

	GEORGIA TECHNOLOGY AUTHORITY	
Title:	Enterprise Operational Environment	
PSG Number:	SO-10-003.02	Topical Area: Operations / Performance and Capacity
Document Type:	Standard	Pages: 5
Issue Date:	July 15, 2011	Effective Date: July 15, 2011
POC for Changes:	Enterprise Governance and Planning	
Synopsis:	Specifies Georgia’s Enterprise Operational Environment, Establishes Application Conversion Priorities, and Provides for Exceptions	

PURPOSE

In 2008 and 2009, GTA executed a major project, acquiring by competitive bid comprehensive IT infrastructure services and managed network services for use by State agencies. By bundling together the IT infrastructure and managed network services requirements of the major agencies and leveraging resulting capabilities for the enterprise, GTA was able to acquire services that minimize the total cost of infrastructure ownership for the State while maximizing the benefits received. The cost model relies on maintaining the State’s bulk acquisition power by using the winning service providers for the State’s entire IT infrastructure and networking needs. To that end, it serves the best interest of the State for GTA to specify these IT infrastructure services and managed network services as Georgia’s Enterprise Operational Environment (EOE). The purpose of this document is:

- To establish a Statewide requirement to use the EOE,
- To specify high level parameters of the EOE for agency awareness, and
- To provide specific conditions that alternatives to EOE must meet that reduce risk to the State.

A major consideration in the execution of many IT investment projects involves the target operational environments of resulting systems or services. In order to appropriately specify the new IT system and, assuming no existing environmental constraints, one would either:

- Start from scratch to build a new environment, incurring infrastructure costs along with system costs,
- Design the new IT system to operate within an established environment, possibly making system design tradeoffs to fit into an established environment.

- Use the software and environment delivered by a third party via pay-for-use or subscription basis costs. This option may allow agencies to avoid a lengthy, expensive State development project.

An additional purpose of this standard is to foster communication between the agency and GTA when design/build decisions are being made.

SCOPE and AUTHORITY

See Information Technology Policies, Standards and Guidelines, policy (PM-04-001)

STANDARD

The IT infrastructure services and managed network services offered by the Georgia Technology Authority shall be Georgia's IT Enterprise Operational Environment (*see below: Capabilities of the Enterprise Operational Environment*).

1. All State agencies proposing to acquire new IT systems or services, or implementing significant modifications to the operational components of current IT systems or services, shall use the Enterprise Operational Environment to support the resulting IT systems' or services' operational requirements. Agencies experiencing exceptional circumstances when planning new IT systems or services, or significant modifications to current systems or services, including but not limited to circumstances such as financial constraints or beneficial outsourcing opportunities, may seek specific exemption from this provision from the State CIO. An exemption request should be processed no later than the investment's Planning Stage of the Enterprise Performance Lifecycle.
2. Third parties who provide IT as a service which is approved as an exemption to this standard shall meet specific minimum provisions to protect the State (agency) in the areas of security and recoverability. The following minimum provisions must be specified fully in the State/vendor contract and associated documents which describe the service:
 - a) If the State (agency) is the data owner, the State (agency) shall retain all ownership of data. Likewise, if the State (agency) is granted custodial authority by the data owner, the State (agency) shall retain custodial authority of the data.
 - b) The third party shall satisfy all provisions of State, federal and other regulatory requirements imposed on the State agency (such as HIPAA),
 - c) The third party's operational environment(s)' design topology shall be designed with an appropriate level (Tier I through Tier IV, "Uptime Institute's Data Center Tier Classification System") to meet the business needs of the agency/solution.
 - d) Data in storage, in processing and in transit between agency and third party physical locations shall be protected by appropriate encryption, security and data protection based on the data categorization assigned by the data owner. Vendor practices for encryption, access monitoring, security and privacy audits shall be defined.
 - e) The third party shall be in compliance with State and agency information technology and security standards,
 - f) The third party shall segregate State (agency) data from other customers'

data at all times.

- g) The third party shall operate business continuity and disaster recovery processes to meet the business needs of the agency.
- h) Exit clauses and merger-and-acquisition protections.
- i) Uptime and performance service-levels with contractual incentives and/or financial penalties to ensure vendor support.
- j) Key schedules defining how work will be performed, scope of work, deliverables, roles and responsibilities.

**BACKGROUND and DEFINITIONS:
SERVICES PROVIDED BY GEORGIA'S INFRASTRUCTURE AND MANAGED
NETWORK CONTRACTS**

The Infrastructure and Managed Network Services contracts include but are not limited to acquisition, operation and support of the following technologies service areas:

- a. Mainframe (IBM)
- b. Application Server (Windows and Unix)
- c. Utility Server (Email, DNS, DHCP, Blackberry, etc.)
- d. Server Storage
- e. Firewall / DMZ
- f. End User Computing
 - i. Personal computers, Laptops, Thin Client, Tablet PC
 - ii. Network Printers and Scanners
 - iii. Non-Standard or Specialized Equipment & Software, e.g. time clocks, finger printing equipment, etc.
- g. Telephony (Digital and Analog)
 - i. Premise Based Systems, e.g. PBX and Key System
 - ii. Central Office Based Systems, e.g. Centrex
 - iii. Voice Mail
 - iv. Contact Center Seat
- h. Interactive Voice Response Systems (IVR) and Auto Attendants
- i. Local and Wide Area Networks to include Wireless Access Points and Internet Access
- j. Virtual Private Networks (VPN) to include single and two factor authentication
- k. Video Conferencing
- l. Related Cross Functional Services (Disaster Recovery, Security, Service Desk, etc.)

CAPABILITIES OF THE ENTERPRISE OPERATIONAL ENVIRONMENT

Georgia's Enterprise Operational Environment (EOE) operated via Georgia Enterprise Technology Services (GETS) is a Tier 4 data center with redundant power, network, and cooling. GETS provides and supports the computing hardware, network, storage, operating systems, and physical database. Computing platforms supported by GETS include several flavors of UNIX (AIX, Solaris, and Linux) and all supported versions of Windows, Z/OS, and AS/400. Other platforms can be

supported on request. GETS provides database support for DB/2, Oracle, and SQL Server, with other relational databases on request.

APPLICATION LAYER AND DATABASE RESPONSIBILITIES OF AGENCIES USING EOE

The application layer and logical database services are not provided by GETS and is the sole responsibility of the business owner agency. For application services, the business owner agency should understand that most mainstream computing platforms are supported by GETS. Agencies planning to source the EOE for its applications services should specify what computing platform their application service uses, as well as dependencies for operating system, database, application servers, web servers, and other middleware, as well as enumerate any other specific software services (Active Directory, clustering, etc.). Access to production is limited for agency and third party developers, so the application and any patches or updates must be packaged such that they can be deployed by EOE personnel through a formal change control process. Access to development, test, and production environments are typically through an SSL-VPN and secure shell or remote desktop. Infrastructure security services are provided by GETS (firewalls, virus protection, intrusion protection, etc.), as are backup services. The application layer is the sole responsibility of the respondent. Any regulatory requirements requiring the encryption of data in motion or data at rest should be provided at the application layer.

DEFINITIONS

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.

EXCEPTIONS THAT MAY APPLY SUBJECT TO GTA APPROVAL

Several "IT as a Service" offerings are found in today's market, often in subscription or service-on-demand solutions. The following generic descriptions of service and deployment models should be referred to by agencies when requesting an exception from this standard:

Service Models:

Cloud Software as a Service (SaaS). 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.

Cloud Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

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

Deployment Models:

Private Cloud. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

Community Cloud. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

Public Cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Hybrid Cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).