

	<b>GEORGIA TECHNOLOGY AUTHORITY</b>	
<b>Title:</b>	<b>Placing Applications into Production</b>	
<b>PSG Number:</b>	SA-10-001.01	Topical Area: Application Development / Enabling Solution Operation and Use
<b>Document Type:</b>	Standard	<b>Pages:</b> 3
<b>Issue Date:</b>	9/15/2009	<b>Effective Date:</b> 3/15/2010
<b>POC for Changes:</b>	Enterprise Governance and Planning	
<b>Synopsis:</b>	Procedural requirements for placing applications into Production	

## PURPOSE

The purposes of this standard are as follows:

1. To introduce standard methods. With complex technological environments hosting ever more complex applications, standard procedures are more necessary to ensure that all work tasks in development efforts are coordinated.
2. To identify and repair design and coding errors earlier in a development lifecycle. Greater value to the State is derived from IT support practices oriented to prevention or, at a minimum, of discovery and repair at the earliest time during development, of design and coding errors. Delayed resolution of problems results in higher development costs and also may result in:
  - a. Customer hardship,
  - b. The added technical challenge and expense of fixing an application when it is already in production, and
  - c. Potential legal and statutory ramifications with may result from a breach of confidential data due to an intrusion attack on an improperly secured application.
3. Set responsibilities for common tasks related to placing information systems into production.

## SCOPE and AUTHORITY

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

## STANDARD

An agency that develops, customizes, or modifies IT application solutions (applications) for use in performing a business function shall develop and implement control procedures to place applications into production. The procedure shall be documented in the agency's IT policy and procedures manual and, at a minimum, shall:

1. Ensure that only authorized system development lifecycles (SDLC) are used by its application development staff and contracted development staff.
2. Incorporate in project work plans appropriate and timely tasks to plan application services, application production and test environments, and application testing at the earliest point during development or maintenance

processes to minimize development and maintenance costs. Work plan tasks shall include data center and operational personnel as appropriate to:

- a. Plan the application production environment and ensure that an appropriate test environment is available that appropriately mirrors requirements for production,
  - b. Develop transaction capacity forecasts and determine Service Level Management requirements,
  - c. Plan for all aspects of application, platform, network, database and information security,
  - d. Develop and implement data sharing arrangements with other applications,
  - e. Provide pre- and post-implementation impact analysis of configuration and security to determine effects of changes,
  - f. Perform selected regression testing after identified problems are resolved,
  - g. Prepare documentation for operations, backout and disaster recovery,
  - h. Plan and implement a program of application testing at appropriate stages of development that includes unit, system, integrated system, platform and network, and deployment readiness. Test plans and results shall form the basis of the Application Owners' recommendation to the CIO to go-live. Any part of the actual testing may be outsourced to one or more third parties, or to the Agency's IT operations provider. Irrespective of who actually executes the test collection, the Application Owners still remain responsible for their execution, and the results thereof. The Application Owners shall vouch to the Agency CIO that their application has successfully satisfied the Deployment Test Suite. Post deployment, should the application fail on any criteria, the Application Owners must explain to the CIO how their application received passing grades during earlier self-certification.
3. Ensure the application or change to application is submitted to pre-deployment reviews. When the Application Owners believe that the application or change is ready for deployment, they submit the application or change, in turn, to an Operational Review, a Security Accreditation Review and the Change Management procedure, obtaining the review and resolution of any shortcomings thereby identified.
  4. Require a go-live decision from the agency's Authorizing Official. The Deployment Certification initiates installation and shall be completed only following successful completion of all pre-deployment reviews and resolution of identified shortcomings.
  5. Require actual installation activities be performed by operational personnel, reinforcing separation of development and production activities.

## REFERENCES

- 1) *"Information Technology Infrastructure Library, version 3"*, Office of Government Commerce, London, UK, [www.best-management-practices.com/itil](http://www.best-management-practices.com/itil)

2) "Guide for Assessing the Security Controls in Federal Information Systems", NIST Special Publication 800-53A, Computer Security Division, National Institute of Standards and Technology

## **TERMS AND DEFINITIONS**

SDLC - A system development lifecycle (SDLC) is a systematic and orderly approach for solving business and IT related problems. A SDLC consists of a methodology of repeatable steps for delivering systems that meet the business requirements.

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.

## **RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES**

1. Management of IT Operations, policy (PO-09-002)
2. Enterprise Information Security Charter, policy (PS-08-005)
3. System Development Lifecycle, standard (SM-10-005)
4. Enterprise Performance Framework, standard (SM-10-006)
5. Enterprise Performance Management, standard (SM-10-007)

## **REFERENCE**

1. "Guide for the Security Certification and Accreditation of Federal Information Systems", NIST Special Publication 800-37, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD