violating a schedule constraint or delaying the project completion date. The late start dates are determined during the backward pass calculation of the project schedule network. (PMBOK 3RD EDITION)

Lead – A modification of a logical relationship that allows an acceleration of the successor activity. For example, in a finish-to-start dependency with a ten-day lead, the successor activity can start ten days before the predecessor has finished. (PMBOK 3RD EDITION)

Least Privilege or **Principle of Least Privilege** refers to assigning access rights that provide the most restrictive access or provides no more access to systems or information than is necessary to perform one's official duties

Legitimate Security Issue - Any incident that upon examination is determined to be an inadvertent or intentional violation of management, operational and/or technical security policies

Lessons Learned – The learning gained from the process of performing the project. Lessons learned may be identified at any point. Also considered a project record, to be included in the lessons learned knowledge base. (PMBOK 3RD EDITION)

Lifecycle - The various stages in the life of an IT Service, configuration item, incident, problem, change etc. The lifecycle defines the categories for status and the status transitions that are permitted. (**ITIL® V3)** For example:

- The lifecycle of an application includes requirements, design, build, deploy, operate, optimize.
- The Expanded Incident Lifecycle includes detect, respond, diagnose, repair, recover, restore.
- The lifecycle of a server may include: ordered, received, In Test, live, disposed etc.

Life-Cycle Cost - The overall estimated cost for a particular object over the time corresponding to the life of the object, including direct and indirect initial costs plus any periodic or continuing costs for operation and maintenance. (GAO)

Live - Refers to an IT Service or configuration item that is being used to deliver service to a customer. (ITIL® V3, Service Transition)

Live Environment - A controlled environment containing live configuration items used to deliver IT Services to customers. (ITIL® V3, Service Transition)

LOE (Level of Effort)- A high level estimate/measurement for the amount of work performance required to complete a project or project activity

Log - A record of the events occurring within an organization's systems and networks

Log Archive - Retaining logs for an extended period of time, typically on removable media, a storage area network (SAN), or a specialized log archival appliance or server

Log Analysis - Studying log entries to identify events of interest or suppress log entries for insignificant events

Log Management Infrastructure - Consists of the hardware, software, networks and media used to generate, transmit, store, analyze, and dispose of log data

Logical Access is the ability to read, write, or execute records or data contained in the information system

Logical Relationship - A dependency between two project schedule activities, or between a project schedule activity and a schedule milestone. The four possible types of logical relationships are: Finish-to-start, Finish-to-finish, Start-to-start, and Start-to-finish. (PMBOK 3RD EDITION)

M

Maintenance Control (Software Application Projects) - The cost of planning and scheduling hardware preventive maintenance, and software maintenance and upgrades, managing the hardware and software baselines, and providing response for hardware corrective maintenance

Maintenance- Routine activities performed on hardware or software application to enable it to be stable, prevent future issues and remain in compliance.

Maintainability - (ITIL® V3, Service Design)
(1) A measure of how quickly and effectively a configuration item or IT Service can be restored to normal working after a failure. Maintainability is often measured and reported as mean time to restore service
(2) The mean ability to be changed or repaired easily

Major Incident - The highest category of impact for an incident. A Major Incident results in significant disruption to the business. (ITIL® V3, Service Operation)

Major IT Project - For the State of Georgia Agency projects, Major IT Projects means any state agency information technology project that is: 1) is mission critical, 2) has statewide application, or 3) has a total estimated cost of more than $1 million

Malware, malicious code, malicious software - refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim. Major forms of malware include but are not limited to: viruses, virus hoaxes, worms, Trojan Horses, malicious mobile code, blended attacks, spyware, attacker backdoors and toolkits.

- Spyware is malware intended to violate a user's privacy and monitor personal activities and conduct financial fraud.
- Phishing is a non-malware threat that is often associated with malware, such as using deceptive computer-based means to trick individuals into disclosing sensitive information.
- Virus hoaxes are false warnings of new malware threats.

Managed Services - (ITIL® V3, Service Strategy)
(1) A perspective on IT Services which emphasizes the fact that they are managed
(2) A synonym for outsourced IT Services

Management System - The framework of policy, processes and functions that ensures an organization can achieve its objectives. (ITIL® V3)

Manual Workaround - A workaround that requires manual intervention. Manual workaround is also used as the name of a recovery option in which the business process operates without the use of IT Services. This is a temporary measure and is usually combined with another recovery option. (ITIL® V3)

Mandatory Projects- Projects that support legal or regulatory requirements such as Executive orders, state legislation, or Federal mandates

Master Schedule – A summary-level project schedule that identifies the major deliverables and work breakdown structure components and key schedule milestones. (PMBOK 3RD EDITION)

Matrix Organization - Any organizational structure in which the project manager shares responsibility with the functional managers for assigning priorities and for directing the work of persons assigned to the project. (PMBOK 3RD EDITION)

Maturity - A measure of the reliability, efficiency and effectiveness of a process, function, organization etc. The most mature processes and functions are formally aligned to business objectives and strategy, and are supported by a framework for continual improvement. (ITIL® V3, Continual Service Improvement)

Maturity Level - A named level in a Maturity model

Mean Time Between Failures (MTBF) - A Metric for measuring and reporting reliability. MTBF is the average time that a configuration item or IT Service can perform its agreed function without interruption. This is measured from when the CI or IT Service starts working, until it next fails. (ITIL® V3, Service Design)

Mean Time Between Service Incidents (MTBSI) - A metric used for measuring and reporting reliability. MTBSI is the mean time from when a system or IT Service fails, until it next fails. MTBSI is equal to MTBF + MTRS. (ITIL® V3, Service Design)

Mean Time To Repair (MTTR) - The average time taken to repair a configuration item or IT Service after a failure. MTTR is measured from when the CI or IT Service fails until it is repaired. MTTR does not include the time required

to recover or restore. MTTR is sometimes incorrectly used to mean Mean Time to Restore Service. (ITIL® V3, Service Design)

Mean Time to Restore Service (MTRS) - The average time taken to restore a configuration item or IT Service after a failure. MTRS is measured from when the CI or IT Service fails until it is fully restored and delivering its normal functionality. (ITIL® V3, Service Design)

Meta-architecture - A set of high-level decisions that will strongly influence the structure of the system, but is not itself the structure of the system. The meta-architecture, through style, patterns of composition or interaction, principles, and philosophy, rules certain structural choices out, and guides selection decisions and trade-offs among others. By choosing communication or co-ordination mechanisms that are repeatedly applied across the architecture, a consistent approach is ensured and this simplifies the architecture

Methodology - The processes, policies, and guidelines that are included as part of the framework for project management

Metric
(1) Something that is measured and reported to help manage a process, IT Service or activity. (ITIL® V3, Continual Service Improvement)
(2) Numeric Indicators used to gauge state-wide program performance and monitor progress toward accomplishing state-wide goals and objectives. Monitors and measures accomplishment of goals by quantifying the level of implementation and effectiveness

Middleware - Software that connects two or more software components or applications. Middleware is usually purchased from a supplier, rather than developed within the IT Service Provider. (ITIL® V3, Service Design)

Milestone - A significant point or event in the project. (PMBOK 3RD EDITION)

Mission Critical Processes or Functions - The critical or primary operational and/or business support functions that could NOT be interrupted or unavailable for more than a mandated or predetermined timeframe without significantly jeopardizing an agency's ability to perform its primary mission. An example of a business function is a logical grouping of processes/activities that produce a product and/or service such as accounting, payroll, tax processing, customer service, etc.

Mission Statement - The Mission Statement of an organization is a short but complete description of the overall purpose and intentions of that organization. It states what is to be achieved, but not how this should be done

Mitigate – Dealing with a risk by developing strategies and actions for reducing (or eliminating) the impact, probability, or both, of the risk to some acceptable level. It may also involve shifting the timeframe when action must be taken. (SEI)

Mitigation Plan - An action plan for risks that are to be mitigated. It documents the strategies, actions, goals, schedule dates, tracking requirements, and all other supporting information needed to carry out the mitigation strategy

Mobile Computing - A generic term describing one's ability to use technology 'untethered', that is not physically connected, or in remote or mobile (non-static) environments

Model - An approximation, representation, or idealization of selected aspects of the structure, behavior, operation, or other characteristics of a real-world process, concept, or system. Note: Models may have other models as components - (SEI). Used to help understand or predict future behavior. (ITIL® V3)

Modeling - A technique that is used to predict the future behavior of a system, process, IT Service, configuration item etc. Modeling is commonly used in Financial Management, Capacity Management and Availability Management. (ITIL® V3)

Monitor Control Loop - Monitoring the output of a task, process, IT Service or configuration item; comparing this output to a predefined norm; and taking appropriate action based on this comparison. (ITIL® V3, Service Operation)

Monitoring - Repeated observation of a configuration item, IT Service or process to detect events and to ensure that the current status is known. (ITIL® V3, Service Operation)

N

Net Present Value -- The difference between the discounted present value of benefits and the discounted present value of costs. This is also referred to as the discounted net

Network Management - The execution of the set of functions required for controlling, planning, allocating, deploying, coordinating, and monitoring the resources of a computer network. (SEI)

Network Management Application - Application that provides the ability to monitor and control the network

Network Management Information - Information that is exchanged between the network management station(s) and the management agents that allows the monitoring and control of a managed device

Network Management Protocol - Protocol used by the network management station(s) and the management agent to exchange management information

Network Session – A lasting connection in a network protocol or between a user and a peer, typically a server, usually involving the exchange of many packets between the user's computer and the server

Non-functional Requirement - Non-functional requirements or system qualities capture required properties of the system, such as performance, maintainability, cost, reliability etc. In other words, non-functional requirements capture how well some behavioral or structural aspect of the system should be accomplished. This type of requirement is not expected to be testable

Non-major IT Project – For the State of Georgia Agency projects, Non-major IT Projects are those technology projects with an estimated total project cost of less than $1 million and not deemed to be mission critical or designated as having statewide application by the Chief Information Officer

Non-Public State Information Assets include all data, e-mail, and other information created, accessed, processed, transmitted and/or stored on behalf of or in the conduction of official State business, that is not otherwise publicly accessible either though public facing websites or open records

Non-Repudiation is a service that is used to provide proof of the integrity and origin of data in such a way that the integrity and origin can be verified by a third party

Non-State Technology Devices include but are not limited to: laptops, PDA's, iPods, mp3 players, USB drives, and other portable processing and storage devices not specifically issued or owned by the State of Georgia. Technology devices include but are not limited to laptops, PDAs, mp3 players, ipods, USB drives, and other portable processing and storage devices (regardless of ownership)

O

Off the Shelf - Synonym for Commercial-Off-the-Shelf

Ongoing Support Cost - The periodic and continuing cost to operate and maintain the product or service delivered by the project

Operate - To perform as expected. A process or configuration item is said to operate if it is delivering the required outputs. Operate also means to perform one or more operations. For example, to operate a computer is to do the day-to-day operations needed for it to perform as expected. (ITIL® V3)

Operation - (ITIL® V3, Service Operation)
(1) Day-to-day management of an IT Service, system, or other configuration item
(2) Any pre-defined activity or transaction, for example, loading a magnetic tape, accepting money at a point of sale, or reading data from a disk drive
(3) The 1st stage of the Run step of the EPLC wherein an IT solution is operated on a day to day basis. This stage may be in effect for several years. ("Enterprise Performance Life Cycle Management" Guideline, published by GTAs Enterprise Project management Office)

Operating System - The core system software running on a hardware platform

Operations and maintenance phase - The period of time in the software life cycle during which a software product is employed in its operational environment, monitored for satisfactory performance, and modified as necessary to correct problems or to respond to changing requirements. (SEI)

Operational Level Agreement (OLA) - An agreement between an IT Service Provider and another part of the same organization. An OLA supports the IT Service Provider's delivery of IT Services to customers. The OLA defines the goods or services to be provided and the responsibilities of both parties. (ITIL® V3, Service Design, Continual Service Improvement)

Operational System - Operational systems are those IT systems that are readily available, in use and actively supporting the business. It is common in the industry to call these systems "Production Systems". Operational systems do not include research, development or test systems

Optimize - Review, plan and request changes, in order to obtain the maximum efficiency and effectiveness from a process, configuration item, application, etc. (ITIL® V3)

Organizational Breakdown Structure (OBS) - A hierarchically organized depiction of the project organization arranged so as to relate the work packages to the performing organizational units. (PMBOK 3RD EDITION)

Organizational Change Management (Projects) – (1) Managing and controlling the workforce structure during the full life cycle of an Agency initiative, program or project. (2) Identifying, documenting, and assigning project roles, responsibilities, and reporting relationships during the full life cycle of an Agency initiative, program or project. Agency 'change control' processes and procedures are used to control project-related workforce structure changes

Organizational Planning - Identifying, documenting, and assigning project roles, responsibilities, and reporting relationships

Outcome - The result of carrying out an activity; following a process; delivering an IT Service etc. The term outcome is used to refer to intended results, as well as to actual results. (ITIL® V3)

Oversight Committee – A body chartered by the Chief Information Officer or an Agency Head to review and make recommendations regarding Major IT projects within that Agency

P

Parallel Testing- The process of feeding test data into two systems, the modified system and an alternative system and comparing results over a specified period of time

Passive Monitoring - Monitoring of a configuration item, an IT Service or a process that relies on an alert or notification to discover the current status. (ITIL® V3, Service Operation)

Path - A set of sequentially connected activities in a project network diagram.

Payback Period -The number of years it takes for the cumulative dollar value of the benefits to exceed the cumulative costs of a project. (GAO)

Percent Complete (PC) - An estimate, expressed as a percent, of the amount of work that has been completed, on an activity or a work breakdown structure component. (PMBOK 3RD EDITION)

Performance - A measure of what is achieved or delivered by a system, person, team, process, or IT Service. (ITIL® V3)

Performance Gap - The gap between what customers and stakeholders expect and what each process and related sub processes produces in terms of quality, quantity, time, and cost of services and products. (GAO)

Performance Goal - The desired results of implementing the security objective or technique that are measured by the metric

Performance Management
(1) The process of developing measurable indicators that can be systematically tracked to assess progress made in achieving predetermined goals and using such indicators to assess progress in achieving these goals. (GAO)
(2) The process responsible for day-to-day Capacity Management Activities. These include monitoring, threshold detection, performance analysis and tuning, and implementing changes related to performance and capacity. (ITIL® V3, Continual Service Improvement)

Performance Measures - The actions required to accomplish the performance goal validated through the completion and analysis of the agency report

Performance testing - Testing conducted to evaluate the compliance of a system or component with specified performance requirements. (SEI)

Personal Information, Personally Identifiable Information (PII) – an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

A. Social Security Number (SSN)
B. Driver's license number or state identification card number
C. Account number, credit or debit card number
D. Account passwords or personal identification numbers (PIN) or other access codes

E. Any of the items A through D when not in connection with the individual's first name or first initial and last name, if the information is sufficient to perform or attempt to perform identity theft of other forms of fraud against the person whose information was compromised.

These terms do not include publicly available information that is lawfully made available to the general public from federal, state, or local government records

Physical Access is the ability to access areas or premises where information systems and technology assets reside.

Pilot - (Service Transition) A limited deployment of an IT Service, a release or a process to the live environment. A Pilot is used to reduce risk and to gain user feedback and acceptance

Plan – (1) An intended future course of action. (2) A major step in the EPLC. ("Enterprise Performance Life Cycle Management" Guideline, published by GTAs Enterprise Project management Office)

Planning Approval – Approval granted by the CIO to proceed with project planning for the project. Specifically, identification of solutions and development of the business case that supports project development approval

Planned Downtime - Agreed time when an IT Service will not be available. Planned downtime is often used for maintenance, upgrades and testing. (ITIL® V3, Service Design)

Planning Stage – The 2nd stage or process in the Plan step of a project life cycle that follows the *Initiation Stage.* It defines activities that will move the Agency's business problem from its' current state to the desired future state. ("Enterprise Performance Life Cycle Management" Guideline, published by GTAs Enterprise Project management Office)

Planned Value – The authorized budget assigned to the scheduled work to be accomplished for a schedule activity or work breakdown structure component. (PMBOK 3RD EDITION)

Platform Architecture - Defines the personal and business computing hardware systems to be used by agencies. The platforms may include servers (e.g., high-end servers and midrange to small servers), storage systems, personal computing devices (desktops, notebooks, and hand-held computing devices), and other hardware (e.g., printers). In addition to platform hardware, the Platform Architecture addresses operating systems, configurations, network and device-to-device interfaces, and selected peripherals (e.g., floppy drives). In the instance of personal computing devices, the architecture also addresses base productivity software, security software, and utilities that are necessary to make the hardware useful to users. The architecture addresses decision criteria and best practices for the acquisition and deployment of platforms. The architecture also identifies management and remote access components, which are critical to platform use. Details regarding management components are addressed in the Systems Management Domain

Platforms – Personal computing devices, servers, and/or storage systems. The type of computing hardware that an application runs on

PMBOK - A project management standard maintained and published by the Project Management Institute. PMBOK stands for Project Management Body of Knowledge. See http://www.pmi.org/ for more information

Policy - Formally documented management expectations and intentions. Policies are used to direct decisions, and to ensure consistent and appropriate development and implementation of processes, standards, roles, activities, IT infrastructure etc.

Portfolio – A collection of projects or programs and other work that are grouped together to facilitate effective management of that work to meet strategic business objectives. The projects or programs of the portfolio may not necessarily be interdependent or directly related. (PMBOK 3RD EDITION)

Portfolio Management – The centralized management of one or more portfolios, which includes identifying, prioritizing, authorizing, managing, and controlling projects, programs, and other related work, to achieve specific strategic business objectives. (PMBOK 3RD EDITION)

Positive User Identification is the validation of user requesting and being granted access credentials to non-public state information resources

Post Implementation Report - Documents the successes and failures of a project and suggest follow up actions. It provides a historical record of the planned and actual budget and schedule. Other selected metrics on the project can also be collected, based upon state organization procedures. The report also contains recommendations for other projects of similar size and scope

Post-implementation Review (PIR) - An evaluation tool that compares the conditions before the implementation of a project (as identified in the business case) or change with the actual results achieved by the project or change. The PIR determines if the change or project was successful, and identifies opportunities for improvement

Predecessor - A task or project whose start or end date determines the start or end date of another project or task

Priority - A category used to identify the relative importance of an incident, problem or change. Priority is based on impact and urgency, and is used to identify required times for actions to be taken. For example the SLA may state that Priority2 Incidents must be resolved within 12 hours. ((ITIL® V3, Service Transition, Service Operation)

Privacy Officer - An individual within an agency with specialized expertise regarding IT privacy matters whose responsibility entails ensuring awareness of data privacy issues and compliance with regulation, legislation and policy

Proactive Monitoring - Monitoring that looks for patterns of events to predict possible future failures. (ITIL® V3, Service Operation)

Proactive Problem Management - Part of the Problem Management Process. The objective of Proactive Problem Management is to identify problems that might otherwise be missed. Proactive Problem Management analyzes incident records, and uses data collected by other IT Service Management processes to identify trends or significant problems. (ITIL® V3, Service Operation)

Problem - A cause of one or more incidents. The cause is not usually known at the time a problem record is created, and the Problem Management Process is responsible for further investigation. (ITIL® V3, Service Operation)

Problem Management - The process responsible for managing the lifecycle of all problems. The primary objectives of problem management are to prevent incidents from happening, and to minimize the impact of incidents that cannot be prevented. (ITIL® V3, Service Operation)

Problem Record - A record containing the details of a problem. Each problem record documents the lifecycle of a single problem. (ITIL® V3, Service Operation)

Procedure - A document containing steps that specify how to achieve an activity. Procedures are defined as part of processes. (ITIL® V3)

Process - A structured set of activities designed to accomplish a specific objective. A process takes one or more defined inputs and turns them into defined outputs. A process may include any of the roles, responsibilities, tools and management Controls required to reliably deliver the outputs. A process may include policies, standards, guidelines, activities, and work instructions if they are needed

Process Control - The activity of planning and regulating a process, with the objective of performing the process in an effective, efficient, and consistent manner. (ITIL® V3)

Process Manager - A role responsible for operational management of a process. The Process Manager's responsibilities include planning and co-ordination of all activities required to carry out, monitor and report on the process. There may be several Process Managers for one process, for example regional Change Managers or IT Service Continuity Managers for each data center. The Process Manager role is often assigned to the person who carries out the Process Owner role, but the two roles may be separate in larger organizations. (ITIL® V3)

Process Management –
(1) the collection of activities of planning and monitoring the performance of a process, especially activities involved with business processes, often confused with reengineering.
(2) The application of knowledge, skills, tools, techniques and systems to define, visualize, measure, control, report and improve processes with the goal to meet customer requirements. It is different from program management in that program management is concerned with managing a group of inter-dependent projects.
(3) The adoption of a process approach when developing, implementing and improving the effectiveness of a quality management system, to enhance customer satisfaction by meeting customer requirements.

Process Owner - A role responsible for ensuring that a process is Fit for Purpose. The Process Owner's responsibilities include sponsorship, design, change management and continual improvement of the process and its metrics. This role is often assigned to the same person who carries out the Process Manager role, but the two roles may be separate in larger organizations. (ITIL® V3)

Procurement - The procedures for obtaining goods or services, including all activities from the planning steps and preparation and processing of a requisition, through receipt and acceptance of delivery and processing of a final invoice for payment

Procurement Cost - The total estimated cost of the goods or services being purchased

Product - General terms used to define the result of a project delivered to a customer

Product Description Statement - A non-formal, high-level document that describes the characteristics of the product/process to be created

Production Environment - Synonym for Live Environment.

Production Support- The processes of supporting the IT hardware and software/applications which are currently being used by the end users. This includes, but is not limited to, tasks such as development of solutions for fixing system issues, troubleshooting, and root cause analysis

Production System - Production systems are those IT systems that are readily available, in use and actively supporting the business. It is common in the industry to call these systems "Operational Systems". Production systems do not include research, development or test systems

Program – (PMBOK 3RD EDITION).
(1) A group of related projects managed in a coordinated way to obtain benefits and control not available from managing them individually. Programs may include elements of related work outside of the scope of the discrete projects in the program
(2) To write the lines of code in a program
(3) A collection of instructions that tell the computer what to do. A program is generically known as "software" and the programs users work with, such as word processors and spreadsheets, are called "applications" or "application programs." Thus, the terms software, application, program and instruction are synonymous in the sense that they all tell the computer what to do
(4) An investment composed of multiple projects in an ongoing implementation. It may apply to new solutions, major enhancements to existing solutions, high-priority, fast track projects, commercial off the shelf (COTS) products acquisitions, major telecommunications projects and infrastructure projects

Program Code or Subprogram Name – (Budget Identification Information) The name/s of the budgeted program/s and/or subprogram/s (as used in the State budget terminology) under which the application is funded

Program Evaluation and Review Technique (PERT) - An event-oriented network analysis technique used to estimate project duration when there is a high degree of uncertainty with the individual activity duration estimates. PERT applies the critical path method to a weighted average duration estimate

Program Management - (PMBOK 3RD EDITION)
(1) The 2nd of 9 PMI standard *Knowledge Areas*. The recommended processes ensure that the projects include all of the work required to complete the project successfully. The recommended processes are: Scope Planning, Scope Definition, Create WBS, Scope Verification, and Scope Control
(2) The application of knowledge, skills, tools, and techniques to project activities to meet the project requirements

Program Management Office (PMO) –
(1) An organization that oversees and/or mentors groups of projects. Often the PMO is responsible for establishing policies and standards for the projects/organization, reviewing and consolidating project reports for external stakeholders, and monitoring project performance against the organization's standards
(2) A project management office (PMO), a project office, and a program management office (PMO) may be the same group in some agencies, performing similar activities

Program Management Plan (PMP) -
(1) At minimum, a documented statement of the intended actions an agency will take in pursuit of a project's goals and objectives
(2) A comprehensive statement of all key factors guiding a management team in their pursuit of project goals and objectives, the strategy and tactics the team will execute, and other information necessary to understand the project, its products and services, its organizational structures, and its intended actions

Program Manager: The Program Manager is responsible for overall planning, execution and performance of the investment or initiative within approved cost, schedule and performance baselines. ("Enterprise Performance Life Cycle Management" Guideline, published by GTAs Enterprise Project management Office)

Progress Analysis -The evaluation of progress against the approved schedule and the determination of its impact. For cost, this is the development of performance indices

Project - A temporary endeavor undertaken to create a unique product, service or result. (PMBOK 3RD EDITION). Projects differ from operations in that operations are ongoing (no ending) and repetitive

Project Administration - Making Project Plan modifications; may result from such things as: new estimates of work still to be done, changes in scope/functionality of end-product(s), resource changes, and unforeseen circumstances. It includes monitoring the various Execution Phase activities, monitoring risks, status reporting, and reviewing/authorizing project changes as needed

Project Assurance –
(1) A central group within a project-performing agency that provides advice and guidance to project managers. This group may be part of the project management office (PMO) when a PMO exists in an agency
(2) In agencies with program managers and no project assurance group, the program managers perform the project assurance role with the 'primary project manager' (refer to definition in the Glossary). Several projects may be involved in internal and/or external agencies; there should be a 'primary project manager' who acts as a 'central liaison' for the program manager
(3) The project assurance group conducts reviews of projects not so much to establish their conformance to standards, but to assess their health (GREEN, YELLOW, RED, GRAY), the likelihood of the projects to achieve declared commitments, and to recommend remedial action where necessary
(4) The project assurance group collects and reports review results to management in monthly (pre-defined) detail and summary-level reports from project managers and program managers. Prior to distributing reports, they are merged by this group ('rolled-up' to the summary level) for management distribution, per pre-defined requirements and schedules

Project assurance is not expensive. It requires perhaps one full time person for every hundred people involved in project work. However, they must be empowered by senior management to exercise project assurance *on their, the senior managers', behalf*. They must be able to call on others to conduct, for example, project Health Checks.

Project Business Objective - A desired result produced by a project that answers or resolves a business problem

Project Change Request (PCR) –
(1) A request to expand or decrease project scope, to modify cost or schedule estimates, etc. Change requests may occur in many forms – oral or written, direct or indirect, externally or internally initiated, and legally mandated or optional. The Project Management Plan should address the process that will be used to manage these requests. This methodology uses a general-purpose form for submitting suggestions for change to the project
(2) The term 'PCR' in Procurement is a *Procurement and Contract Request.* This term is not addressed in the project glossary

Project Charter – A document issued by the project initiator or sponsor that formally authorizes the existence of a project, and provides the project manager with the authority to apply organizational resources to project activities. (PMBOK 3RD EDITION). The Project Charter contains the first agreed upon scope of the project. It should include the business need, product description with business, technical and quality objectives, high level budget and time estimates along with known constraints, assumptions, dependencies and risks

Project Close – The final process in the project management life cycle is the *Project Close Process*. It follows the *Execution Process*. At minimum, close-out activities are:

- Administrative Close – project records and project and team performance information
- Contract Close – Completing the contract file, including records of project deliverables acceptance, vendor performance information, and any other information needed by the procurement officer to close the files
- Transition to ongoing operations – The project is turned over to the appropriate owner, including Lessons learned and other relevant information

Project Concept Document (PCD) - The document that is the foundation for making a decision to initiate a project. It describes the project purpose and presents a preliminary business case for pursuing the project. It gives decision makers the opportunity to determine project viability

Project Cost - The total cost to provide the business driven, technology-based product or service. The costs include the hardware, software, services, installation, management, maintenance, support, training, and internal staffing costs planned for the project. Internal staffing costs are the apportioned salaries and benefits of the project team members

Project Description – An initial, high-level statement describing the purpose, benefits, customer(s), general approach to development and characteristics of a product or service required by the organization

Project Duration - The elapsed time from project start date through to project finish date

Project Execution – The *Project Execution Process* follows the *Project Planning Process* in the project life cycle. *Project Control Process* activities are included in *Project Execution*, but occur across the full project life cycle. It is usually the longest process and typically consumes the most energy and resources. During this process, the Project Management Plan (PMP) is implemented and physical project deliverables are built and presented to the customer for signoff

Project Human Resource Management – Includes the processes that organize and manage the project team. (PMBOK 3RD EDITION)

Project Initiation –
(1) The conceptual development phase of a project; a process that leads to approval of the project concept and authorization (through a Project Charter) to begin detailed planning
(2) *Project Initiation* is the first process of the State of Georgia Agency's project life cycle, represented by the submission of an Agency Project Request (APR) or a Project Internal Request (PIR)

Project Life Cycle Management –
(1) The processes of initiating, planning, executing, controlling, and closing a project that describe, organize, and complete the work of the project/product. Project management processes and project/product-oriented processes overlap and interact throughout the project. The conclusion of a project phase is generally marked by a review of both key deliverables and project performance. The project/product life cycle serves to define the beginning and end of the project
(2) For software development and implementation project life cycle phases, processes, and other related terms, refer to the SEI glossary located on the Software Engineering Institute (SEI) site

Project Management Institute (PMI) - A non-profit organization for the promotion of project management knowledge

Project Manager (or Project Management Officer) **-** The person assigned by the performing organization to achieve the project objectives. (PMBOK 3RD EDITION).
(1) The individual who directs, controls, administers, and regulates a project
(2) The project manager is the individual ultimately responsible to the customer
(3) The individual responsible for managing a project
(4) The individual responsible for tracking agency projects and applications

Project Measures of Success - The measurable, business-oriented indicators that will be used to assess progress made in achieving planned project objectives

Project Office (PO) - The group responsible for project delivery, including administrative, financial, contract, technical and quality assurance staff. The project office may oversee a contractor who is performing the primary activities (planning, development, etc.)

Project Oversight - A process that employs a variety of quality control, inspection, test measurement, and other observation processes to ensure that planned project objectives are achieved in accordance with an approved plan. Project oversight includes both technical and management oversight. Project oversight is usually done by an independent entity (separate from the project team) trained or experienced in a variety of management and technical review methods

Project Phase –
(1) A collection of logically related project activities, usually culminating in the completion of a major deliverable. (PMBOK 3RD EDITION)
(2) Some of the 'standard' PMI processes (e.g., concept, initiation, planning, execution, control and closing) are sometimes used in work breakdown structures (WBS's) as project phases

Project Plan - A formal, approved document used to guide both project execution and project control. The primary uses of the Project Plan are to document planning assumptions, decisions and project baselines; facilitate communication among stakeholders; and, essentially describe how the project will be executed and controlled

Project Planning – Activities to conduct effective initial analysis of business needs and potentially useful technologies required for development of a detailed business case, incorporating a comprehensive definition of scope and supported by sound financial and cost based analysis

Project Procurement Management - Includes the processes to purchase or acquire the products, services, or results needed from outside the project team to perform the work. (PMBOK 3RD EDITION)

Project Quality Management - Includes the processes and activities of the performing organization that determine quality policies, objectives, and responsibilities so that the project will satisfy the needs for which it was undertaken. (PMBOK 3RD EDITION)

Project Repository - The set of reference materials and historical project assets maintained by the Project/Program Management Office (PMO) as a knowledge repository for project management

Project Risk Management -Includes the processes concerned with conducting risk management planning, identification, analysis, responses, and monitoring and control on a project. (PMBOK 3RD EDITION)

Project Schedule -The planned dates for performing schedule activities and the planned dates for meeting schedule milestones. (PMBOK 3RD EDITION)

Project Scope Management - Includes the processes required to ensure that the project includes all the work required, and only the work required, to complete the project successfully. (PMBOK 3RD EDITION)

Project Status Report - A report that summarizes the status of the project in written or verbal form. It should contain enough information to give the reader a good view of the health of the project. These reports are usually prepared and distributed by the project manager and distributed to project teams weekly and summarized for senior management monthly

Project Time Management -Includes the processes required to accomplish timely completion of the project. (PMBOK 3RD EDITION)

Project Transition Checklist -A document that ensures that the activities of a Phase have been finished, reviewed, and signed off so the project may move from one Phase into the next

Projected Service Outage (PSO) - A document that identifies the effect of planned changes, maintenance activities and test plans on agreed Service Levels. (ITIL® V3**,** Service Transition)

Protocol – A set of conventions that govern the interaction of processes, devices, and other components within a system. (SEI)

Q

Qualification - An activity that ensures that IT infrastructure is appropriate, and correctly configured, to support an application or IT Service. (ITIL® V3, Service Transition)

Qualification Phase (Software Application Projects) - The period of time in the software life cycle during which it is determined whether a system or component is suitable for operational use.

Quality –
(1) A composite of attributes (including performance features and characteristics) of the product, process, or service required to satisfy the need for which the project is undertaken
(2) The ability of a product, service, or process to provide the intended value
(3) Process quality requires an ability to monitor effectiveness and efficiency, and to improve them if necessary

Quality Assurance (QA) -
(1) The process of evaluating overall project performance on a regular basis to provide confidence that the project will satisfy the relevant quality standards
(2) The function that ensures a project operates in a controlled environment that ensures the products and activities of the team comply with the following principles: Objective verification ensures products and activities adhere to applicable standards, guidelines, and requirements; affected groups and individuals are informed of project quality assurance activities and results; management addresses noncompliance issues that cannot be resolved within the project; and Quality Assurance activities are planned
(3) The organizational unit that is assigned responsibility for quality assurance

Quality Assurance Plan (QAP) - A plan outlining the expectation of a project regarding quality of deliverables, quality expectations of the project team, and the quality expectations of resources used to support the project. An essential part of the Project Management Plan

Quality Control (QC) - (1) The process of monitoring specific project results to determine if they comply with relevant quality standards and identifying ways to eliminate causes of unsatisfactory performance. (2) The organizational unit that is assigned responsibility for quality control

Quality Management –
(1) The 5th of nine PMI standard *Knowledge Areas*. The recommended processes ensure that the project will satisfy the needs for which it was undertaken. The recommended processes in Quality Management are: Quality Planning, Perform Quality Assurance, and Perform Quality Control
(2) A collection of quality policies, plans, procedures, specifications, and requirements is attained through quality assurance (managerial) and quality control (technical)
(3) The set of processes responsible for ensuring that all work carried out by an organization is of a suitable quality to reliably meet business objectives or service levels. (ITIL® V3)

Quality Management Plan- The Quality Management Plan defines the acceptable level of quality as defined by the Business Owner or customer. It further defines how a project will ensure the level of quality in its deliverables and work processes. The quality management activities look to ensure that:

- Products meet agreed upon standards and requirements
- Processes and procedures are performed as documented
- Any non-conformance identified follows the appropriate corrective action

Quality Planning - The process of identifying which quality standards are relevant to the project and determining how to satisfy them. (PMBOK 3RD EDITION)

R

RACI - A Model used to help define roles and responsibilities. RACI stands for Responsible, Accountable, Consulted and Informed. (ITIL® V3, Service Design, Continual Service Improvement)

Reactive Monitoring - Monitoring that takes action in response to an event. For example submitting a batch job when the previous job completes, or logging an incident when an error occurs. (ITIL® V3, Service Operation)

Reciprocal Arrangement - A recovery option. An agreement between two organizations to share resources in an emergency. For example, computer room space or use of a mainframe. (ITIL® V3, Service Design)

Record

(1) A document containing the results or other output from a process or activity. Records are evidence of the fact that an activity took place and may be paper or electronic. For example, an Audit report, an Incident Record, or the minutes of a meeting. (ITIL® V3)

(2) Georgia statute defines records as "all documents, papers, letters, maps, books (except books in formally organized libraries), microfilm, magnetic tape, or other material, regardless of physical form or characteristics, made or received pursuant to law or ordinance or in performance of functions by any agency". (Official Code of Georgia Annotated, § 50-18-91[5])

Records Management is the development and implementation of a life-cycle management process from the creation and receipt of records, through their active life, storage, and to their final disposition. According to the Georgia statute "Records management" means the application of management techniques to the creation, utilization, maintenance, retention, preservation, and disposal of records undertaken to reduce costs and improve efficiency of record keeping. "Records management" includes management of filing and microfilming equipment and supplies; filing and information retrieval systems; files, correspondence, reports, and forms management; historical documentation; micrographics; retention programming; and vital records protection

Recovery (Software Application Projects) - The restoration of a system, program, database, or other system resource to a prior state following a failure or externally caused disaster; for example, the restoration of a database to a point at which processing can be resumed following a system failure (SEI). After Recovery, further steps may be needed before the IT Service can be made available to the users (Restoration). (ITIL)

Recovery Option - A strategy for responding to an interruption to service. Commonly used strategies are Do Nothing, Manual Workaround, Reciprocal Arrangement, Gradual Recovery, Intermediate Recovery, Fast Recovery and Immediate Recovery. Recovery Options may make use of dedicated facilities, or Third Party facilities shared by multiple businesses. (ITIL® V3, Service Design)

Recovery Point Objective (RPO) - The maximum amount of data that may be lost when service is restored after an interruption. Recovery Point Objective is expressed as a length of time before the failure. For example a Recovery Point Objective of one day may be supported by daily backups, and up to 24 hours of data may be lost. Recovery Point Objectives for each IT Service should be negotiated, agreed and documented, and used as requirements for Service Design and IT Service Continuity Plans. (ITIL® V3, Service Operation)

Recovery Time Objective (RTO) - (Service Operation) The maximum time allowed for recovery of an IT Service following an interruption. The Service Level to be provided may be less than normal Service Level Targets.

Recovery Time Objectives for each IT Service should be negotiated, agreed and documented. (ITIL® V3, Service Operation)

Redundancy - Synonym for Fault Tolerance. The term Redundant also has a generic meaning of obsolete, or no longer needed. (ITIL® V3, Service Operation)

Relationship - A connection or interaction between two people or things. In Business Relationship Management it is the interaction between the IT Service Provider and the business. In Configuration Management it is a link between two configuration items that identifies a dependency or connection between them. For example Applications may be linked to the Servers they run on, IT Services have many links to all the CIs that contribute to them. (ITIL® V3)

Regression Testing (Software Application Projects) - Selective retesting of a system or component to verify that modifications have not caused unintended effects and that the system or component still complies with its specified requirements. (SEI)

Release - A collection of hardware, software, documentation, processes or other components required to implement one or more approved changes to IT Services. The contents of each release are managed, tested, and deployed as a single entity. (ITIL® V3, Service Transition)

Release and Deployment Management - The process responsible for both Release Management and Deployment. (ITIL® V3, Service Transition)

Release Identification - A naming convention used to uniquely identify a release. The Release Identification typically includes a reference to the Configuration Item and a version number; for example, Microsoft Office 2003 SR2. (ITIL® V3, Service Transition)

Release Management - The process responsible for planning, scheduling and controlling the movement of releases to test and live environments. The primary objective of Release Management is to ensure that the integrity of the live environment is protected and that the correct components are released. Release Management is part of the Release and Deployment Management Process. (ITIL® V3, Service Transition)

Release Record - A record in the CMDB that defines the content of a release. A Release Record has relationships with all configuration items that are affected by the release. (ITIL® V3, Service Transition)

Release Unit - Components of an IT Service that are normally released together. A Release Unit typically includes sufficient components to perform a useful function. For example one Release Unit could be a Desktop PC, including Hardware, Software, Licenses, documentation etc. A different Release Unit may be the complete Payroll Application, including IT Operations Procedures and User training. (ITIL® V3, Service Transition)

Release Window - Synonym for Change Window.

Reliability - A measure of how long a configuration item or IT Service can perform its agreed function without interruption - usually measured as MTBF or MTBSI. The term reliability can also be used to state how likely it is that a process, function etc. will deliver its required outputs. (ITIL® V3, Service Design, Continual Service Improvement)

Remaining Duration (RD) - The time in calendar units, between the data date of the project schedule and the finish date of a schedule activity that has an actual start date. This represents the time needed to complete a schedule activity where the work is in progress. (PMBOK 3RD EDITION)

Remediation - Recovery to a known state after a failed change or release. (ITIL® V3, Service Transition)

Remote Access - The ability of an organization's users to access its non-public computing resources from locations other than the organization's facilities

Repair - The replacement or correction of a failed configuration item. (ITIL® V3, Service Operation)

Request for Change (RFC) - A formal proposal for a change to be made. An RFC includes details of the proposed change, and may be recorded on paper or electronically. The term RFC is often misused to mean a Change Record, or the Change itself. (ITIL® V3, Service Transition)

Request for Estimate (RFE) – A request to provide a quick estimate or quote, to generate a purchase order (P.O.)

Request Fulfillment - The process responsible for managing the lifecycle of all service requests. (ITIL® V3, Service Operation)

Request for Information (RFI) - An informal document issued when an agency is not aware of the products available in the market which may satisfy its requirements. The use of an RFI does not require a purchase requisition, however a RFI may result in the development of a requisition, or the issuance of an IFB or RFP after an agency determines the types of products that are available which will satisfy its requirements. An RFI cannot be made into an agreement

Request for Proposals (RFP) - All documents, whether attached or incorporated by reference, utilized for soliciting proposals; the RFP procedure requires negotiation with offerors (to include prices) as distinguished from competitive bidding when using an Invitation for Bids

Request for Quotation (RFQ) - An informal solicitation or request for information where oral or written quotes are obtained from vendors. There is no formal advertising or receipt of sealed bids. An RFQ is used only where statutes do not require formal sealed bids, such a small or emergency purchases, but price competition is desired

Request for Qualified Contractors (RFQC) – A form of RFQ that provides for greater flexibility and opportunity for an offeror to change its proposal as it becomes more familiar with the agency needs and requirements. It includes a number of gates and phases. There is no disclosure of proposals submitted by competing offerors. Fair and equal treatment is required

Requirement(s) – A statement or set of statements that define what the user(s) of a product want that product to do. Generally, it defines what capabilities a product needs to have, based on the needs of the users

Requirements Document - A formal document that consists of a statement or set of statements that define product functions and capabilities as set by the end user

Requirements Phase (Software Application Projects) - The period of time in the software life cycle during which the requirements for a software product are defined and documented. (SEI)

Requirements Tracing - Describing and following the life of a requirement in both forwards and backwards direction (i.e., from its origins, through its development and specification, to its subsequent deployment and use, and through periods of ongoing refinement and iteration in any of these phases. (SEI)

Requirements Mapping/ Matrix- See Requirements Tracing definition.

Resolution - Action taken to repair the root cause of an incident or problem, or to implement a workaround. (ITIL® V3, Service Operation)

Resource -Skilled human resources (specific disciplines either individually or in crews or teams), equipment, services, supplies, commodities, material, budgets, or funds. (PMBOK 3rd Edition) Resources, including infrastructure, are considered to be assets of an organization. (ITIL)

Resource Leveling - Any form of schedule network analysis in which scheduling decisions (start and finish dates) are driven by resource constraints (e.g., limited resource availability or difficult-to-manage changes in resource availability levels.) (PMBOK 3RD EDITION)

Response Time - A measure of the time taken to complete an operation or transaction. Used in Capacity Management as a measure of IT infrastructure performance, and in Incident Management as a measure of the time taken to answer the phone, or to start diagnosis. (ITIL® V3)

Responsibility Assignment Matrix (RAM) - A structure that relates the project organizational breakdown structure to the work breakdown structure to help ensure that each component of the project's scope of work is assigned to a responsible person. (PMBOK 3RD EDITION)

Restore - Taking action to return an IT Service to the users after repair and recovery from an incident. This is the primary objective of Incident Management. (ITIL® V3, Service Operation)

Retirement
(1) In Software Application Projects, the period of time in the software life cycle during which support for a software product is terminated (SEI)
(2) The permanent removal of an IT Service, or other configuration item, from the live environment. Retired is a stage in the lifecycle of many configuration items. (ITIL® V3, Service Transition)

Return on Investment (ROI) - A figure of merit used to help make capital investment decisions. ROI is calculated by considering the annual benefit divided by the investment amount (GAO) or net profit of an investment divided by the net worth of the assets invested. (ITIL® V3)

Return to Normal - The phase of an IT Service Continuity Plan during which full normal operations are resumed. (ITIL® V3, Service Design)

Review - An evaluation of a change, problem, process, project etc. Reviews are typically carried out at predefined points in the lifecycle, and especially after closure. The purpose of a review is to ensure that all deliverables have been provided, and to identify opportunities for improvement. (ITIL® V3)

Rights - Entitlements, or permissions, granted to a user or role. For example the Right to modify particular data, or to authorize a change. (ITIL® V3, Service Operation)

Risk
(1) An uncertain event or condition that, if it occurs, has a positive or negative effect on a project's objectives. (PMBOK 3RD EDITION)
(2) A risk is measured by the probability of a threat, the vulnerability of the asset to that threat, and the impact it would have if it occurred
(3) A function of the likelihood of a given threat source exploiting a potential vulnerability, and the resulting impact of that adverse event on the organization

Risk Acceptance – A risk response planning technique that indicates that the project team has decided not to change the project management plan to deal with a risk, or is unable to identify any other suitable response strategy. (PMBOK 3RD EDITION)

Risk Analysis - A technique to identify and assess factors that may jeopardize the success of a project or achieving a goal. The technique also helps define preventive measures to reduce the probability of these factors from occurring and identify countermeasures to successfully deal with these constraints when they develop. (GAO)

Risk Avoidance – A risk response planning technique for a threat that creates changes to the project management plan that are meant to either eliminate the risk or to protect the project objectives from its impact.(PMBOK 3RD EDITION)

Risk Assessment - The initial steps of Risk Management. Review, examination, and judgment of whether or not the identified risks are acceptable. Analyzing the value of assets to the business, identifying threats to those assets, and evaluating how vulnerable each asset is to those threats. Risk Assessment can be quantitative (based on numerical data) or qualitative

Risk Assessment Report (RAR) - A formal project deliverable, first approved at the end of the planning phase and continuously updated thereafter. It presents the current risk profile for the project and defines the criteria for identifying risks in all key aspects of the project

Risk Based Testing – A type of testing that prioritizes the tests of features and functions based on risk of failure and impact to the outcome based on a risk analysis of likelihood this risk would impact the projects outcome and stakeholder tolerance

Risk Control - Involves executing the Risk Management Plan in order to respond to risk events over the course of the project

Risk Event - A discrete occurrence that may adversely or favorably affect the project

Risk Identification - The process of determining which risks might affect the project and documenting their characteristics. (PMBOK 3RD EDITION)

Risk Management –
(1) The 8th of 9 PMI standard *Knowledge Areas*. The recommended processes are concerned with identifying, analyzing, and responding to project risk. The recommended processes are: Risk Management Planning, Risk Identification, Qualitative Risk Analysis, Quantitative Risk Analysis, Risk Response Planning, Risk Monitoring and Control
(2) The process of identifying, analyzing, and responding to risk factors throughout the life of a project and in the best interests of its objectives. The art and science of identifying, analyzing, and responding to risk factors throughout the life of a project and in the best interests of its objectives
(3) The process of identifying, controlling, and mitigating information system–related risks. It includes risk assessment; cost-benefit analysis; and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws
(4) The process of measuring, or assessing risk and developing strategies to manage it. Strategies include transferring the risk to another party, avoiding the risk, reducing the negative effect of the risk, and accepting some or all of the consequences of a particular risk. It is the selection and specification of security controls necessary to protect individuals and the operations and assets of the organization as part of an organization-wide information security program that involves the *management of organizational risk*---that is, the risk to the organization or to individuals associated with the operation of an information system. The management of organizational risk is a key element in the organization's information security program and provides an effective framework for selecting the appropriate security controls for an information system

Risk Management Framework - A methodology for identifying, controlling, and mitigating information system–related risks. The methodology includes risk assessment; cost-benefit analysis; and the selection, implementation, test, and security evaluation of safeguards / controls

Risk Management Plan - The document describing how project risk management will be structured and performed on the project. (PMBOK 3RD EDITION)

Risk Management Report (RMR) - A report to measure actual risk management against the Risk Management Plan (RMP). Usually contains three areas of concern: (1) The status of known risks, (2) Mitigation Strategies against those risks, and (3) Trigger points for escalation.

Risk Mitigation - A risk response planning technique associated with threats that seeks to reduce the probability of occurrence or impact of a risk to below an acceptable threshold. (PMBOK 3RD EDITION)

Risk Statement (also known as statement of risk) - A description of the current conditions that may lead to a loss or a description of the loss or consequence. (SEI)

Role - A set of responsibilities, activities and authorities granted to a person or team. A role is defined in a process. One person or team may have multiple roles, for example the roles of Configuration Manager and Change Manager may be carried out by a single person. (ITIL® V3)

Rollout - Synonym for Deployment. Most often used to refer to complex or phased deployments or deployments to multiple locations. (ITIL® V3, Service Transition)

Root Cause - The underlying or original cause of an incident or problem. (ITIL® V3, Service Operation)

Root Cause Analysis (RCA) - An activity that identifies the Root Cause of an incident or problem. RCA typically concentrates on IT infrastructure failures. (ITIL® V3, Service Operation)

Run – A major step in the EPLC. ("Enterprise Performance Life Cycle Management" Guideline, published by GTAs Enterprise Project management Office)

S

SAAS (Software as a service) –

(1) May be referred to as "on-demand software" supplied by an Application Service Provider (ASP)
(2) The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). 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.

SAISO - The Senior Agency Information Security Officer (SAISO), formerly referred to as Agency ISO is the primary/lead/senior person in an agency responsible for managing the information security program for the agency. The term has been adopted by Georgia from materials of the National Institute of Standards and Technology (NIST).

Scalability - The ability of an IT Service, process, configuration item etc. to perform its agreed function when the workload or scope changes. (ITIL® V3)

Schedule Development - The process of analyzing schedule activity sequences, schedule activity durations, resource requirements, and schedule constraints to create the project schedule. (PMBOK 3RD EDITION)

Schedule Performance Index (SPI) - The measure of schedule efficiency on a project. IT is the ratio of earned value (EV) to planned value (PV). The SPI = EV divided by PV. An SPI equal to or greater than one indicates a favorable condition and a value of less than one indicates an unfavorable condition. (PMBOK 3RD EDITION)

Schedule Management - The 3rd o f 9 PMI standard *Knowledge Areas*. The recommended processes ensure timely completion of the project. The recommended processes are: Activity Definition, Activity Sequencing, Activity Resource Estimating, Activity Duration Estimating, Schedule Development, and Schedule Control

Schedule Variance (SV) - A measure of schedule performance on a project. It is the algebraic difference between the earned value (EV) and the planned value (PV). SV = EV minus PV. (PMBOK 3RD EDITION)

Scope
(1) The sum of the products, services, and results to be provided as a project. (PMBOK 3RD EDITION)
(2) The boundary, or extent, to which a process, procedure, certification, contract etc. applies.

Scope Change - Any change to the project scope. A scope change almost always requires an adjustment to the project cost or schedule. (PMBOK 3RD EDITION)

Scope Creep – Adding features and functionality (project scope) without addressing the effects on time, costs, and resources, or without customer approval. (PMBOK 3RD EDITION)

Scope Definition - The process of developing a detailed project scope statement as the basis for future project decisions. (PMBOK 3RD EDITION)

Scope Management – Management and control of the products, services, and results to be provided during the full life cycle of an Agency initiative, program or project. Agency 'change control' processes and procedures are used to control scope

Scope Planning -The process of creating a project scope management plan. (PMBOK 3RD EDITION)

Scope Statement – A document capturing the sum of products and services to be provided as a project. The Scope Statement is part of the Project Plan

Scope Verification - The process of formalizing acceptance of the completed project deliverables. (PMBOK 3RD EDITION)

Second-line Support - The second level in a hierarchy of support groups involved in the resolution of incidents and investigation of problems. Each level contains more specialist skills, or has more time or other resources. (ITIL® V3, Service Operation)

Security Breach – A security breach has occurred when it is reasonably believed that unauthorized acquisition of personally identifiable information has occurred

Security Categorization - A ranking of system or application risks:
High - High Impact is the system or application categorization assigned if, for ANY security objective, the potential for loss of life, severe or catastrophic adverse effect on organizational operations, assets or individuals
Moderate - Moderate Impact is the system or application categorization assigned if, for ANY security objective, the potential for serious adverse effect on organizational operations, assets, or individuals

Low - Low Impact is system/application categorization assigned if, for ALL security objectives, the potential for limited or minimal adverse effect on organizational operations, assets, or individuals

Security Incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices which may include, but are not limited to: widespread infections from virus, worms, Trojan horse or other malicious code; unauthorized use of computer accounts and computer systems; unauthorized, intentional or inadvertent disclosure or modification of sensitive/critical data or infrastructure; intentional disruption of critical system functionality; intentional or inadvertent penetration of firewall; compromise of any server, including Web server defacement; exploitation of other weaknesses; child pornography; attempts to obtain information to commit fraud or otherwise prevent critical operations or cause danger to state or national security; and violations of the State security policies or standards that threaten or compromise the security objectives of the State's data, technology or communications systems

Security Log Infrastructure - The hardware, software, networks and media used to generate, transmit, store, analyze, and dispose of log data

Security Log Management - The process for generating, transmitting, storing, analyzing and disposing of computer security log data

Security Objective – Confidentiality, Integrity, and Availability
Confidentiality **-** "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542] (A loss of *confidentiality* is the unauthorized disclosure of information.)
Integrity **-** "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542] (A loss of *integrity* is the unauthorized modification or destruction of information.)
Availability **-** "Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542] (A loss of *availability* is the disruption of access to or use of information or an information system.)

Security Program - An internal information security infrastructure that includes all the following program elements:
a) Security management organization that assesses risk, develops and implements policies, processes, and technology to adequately protect the information assets, personnel and facilities under their control and ensures compliance with Enterprise policies and standards and federal and state requirements.
b) A risk management framework
c) Business Continuity and Disaster Recovery Plan/s
d) An Incident Management and Response capability
e) Security Education and Awareness component
f) Internal policies and procedures
g) Assessment, Compliance and Enforcement mechanisms

Server – A computer that provides some service for other computers connected to it via a network

Services - Any activities performed by an independent contractor wherein the service rendered does not consist primarily of acquisition of equipment or materials, or the rental of equipment, materials and supplies

Service (ITIL term) - A means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks. (ITIL® V3)

Service Acceptance Criteria (SAC) - (Service Transition) A set of criteria used to ensure that an IT Service meets its functionality and quality requirements and that the IT Service Provider is ready to operate the new IT Service when it has been deployed. (ITIL® V3**)**

Service Asset - Any capability or resource of a Service Provider. (ITIL® V3)

Service Asset and Configuration Management (SACM) - (Service Transition) The process responsible for both Configuration Management and Asset Management. (ITIL® V3)

Service Capacity Management (SCM) - The activity responsible for understanding the performance and capacity of IT Services. The resources used by each IT Service and the pattern of usage over time are collected, recorded, and analyzed for use in the Capacity Plan. (ITIL® V3, Service Design, Continual Service Improvement)

Service Catalog - A database or structured document with information about all live IT Services, including those available for deployment. The Service Catalog is the only part of the Service Portfolio published to customers, and is used to support the sale and delivery of IT Services. The Service Catalog includes information about deliverables, prices, contact points, ordering and request processes. (ITIL® V3, Service Design)

Service Contract - A contract to deliver one or more IT Services. The term Service Contract is also used to mean any agreement to deliver IT Services, whether this is a legal contract or an SLA. (ITIL® V3, Service Strategy)

Service Desk - The Single Point of Contact between the Service Provider and the users. A typical Service Desk manages incidents and Service Requests, and also handles communication with the users. (ITIL® V3, Service Operation)

Service Hours - An agreed time period when a particular IT Service should be available, for example, "Monday-Friday 08:00 to 17:00 except public holidays". Service Hours should be defined in a Service Level Agreement. (ITIL® V3, Service Design, Continual Service Improvement)

Service Improvement Plan (SIP) - A formal plan to implement improvements to a process or IT Service. (ITIL® V3**,** Continual Service Improvement)

Service Level - Measured and reported achievement against one or more Service Level Targets. The term Service Level is sometimes used informally to mean Service Level Target. (ITIL® V3)

Service Level Agreement (SLA) - An agreement between an IT Service Provider and a customer. The SLA describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service Provider and the customer. A single SLA may cover multiple IT Services or multiple customers. (ITIL® V3, Service Design and Continual Service Improvement)

Service Level Objective (SLO)- The SLO details the characteristics of the support services supplied to sustain quality operations of an application and serves as a service contract between an ASP and their customers who utilize their application. SLOs are similar to SLAs; however, an SLO is not a signed agreement

Service Level Management (SLM) - The process responsible for negotiating Service Level Agreements, and ensuring that these are met. SLM is responsible for ensuring that all IT Service Management processes, operational level agreements, and underpinning contracts, are appropriate for the agreed Service Level Targets. SLM monitors and reports on Service Levels, and holds regular customer reviews. (ITIL® V3, Service Design, Continual Service Improvement)

Service Level Requirement (SLR) - A customer requirement for an aspect of an IT Service. SLRs are based on business objectives and are used to negotiate agreed Service Level Targets. (ITIL® V3, Service Design, Continual Service Improvement)

Service Level Target - A commitment that is documented in a Service Level Agreement. Service Level Targets are based on Service Level Requirements, and are needed to ensure that the IT Service design is Fit for Purpose. (ITIL® V3, Service Design, Continual Service Improvement)

Service Maintenance Objective - The expected time that a configuration item will be unavailable due to planned maintenance activity. (ITIL® V3**,** Service Operation)

Service Provider - An organization supplying services to one or more internal customers or external customers. Service Provider is often used as an abbreviation for IT Service Provider. (ITIL® V3, Service Strategy)

Service Reporting - The process responsible for producing and delivering reports of achievement and trends against Service Levels. Service Reporting should agree the format, content and frequency of reports with customers. (ITIL® V3, Continual Service Improvement)

Service Request - A request from a user for information, or advice, or for a Standard Change or for access to an IT Service. For example to reset a password, or to provide standard IT Services for a new user. Service Requests are usually handled by a Service Desk, and do not require an RFC to be submitted. (ITIL® V3, Service Operation)

Single Point of Contact - Providing a single consistent way to communicate with an organization or business unit. For example, a Single Point of Contact for an IT Service Provider is usually called a Service Desk. (ITIL® V3, Service Operation)

Slack – Term used in PERT or arrow diagramming method for float. (PMBOK 3RD EDITION)

Slippage – The tendency of a project to exceed original estimates of budget and time

Software - A general term that refers to all programs or instructions that are used to operate computer hardware. Software causes computer hardware to perform activities by telling a computer how to execute functions and tasks

Software Architecture - The structure of the components of a program/system, their interrelationships, and principles and guidelines governing their design and evolution over time. (SEI)

Software Life Cycle - The period of time that begins when a software product is conceived and ends when the software is no longer available for use. The life cycle typically includes a concept phase, requirements phase, design phase, implementation phase, test phase, installation and checkout phase, operation and maintenance phase, and sometimes, retirement phase. These phases may overlap or be performed iteratively, depending on the software development approach used. (SEI)

Software Development Life Cycle – See *Software Life Cycle* and *Project Life Cycle Management* in the glossary.

Sole Source – A product or service which is practicably available only from one source. Sole source is not "best" source or the "only" source to consider. A sole source situation occurs when no other product or service can conceivably serve the needs of an agency. Some 'sole source' examples are:

- A software maintenance agreement may be a sole source because the software owner is the only one capable of maintaining and servicing the software. However, an alarm system maintenance contract is probably not a sole source, as there are often multiple firms qualified to service the system
- Parts to repair a specific piece of equipment may only be produced by one manufacturer. However, there may be more than one source for the parts. It is often possible to obtain quotes from suppliers that service other areas or states. If cheaper parts can only be purchased from a source that is 2000 miles away, the local source is probably taking advantage of its captive market

- Membership in a specific organization is considered a sole source

Sourcing Agency – an external entity responsible for staffing state contracts on behalf of the sponsoring agencies

Specification - A formal definition of requirements. A specification may be used to define technical or operational requirements, and may be internal or external. (ITIL® V3)

Specification Documents - Documents that provide specific information about the project deliverable characteristics

Sponsoring Agency – is the state agency that has acquired the services of a third-party or otherwise responsible for granting physical and/or logical access to facilities, information, and/or information systems to entities external to state government, to include but not limited to those defined in Third Party

Stage Deliverables - All deliverables are created in support of the investment objectives. Their purpose in each stage is to provide the supporting material for the business owner to have confidence in achieving the benefits of the investment. ("Enterprise Performance Life Cycle Management" Guideline, published by GTAs Enterprise Project management Office)

Stage Exit Criteria - Exit Criteria are established as Stage 'fitness' measures that must be attained to successfully complete a given stage. This creates a defined measure of performance at key points in the life of an investment and provides the Business Owner with a means of gauging progress or performance. Exit criteria can be documents, deliverables or specific actions that must be accomplished. ("Enterprise Performance Life Cycle Management" Guideline, published by GTAs Enterprise Project management Office)

Stage Gate Review - The last step of a specified stage, as defined in the EPLC, is a Stage Gate Review to ensure that the investment status may progress to the next phase. Stage Gate Reviews consist of an independent confirmation by Key Stakeholders for an investment that the Program (or Project) Manager has satisfactorily produced all the required deliverables and adequately met all exit criteria for the phase to permit advancement to the next phase. The emphasis of Stage Gate Reviews is on:
• The successful accomplishment of the phase objectives
• The plans for the next life cycle phase
• The risks associated with moving into the next life cycle phase
("Enterprise Performance Life Cycle Management" Guideline, published by GTAs Enterprise Project management Office)

Stakeholder - Persons and organizations such as customers, sponsors, performing organization and the public, that are actively involved in the project, or whose interests may be positively or negatively affected by execution or completion of the project. (PMBOK 3RD EDITION)

Standard - Specific and, where applicable, technical documents containing directives and mandatory specifications governing the management, development, and use of information technology resources

Standard Change - A pre-approved change that is low risk, relatively common and follows a procedure or work instruction. For example password reset or provision of standard equipment to a new employee. RFCs are not required to implement a Standard Change, and they are logged and tracked using a different mechanism, such as a Service Request. (ITIL® V3, Service Transition)

Standby - Used to refer to resources that are not required to deliver the live IT Services, but are available to support IT Service Continuity Plans. For example a Standby Data Center may be maintained to support Hot Standby, Warm Standby or Cold Standby arrangements. (ITIL® V3, Service Design)

State Critical Projects Committee - A State level IT Governance Organization.

State Information Assets include all data, e-mail and/or information created, accessed, processed, transmitted and/or stored on behalf of official State business that is not otherwise accessible through the public access domains

Statement of Work (SOW) - (1) A narrative description of products, services or results to be supplied. (PMBOK 3RD EDITION) (2) A detailed description of work which the requestor wants the contractor to perform

Status Reports - A report containing information on a specific project, indicating if the project is ahead of schedule, on schedule, or behind schedule in relation to the project plan

Steering Committee- An advisory committee usually made up of high level stakeholders and/or experts who provide guidance on key project issues such as project objectives, budgetary control, resource allocation, and decisions involving large project expenditures

Storage Management - (Service Operation) The process responsible for managing the storage and maintenance of data throughout its lifecycle. (ITIL® V3)

Super User - A user who helps other users, and assists in communication with the Service Desk or other parts of the IT Service Provider. Super Users typically provide support for minor incidents and training. (ITIL® V3, Service Operation)

Supplier - A Third Party responsible for supplying goods or services that are required to deliver IT services. Examples of suppliers include commodity hardware and software vendors, network and telecom providers, and outsourcing organizations. (ITIL® V3**,** Service Strategy, Service Design)

Support Hours - The times or hours when support is available to the users. Typically this is the hours when the Service Desk is available. Support Hours should be defined in a Service Level Agreement, and may be different from Service Hours. For example, Service Hours may be 24 hours a day, but the Support Hours may be 07:00 to 19:00. (ITIL® V3, Service Design, Service Operation)

Supportive Business Application - Application supports only basic agency functions and is not necessary to achieve agency goals. See Application Risk Categories

System –
1) A discrete set of information resources (workstations, servers, minor applications, network, etc) working together for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information
2) Operational systems (Production Systems) are those IT systems that are readily available, in use and actively supporting the business. Operational systems do not include research, development or test systems

Systems Analyst- An individual whose primary job is to research application and/or business problems, plan solutions, recommend software and systems and coordinate development to meet business or other requirements

System Boundary – All the components of an information system or an interconnected set of information resources under the same direct management control and security support structure, that share common functionality (normally includes hardware, software, information, data, applications, communications, and people)

System Integration- A process or phase concerned with joining different subsystems or components as one large system

System Lifecycle is the overall process of developing/acquiring, implementing, and retiring information systems

through a multi-step process from initiation, design, implementation, and maintenance to disposal

System Media – any form of data or software stored outside the security boundaries of the system including but not limited to; paper printouts, tapes, diskettes, flash memory drives (i.e. USB, jump, thumb), internal hard drives, laptops, PDAs, CDs, DVDs, etc.

System Program – See application software and systems software

System Security Plan is a formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements

Systems Software - Any computer software which manages and controls computer hardware, allowing application software to perform a task. Operating systems, such as Microsoft Windows, Mac OS X or Linux, are examples of system software. System software contrasts with application software, which are programs that enable the end-user to perform specific, productive tasks, such as word processing or image manipulation

System software performs tasks like transferring data from memory to disk, or rendering text onto a display device. Specific kinds of system software include loading programs, Operating systems, device drivers, programming tools, compilers, assemblers, linkers, and utility software

System Testing (Software Application Projects) - Testing conducted on a complete, integrated system to evaluate the system's compliance with its specified requirements. (SEI)

T

Tangible Benefits - Benefits that can be measured and quantified. Tangible benefits include savings that result from improved performance and efficiency

Tangible Costs – Costs that can be measured and quantified. Tangible costs include costs for hardware, software, people, and supplies for both the development process and ongoing operations

Task – Well defined components of project work. Often a task is referred as a work package. This is not a term used by PMI, which uses 'activities'

Technical Specifications - Specifications that establish the material and performance requirements of goods and services

Technology Enterprise Management - Methods for managing technology resources for all agencies considering the priorities of state planners, with an emphasis on making communications and sharing of data among agencies feasible and ensuring opportunities of greater access to state services by the public.
[O.C.G. A. 50-25-1(b)(13)]

Technology Infrastructure - Means telecommunications, automated data processing, word processing and management information systems, and related information, equipment, goods and services

Technology Investments – Assets such as business-driven applications, data, facilities, IT human resources, infrastructure, services, operations and processes used to support the flow or processing of information for business activities

Technology Portfolio - A management tool comprised of essential information about technology investments, structured to facilitate the evaluation of investment alternatives in support of an agency's overall strategic business plan

Technology Portfolio Management - An approach for analyzing and ranking potential technology investments based upon state priorities and a cost benefit analysis to include, but not be limited to, calculated savings, direct and indirect, and revenue generation related to technology expenditures and selecting the most cost-effective investments. The minimization of total ownership costs, i.e., purchase, operation, maintenance, and disposal, of technology resources from acquisition through retirement while maximizing benefits is to be emphasized. [O. C. G. A. 50-25-1(b)(15)]

Telecommunications - Any origination, transmission, emission, or reception of signals, writings, images, and sounds or intelligence of any nature, by wire, radio, television, optical or other electromagnetic systems

Telecommunications Equipment - Defined as, but not limited to: channel service units, data compression units, line drivers, bridges, routers, and Asynchronous Transfer Mode switches (ATM), multiplexers and modems. Also, private branch exchanges (PBX), Integrated Services Digital Network (ISDN) terminal equipment, voice mail units, automatic call distribution (ACD), voice processing units and key systems. Video communications products such as: coders, multi-point conferencing units and inverse multiplexers

Telecommunications Services - These services include, but are not limited to; data communication services, such as point-to-point and multipoint circuits, Internet, Frame Relay SMDS, ATM, and dial up lines, and voice communications services such as Centrex, business/private lines and WATS lines including 800 services, tie and access lines, long distance services, voice mail, pay phones, wireless communications and cellular services (see also "Public Telecommunications Services")

Telework or Telecommute - The ability of an organization's employees and contractors to conduct work from locations other than the organization's facilities

Template – A partially complete document in a predefined format that provides a defined structure for collecting, organizing and presenting information and data. Templates are often based upon documents created during prior projects. Templates can reduce the effort needed to perform work and increase the consistency of results. (PMBOK 3RD EDITION)

Test
(1) In Software Application Projects, an activity in which a system or component is executed under specified conditions, the results are observed or recorded, and an evaluation is made of some aspect of the system or component. (SEI)
(2) An activity that verifies that a configuration item, IT Service, process, etc. meets its specification or agreed requirements (ITIL® V3, Service Transition

Test Environment - A controlled environment used to test configuration items, builds, IT Services, processes etc. (ITIL® V3, Service Transition)

Test Phase (Software Application Projects) -The period of time in the software life cycle during which the components of a software product are evaluated and integrated, and the software product is evaluated to determine whether or not requirements have been satisfied. (SEI)

Test Scripts- A set of instructions that will be performed on a software application or system in the process of being changed to test that the system functions as expected

Test Tools (Software Application Projects) - Computer programs used in the testing of a system, a component of the system, or its documentation. Examples include monitor, test case generator, timing analyzer. (SEI)

Testing -The actual test of the products or processes created within the development phase of an Information Technology project

Third-Party is synonymous with contractor, service provider, consultant or any other individual or organization external to state government providing services on behalf of, for, or as an agent of state government or otherwise requiring access to non-public state facilities and/or information resources

Threat - Anything that might exploit vulnerability. Any potential cause of an incident can be considered to be a Threat. For example a fire is a Threat that could exploit the vulnerability of flammable floor coverings. This term is commonly used in Information Security Management and IT Service Continuity Management, but also applies to other areas such as Problem and Availability Management. (ITIL® V3)

Threshold - The value of a metric which should cause an alert to be generated, or management action to be taken. For example "Priority1 Incident not solved within 4 hours", "more than 5 soft disk errors in an hour", or "more than 10 failed changes in a month". (ITIL® V3)

Throughput - A measure of the number of transactions, or other operations, performed in a fixed time. For example 5000 emails sent per hour, or 200 disk I/Os per second. (ITIL® V3, Service Design)

Timeframe - The period when action is required to mitigate the risk. Timeframe is one of the three attributes of risk. (SEI)

Total Cost - The sum of all cost (fixed and variable) for a particular item or activity over a specified period

Total Cost of Ownership (TCO) - A calculation of the fully burdened cost of owning a component. The calculation helps consumers and enterprise managers assess both direct and indirect costs and benefits related to the purchase of IT components. For the business purchase of a computer, the fully burdened costs can also include such things as service and support, networking, security, user training, and software licensing

Training (Software Application Projects) - Provisions to learn how to develop, maintain, or use the software system

Transformational Projects - Projects that change the way an organization does business

Triggers - Indications that a risk has occurred or is about to occur. Triggers may be discovered in the risk identification process and watched in the risk monitoring and control process. (PMBOK 3RD EDITION)

Triple Constraint – A framework for evaluating competing demands. The triple constraint is often depicted as a triangle where one of the sides or one of the corners represents one of the parameters being managed by the project team. (PMBOK 3RD EDITION)

Trusted Partner – An Agency of the State of Georgia that has met the requirements set forth in a data sharing agreement between agencies and agreed to be bound by the principles, policies and procedures established in that agreement

U

Underpinning Contract (UC) - A Contract between an IT Service Provider and a Third Party. The Third Party provides goods or services that support delivery of an IT Service to a customer. The Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA. (ITIL® V3, Service Design)

Unit Testing (Software Application Projects) - Testing of individual hardware or software units or groups of related units. (SEI)

User Acceptance Testing (UAT) - Phase of testing where users determine whether a system meets all their requirements and supports the business for which it was designed

Urgency - A measure of how long it will be until an incident, problem or change has a significant impact on the business. For example a high impact incident may have low urgency, if the impact will not affect the business until the end of the financial year. Impact and Urgency are used to assign Priority. (ITIL® V3, Service Transition, Service Design)

Usability - The ease with which an application, product, or IT Service can be used. Usability Requirements are often included in a Statement of Requirements. (ITIL® V3, Service Design)

Use Case -

(1) A technique used to define required functionality and objectives, and to design tests. Use cases define realistic scenarios that describe interactions between Users and an IT Service or other System
(2) A use case defines a goal-oriented set of interactions between external actors and the system under consideration. That is, use cases capture who (actors) does what with the system (interactions), for what purpose (goal). A complete set of use cases specifies all the different ways to use the system, and thus defines all behavior required of the system--without dealing with the internal structure of the system. (ITIL® V3, Service Design)

User - A person who uses an IT Service or application on a day-to-day basis. Users are distinct from Customers, as some Customers do not use the IT Service directly. May also be referred to as end user

User interface (Software Application Projects) - An interface that enables information to be passed between a human user and hardware or software components of a computer system. (SEI)

User Profile (UP) - A pattern of user demand for IT Services. Each user profile includes one or more patterns of business activity. (ITIL® V3, Service Strategy)

V

Validation

1) The technique of evaluating a component or product during or at the end of a phase or project to ensure it complies with the specified requirements. Contrast with verification. (PMBOK 3RD EDITION)
(2) An activity that ensures a new or changed IT Service, process, plan, or other deliverable meets the needs of the business. Validation ensures that business requirements are met even though these may have changed since the original design. (ITIL® V3, Service Transition)

Variance – A quantifiable deviation, departure, or divergence away from a known baseline or expected value. (PMBOK 3RD EDITION)

Vendor Management - The 9th of 9 PMI standard *Knowledge Areas*. The recommended processes are concerned with acquiring goods and services from outside the agency. The recommended processes are: Plan Purchases and Acquisitions, Plan Contracting, Request Seller Responses, Select Sellers, Contract Administration, Contract Closure

Verification –
(1) The technique of evaluating a component or product at the end of a phase or project to assure or confirm it satisfies the conditions imposed. Contrast with validation. (PMBOK 3RD EDITION)
(2) An Activity that ensures a new or changed IT Service, process, plan, or other deliverable is complete, accurate, reliable and matches its design specification. (ITIL® V3, Service Transition)

Verification and Audit - The Activities responsible for ensuring that information in the CMDB is accurate and that all Configuration Items have been identified and recorded in the CMDB. Verification includes routine checks that are part of other Processes. For example, verifying the serial number of a desktop PC when a User logs an Incident. Audit is a periodic, formal check. (ITIL® V3, Service Transition)

Version - Service Transition) A Version is used to identify a specific Baseline of a Configuration Item. Versions typically use a naming convention that enables the sequence or date of each Baseline to be identified. For example Payroll Application Version 3 contains updated functionality from Version 2. (ITIL® V3, Service Transition)

Vulnerability - A weakness that could be exploited by a threat. For example an open firewall port, a password that is never changed, or a flammable carpet. A missing control is also considered to be vulnerability. (ITIL® V3)

W

W3C – Accepted acronym for the World Wide Web Consortium. The World Wide Web Consortium is a consortium of over 500 member organizations that develop interoperable technology specifications, guidelines, software, and tools related to the Internet. The URL for their website is http://www.w3.org/.

WAN - A Wide Area Network spans a relatively large geographical area. Computers connected to a wide area network are often connected through public networks, such as the telephone system as well as private leased lines. A WAN also provides the mechanism for users on one agency's LAN to communicate with users on a different agency's LAN. For purposes of this document, the State of Georgia's WAN is that Wide Area Network that acts as the backbone for interagency electronic communication, and is installed and maintained by the Georgia Technology Authority

Warm Standby - Synonym for Intermediate Recovery

Warranty - A promise or guarantee that a product or Service will meet its agreed Requirements. (ITIL® V3, Service Strategy)

Web Server - A computer that provides World Wide Web (WWW) services on the Internet. It includes the hardware, operating system, Web server software, and Web site content (Web pages). If the Web server is used internally and not by the public, it may be known as an "intranet server"

Webmaster - A person responsible for the implementation of a Web site. Webmasters should be proficient in HTML and one or more scripting and interface languages, such as JavaScript and Perl. They may or may not be responsible for the underlying server

Wintel -A term describing any computer platform consisting of some version of Microsoft Windows running on an Intel 80x86 processor or compatible. (The Free On-line Dictionary of Computing, 2003. http://www.foldoc.org/, Editor Denis Howe.

Work Breakdown Structure (WBS) - A deliverable-oriented hierarchical decomposition of the work to be executed by the project team to accomplish the project objectives and create the required deliverables. It organizes and defines the total scope of the project. Each descending level represents an increasingly detailed definition of the project work. The WBS is decomposed into work packages. The deliverable orientation of the hierarchy includes both internal and external deliverables. (PMBOK 3RD EDITION)

Work in Progress (WIP) - A Status that means activities have started but are not yet complete. It is commonly used as a status for incidents, problems, changes etc. (ITIL® V3)

Work Package - A deliverable or project work component at the lowest level of each branch of the work breakdown structure. The work package includes the schedule activities and schedule milestones required to complete the work package deliverable or project work component. (PMBOK 3RD EDITION)

Workaround –
(1) A response to a negative risk that has occurred. Distinguished from contingency plan in that a workaround is not planned in advance of the occurrence of the risk event. (PMBOK 3RD EDITION)
(2) Reducing or eliminating the Impact of an Incident or Problem for which a full Resolution is not yet available, for example, restarting a failed configuration item. Workarounds for Problems are documented in Known Error Records. Workarounds for incidents that do not have associated problem records are documented in the incident record. (ITIL® V3, Service Operation)

Workforce Management – (1) The 6th o f 9 PMI standard *Knowledge Areas*. The recommended processes make the most effective use of the people involved with the project. The recommended processes are: HR Planning, Acquire Project Team, Develop Project Team, and Manage Project Team. (2) Managing a systematic process for identifying the human capital required to meet agency goals and developing the strategies to meet these requirements

Workstation - A wintel platform desktop or laptop general-purpose computer deployed to State knowledge (i.e. business or office) workers.

For the State's purpose, PC and Workstation are used more or less interchangeably. A state definition is a desktop or laptop general-purpose computer deployed to a single State knowledge worker (i.e. business or office) typically running a Windows operating system on an Intel x86 or equivalent architecture. Traditional RISC/Unix based workstations are considered a very small subset of the total population of workstations and are referred to as not a Wintel workstations or specialized workstations.