

# 2012 Information Technology Governance Report (ITGR) Frequently Asked Questions (FAQ)

---

## **General Information, Process and System Access**

### **Q1: What is the ITGR and why does my agency have to report every year?**

**A:** The Information Technology Governance Report (ITGR) website is the tool used to collect IT information from state agencies to fulfill their legally mandated reporting requirements<sup>1</sup>. GTA uses this information to produce its legislatively required State IT Annual Report<sup>2</sup>. Together these reports help the state better understand its dependency on technology and how IT enables critical services for our citizens. The primary audience for these reports is the Governor, legislators and the public, but they also provide agency leaders and decision makers with data for setting priorities and making cost-effective, risk-based decisions regarding needed improvements.

Each year, state leaders make important decisions regarding strategic goals and objectives for the coming year. These reports help facilitate informed decision making in support of those goals. They provide uniform methods to regularly measure the health of information technology matters that affect how the state manages the IT services it provides and the information entrusted to its care.

The report also documents quantifiable progress in accomplishing strategic goals year over year as well as identifying areas that require more attention.

### **Q2: What are the fundamental assumptions that should be kept in mind, when completing the ITGR?**

**A.** The purpose of the ITGR is to produce information that will result in an ever maturing IT capacity for the state. The ITGR and the Annual Report are designed to collect and document metrics used to measure improvement over time. Because the ITGR is the data source that drives the State IT Annual Report, it is important that the qualitative information, quantitative data and cost and expenditure data be as valid and reliable as possible.

Previously, GTA collected several reports per year from agencies. It has focused its recent efforts to streamline the agency reporting process in the hope that the process would be less burdensome on the agencies and the information provided would be more accurate. This latest version of the ITGR was created with representative agency involvement. It is GTA's plan to offer agency leaders a tool that can be used to collect data about their IT functions throughout the year and not just when it is time to submit

---

<sup>1</sup> Agencies shall be required to submit information technology reports to the authority not more than twice annually and with such content as the board shall define. The authority shall establish standards for agencies to submit the reports or updates. Standards shall include, without limitation, content, format, and frequency of updates. O.C.G.A. § 50-25-7.10(b)

<sup>2</sup> The executive director shall publish in print or electronically an annual state information technology report ... O.C.G.A. § 50-25-7.10(a)

a report to GTA. This first revision of the ITGR should be seen as a tool that gives back something for the effort used to complete it. Time will tell and you will be the judge if this goal has been met as we rollout other revisions over time.

**Q3: What are the differences between this year’s and last year’s ITGR tool?**

**A:** Based on agency feedback from last year’s ITGR we have reviewed those recommendations to enhance the user experience and to make it available as an ongoing data repository and management tool for use throughout the year. The goal expanded from simply meeting legislative requirements to include providing agencies with the ability to review their IT and related activities year round. Some of the improvements include:

- The ability to attach a document(s) to support your agency response to a question
- Enhanced historical reporting will be available under the agency report section
- ITGR question cleanup
- The Project Portfolio section has been removed from ITGR and agencies will have to provide this information in the new GEMS tool.

**Q4: If I partially complete a Section, and plan to go back later to complete, will the data I entered be saved automatically?**

**A:** No. Each Section must be completed in its entirety or the partial data already entered will be lost. You must save it first.

**Q5: Does the ITGR time out after a predetermined number of minutes?**

**A:** Yes, the system **WILL** time out after 30 minutes of inactivity. The data will be lost as it will be if you close the page and want to go back to it later. This can be avoided by periodically saving your data.

**Q6: What is the deadline for submitting my agency’s ITGR?**

**A:** ITGR timeline and deliverables (all dates are for year 2012):

March 31	GTA publishes the IT Reporting Standard for that year
Year round	GTA makes ITGR system available to agencies to complete their ITGR online. Starting this year the ITGR system is available year-round for agencies to maintain and update their information as the environment changes rather than waiting for June of each year.
July 31	Completed and Approved ITGR due. Snapshot taken of submitted agency data on Aug. 1 ITGR locked until agency contacts are notified that the tool is unlocked.
Oct 1	GTA publishes annual State IT Report. This report includes the Enterprise Information

**Q7: What time period does the report cover?**

**A:** The report pertains to the fiscal year that just ended. For example, the report due on July 31, 2012 will cover the reporting period of FY 2012 (July 1, 2011 to June 30, 2012).

**Q8: What is the consequence to my agency if we aren't able to show progress from the 2011 Plan of Actions and Milestones (POA&Ms)?**

**A:** The ITGR is intended to collect information regarding the security, reliability and effectiveness of an agency's use of information technology. To accomplish that goal, each agency must report its information accurately. There may be many reasons why an agency fails to show progress against its POA&Ms including higher priorities and budget constraints. The ITGR is not used to pass judgment on an agency but instead to initiate conversations with state leadership.

Previous years' information is used as baselines for the future. It is the intent that over time agencies and state leadership will be able to see how agency technology and management processes are maturing toward a more stable and efficient environment. In addition, the State IT Report should document these same issues on a statewide level.

**Q9: When will the ITGR system be available and how do I get access?**

**A:** The ITGR system is now operational and available year round.

Agency personnel must be registered online at the ITGR website to gain access to the system. User verification and account activation will be communicated to the user via email messages, normally within 24 hours.

For users who were registered last year you are still registered. The user IDs, passwords, and security questions from last year have been carried forward. However, prior-year users will receive an email asking them to respond and revalidate their accounts.

If anyone needs assistance or has forgotten their password, they may click on the ["forgot your password" link on the homepage](#) and request a new password. They will need to make sure they know the answers to the security question that were setup when they first registered.

**Q10: Can I register for an ITGR system account on behalf of my commissioner or others in my agency who need access?**

**A:** Yes. Go through the online registration process as you would for yourself, but enter the person's data for whom the user account is being created. The ITGR administrator will validate the user data and notify the user via email when their account is created.

If your commissioner, or other personnel, were registered last year, their accounts should still be in the system. However, they will have to be re-validated as personnel assignments and roles are continually changing.

If you have difficulty accessing or need a password reset, contact the system administrator via directions on the website. Please be sure to select "approver" from the User Type drop down when registering your "Commissioner." Only the enrolled Commissioner will be allowed to approve / submit the report.

**Q11: Do I have to use the ITGR System to do my reporting?**

**A:** Yes. All reports must be submitted through the ITGR system. No other forms will be acceptable but detail used to support your report is available through the "attachment" feature include in this release of ITGR.

**Q12: Who in my agency is required to complete this report?**

**A:** Per the Governor's executive order, the agency head (exact titles will vary) is responsible for reporting the status of the information technology that supports their agency. He/She may delegate the task of completing some or all the report to one or more personnel within that agency.

The ITGR system accommodates multiple users from a single agency to access/update their agency's report. This allows, at the discretion of the agency, various agency representatives with specific subject matter expertise (SME) to accurately complete relevant sections of the report. Please assist by reviewing the topic areas and ensuring that the appropriate staff are actively involved in your agency's reporting.

**Q13: I have finished my ITGR but I cannot select the "Finalize and Approve" option in the ITGR website, why not?**

**A:** Only a user designated as the "**Agency Approver**" has permissions to approve and submit the finished ITGR. Each agency must designate **one** user as "**Agency Approver**" during the registration process. The Agency Approver is the only user role that can finalize and approve the completed agency ITGR. Ideally, your agency head has this designation. However, he/she may delegate this designation to someone else in the agency by providing GTA with a formal request delegating someone to submit/approve the agency ITGR on his/her behalf (see next Q&A).

**Q14: My agency's Executive Director wants me to sign off as the "Agency Approver" for the completed ITGR. Can I do that?**

**A:** Yes. When you register on the ITGR website, select "Agency Approver" as your role in the user profile page. However, your agency executive director or commissioner must formally delegate this designation to you using the template letter below and provide the letter to GTA. Approver delegation DOES NOT carry

over from year to year and a new letter must be completed for each reporting year. The ITGR administrator must verify that the letter was received before granting you this access. A copy of the signed Delegation Letter must be sent to GTA so that your "user type" will be changed to "Approver" to be able to submit your agency report.

Please refer to the Helpful Links section on the ITGR Home page at: <https://services.georgia.gov/gta/itgr/startLogin.do> for a suggested delegation letter

**Q15: My agency head or designee has locked/finalized our agency's ITGR but we need to make some changes. Can we have it unlocked?**

**A:** After the agency's report is marked as "Finalized and Approved" the report will be locked and available in READ-ONLY mode. Agencies must contact the [ITGR Administrator](#) if they need to make changes and it is BEFORE the August 1 reporting deadline.

With very few exceptions, after the reporting deadline the ITGR system will be READ-ONLY for GTA to extract and analyze the data for reporting purposes. Agency contacts will be notified when the ITGR is unlocked and again available for updates.

**Q16: What is meant by the term "Enterprise"?**

**A:** The term generally applies to an organization with common or unifying business interests and can mean different things, depending on one's perspective. For example, 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.

*\*\*For the purposes of the ITGR consider the term to mean the State of Georgia level.\*\**

**Q17: Our agency will not be able to complete the ITGR by the July 31<sup>st</sup> deadline. Can we request an extension?**

**A:** Extension requests are discouraged but are at times unavoidable and will be handled on a case-by-case basis. All extension requests must be approved by the State CIO Calvin Rhodes. Contact the [ITGR Administrator](#) for more information.

**Q18: Who do I contact if I have other questions or need help with the ITGR website?**

**A:** Please direct all ITGR system and security related questions to the ITGR Administrator, [ITReports@gta.ga.gov](mailto:ITReports@gta.ga.gov) or 404-463-8474.

## **Agency Profile**

### **Q19: How do I know or where do I find my agency's Branch of Government?**

**A:** Contact your agency head. Your agency head should have this information.

### **Q20: How do I find out if my agency head was appointed or elected?**

**A:** Contact your agency head. Your agency head should have this information.

### **Q21: How do I determine my reporting relationship with other agencies?**

**A:** To determine your reporting relationship with other agencies, use the following definitions:

- a.) Self: State agencies that are responsible ONLY to themselves in the area of technology, security and risk management;
- b.) Self and Others: State agencies that report on their own behalf as well as for those agencies matrixed to them with a dependency to receive Information Technology services and/or risk management functions;
- c.) Other: State agencies that are matrixed to another agency/organization and are dependent on that agency to receive Information Technology services and/or risk management and technology reporting functions.

*NOTE: All Agencies retain fiduciary responsibility for the information security of the information they own regardless of who actually operates the system on a day to day basis such as with an outsourced service provider or matrixed relationship.*

### **Q22: Do I include information for an agency(-ies) that is attached to mine for administrative purposes in the ITGR that I submit for my agency ?**

**A:** Yes. Normally the data for any agency that is attached to another for administrative purposes would be included in the ITGR for the "parent" agency. The parent must clearly indicate the agency or agencies included in their ITGR. In some situations the attached agency receives no IT, security, business continuity services or application/project management from the "parent". The parent assumes no responsibility for such services. In that case the agency should indicate no information is included for attached agencies in the "Agency Profile Section". If an agency's ITGR data includes some but not all attached agencies, please name those included and those not included.

### **Q23: What is an MOU/MOA?**

**A:** An MOU/MOA for Information Technology Services and Reporting is a written agreement between two agencies detailing the services to be performed for one agency by another. Such an agreement is required for the reporting relationships outlined in the above question.

**Q24: What/Who is a CIO?**

**A:** An agency Chief Information Officer is the most senior executive in an organization responsible for ensuring that information technology and resources are acquired and managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and agency goals/priorities. He/she holds ultimate responsibility for the technology assets and security of information assets held by the agency.

**Q25: What/Who is a SAISO?**

**A:** An agency Senior Agency Information Security Officer; formerly referred to as Agency ISO. This is the formal title (under [National Institute of Standards and Technology](#)) of the primary/lead/senior person in each agency managing the information security program for that agency.

**Q26: Why are you asking about a Privacy Officer? Is it required?**

**A:** A Privacy Officer is an individual within the agency with specialized expertise regarding privacy matters (both personal and professional) and whose role is to ensure awareness of data privacy issues, and compliance with regulation, legislation and policy. A Privacy Officer is not required. However, with ever increasing legislation and legal issues regarding privacy matters (both personal and professional), industry is recognizing the need to rely on individuals with specialized expertise in the area of privacy to focus in these matters. This question identifies those agencies that have chosen to create this function if the agency collects or uses federally regulated information. The SAISO should know if their agency is required to have a privacy officer.

**Q27: Who/What is a BC Planner / Coordinator?**

**A:** Business Continuity Planner or Coordinator: A role within the Business Continuity Management program that coordinates planning and implementation for business process sustainment and overall recovery of an agency during an emergency.

**Q28: Who/What is a PMO?**

**A:** **Project Management Office**, also known as a PMO. The Director or Manager is the individual responsible for tracking the agency projects.

**Q29: How do I know if my agency is identified as an ESF agency?**

**A:** ESF means Emergency Support Function- Agencies are identified in the Governor's EO and the Georgia Emergency Operations Plan as having primary and/or support responsibilities to provide essential services or support for those services during a man made, natural, or environmental state emergency.

Click this link to search and see if your agency is listed as ESF in the [Governor's Executive Order](#) for your agency's name.

Click here to access the [Georgia Emergency Management Agency](#) website for more information on the GEOP.

**Q30: How do I calculate the total number of agency employees?**

**A:** Use the sum of the total number of filled full and part-time State employee positions as of current date and the number of active contractors employed in any capacity by the agency. Please access the "Help" button next to this question for more information.

*\*\*Remember to include the employees and contractors of those agencies for which your agency has taken reporting responsibility.\*\**

**Q31: I am not responsible for budget, how do I complete the questions related to Information Technology costs expended over the past Fiscal Year and budget for next Fiscal Year?**

**A.** The budget section of your agency or the individual that handles the function is normally the best source for this data. That person or persons can enter the data directly (must be registered as a contributor) or supply the information to another person.

**Q32: We're a GETS agency, isn't GTA, through its vendors, responsible for the risk and security management of our systems?**

**A:** No. Under GETS, GTA manages the IT service provider/s ONLY. The service provider operates and maintains the technology as directed by the system/business owners. Each GETS agency (or any agency using a service provider) always retains ownership of its business, and ultimately responsible for ensuring the information technology adequately supports that business. Therefore, Business Owners must define the operational and security requirements for its data and ensure those requirements are being met. The service provider is responsible for meeting those requirements as requested, directed and paid for by the customer in the most efficient manner possible.

**Q33: We are not a GETS agency but our IT is provided by an outside third party vendor. Are we still responsible for reporting on our IT services?**

**A:** Yes. The same as with GETS agencies, the third party service provider operates and maintains the technology as directed by your agency. Any agency using a service provider always retains ownership of its business processes and is always responsible for ensuring adequate protection of the data and effectiveness of the technology used to support that business. Therefore, Business Owners must define the operational and security requirements for its data and ensure

those requirements are being met. The service provider is responsible for meeting those requirements as requested, directed and paid for by the customer in the most efficient manner possible.

## **AGENCY SECURITY**

### **Q34: What is a Security Program?**

**A:** A formal documented security program is an internal information security infrastructure that includes ALL of the following program elements:

- a.) Security management organization that assesses, 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.) Internal policies and procedures
- d.) An Incident Management and Response capability
- e.) Security Education and Awareness component
- f.) Assessment, Compliance and Enforcement mechanisms

### **Q35: What is Information Security Governance?**

**A:** Information Security Governance is the development, maintenance and enforcement of security policies, standards, guidelines, processes and procedures.

Click here for the [Enterprise Security Policies and Standards](#).

### **Q36: What is Security Categorization?**

**A:** The level of risk (High, Moderate, or Low) that an agency poses to the State's enterprise and/or their constituency for the security objectives of Confidentiality, Integrity, and Availability. 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:

**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

**Q37: When asked about “How many agency employees completed annual security awareness training” do you mean how many completed annual training during the Fiscal Year for which we are reporting?**

**A:** Yes. Security awareness training is required to be completed every year fiscal year by every employee.

**Q38: What do you mean by “Readily Available?”**

**A:** "Readily Available" means easily accessible by employees at any time.

**Q39: What is a “legitimate” security issue?**

**A:** A legitimate security issue is associated with any incident that upon examination is determined to be an inadvertent or an intentional breach or violation of management, operational and/or technical security policies.

**Q40: What is a Security Incident Response Plan?**

**A:** A Security Incident Response Plan is your agency's methodology for preventing, monitoring, detecting, containing, responding, recovering, reporting and escalating threats or violations of security policy and/or controls and limiting their impact to the organization. See Enterprise PSG: SS-08-004 [Incident Response and Reporting Standard](#)

**Q41: Does my agency have to have a documented Security Incident Management Plan?**

**A:** Yes, see Enterprise PSG: SS-08-004 [Incident Response and Reporting Standard](#)

**Q42: What is Business Continuity?**

**A:** The ability of an agency to provide service and support for its constituents and to maintain its viability before, during, and after an event.

**Q43: What is a Business Continuity Management Program?**

**A:** It is an ongoing management and governance process supported by senior management and resourced to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans and ensure continuity of products/services through exercising, rehearsal, testing, training, maintenance and assurance.

**Q44: What is Business Continuity Planning (BCP)?**

**A:** The process which occurs, based on risk evaluation and business impact analysis, to identify procedures, priorities and resources for:

- emergency response operations;
- business continuity strategies for the agency's functions and supporting infrastructure;
- crisis communications; and coordination with external agencies.

**Q45: What is a Business Continuity Plan?**

**A:** Process of developing and documenting arrangements and procedures that enable an agency to respond to an event that lasts for an unacceptable period of time and return to performing its critical functions after an interruption.

**Q46: Is a Business Process the same as a business plan?**

**A:** No, a "business process" is owned and carried out by the business side of the agency, not the IT department, although a business process may depend upon the IT department. An agency business process contributes to the delivery of a product or service to the agency clients. For example, the Department of Revenue needs a methodology to receive, deposit and account for tax revenues in order to deliver services to their business customers the taxpayers. "Core" business processes are absolutely required to accomplish business.

**Q47: What is LDRPS?**

**A:** LDRPS (Living Disaster Recovery Planning System) is a tool provided by GTA to agencies free of charge used to assist and guide them in the Business Continuity (BC) and Disaster Recovery (DR) Planning process. The end result of those BCP activities are viable BC & DR plans.

**Q48: How does my agency obtain access to LDRPS ?**

**A:** Please contact Jack Welch via email @ [jack.welch@gta.ga.gov](mailto:jack.welch@gta.ga.gov) or by phone @ 404-463-5907.

 ***Production System Inventory***

**Q49: Explain what you classify as a "system" ?**

**A: An information system is, "A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, "44 U.S.C., Sec. 3502. Examples of information resources are workstations, servers, minor applications, and networks.**

NOTE: For the purposes of the State IT Governance Report, only Production systems are reported (not major business applications within the system boundaries).

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.

**Q50: Why do I have to document the characteristics of all my systems?**

**A:** To effectively run and improve a business, the business must understand the risks. To understand the risks and effectively mitigate them, the business must know what it has, how it uses it and what it needs. To know this and make crucial business decisions, systems must be fully and accurately documented. Please provide information for each system your agency operates.

**Q51: What are the Security Objectives?**

**A:** The security objectives are:

**Confidentiality** - to prevent unauthorized disclosure of information

**Integrity** - to prevent unauthorized modification, destruction or disputable authenticity of information

**Availability** - to prevent disruption of access or use of information or an information system

**Q52: What is an Information System Security Plan?**

**A:** System Security plans are living documents that are developed, reviewed and updated throughout the system's lifecycle to accurately reflect the current state of the information system. See Enterprise PSG: SS-08-028.01 [System Security Plans Standard](#).

**Q53: What is a FISMA-based security assessment?**

**A:** A FISMA-based assessment of system or application security controls is based on the FISMA risk management framework and NIST SP800-53. (The Federal Information Security Management Act formed the basis of the National Institute of Standards for Technology reference SP800-53, which is endorsed and adopted by GTA for security management)

Required by Enterprise PSG SS-08-042.01, [Independent Security Assessments Standard](#).

**Q54: Who is the Business Owner?**

**A:** The Business Owner is the individual 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. See Enterprise Standards: SA-10-001.01 [Placing Applications into Production](#).

**Q55: What is a Disaster Recovery Plan (DRP)?**

**A:** A disaster recovery plan is an element of BC Planning that documents the processes and procedures to identify, to prioritize and to restore the IT operations which support business following an interruption.

**Q56: Who is the service provider?**

**A:** The State's Enterprise Operating Vendors are those who operate GETS (IBM and AT&T).

**Q57: How do I calculate agency FTEs and contractor FTE's?**

**A:** FTE - Full Time Equivalent State employees is a calculated figure to indicate the proportion of full time labor applied to a given task. It is calculated as follows:

Calculate FTE for State employee positions

- A staff position applied full-time in support = 1.0 FTE
- If a portion of the position is applied in support (say 10%) =  $1.0 \times .10 = .10$  FTE
- If 5 staff positions each spend 30% in support =  $5 \times .30 = 1.50$  FTE
- If part-time hourly position works 500 hours annually and spends 10% of that supporting this application, the FTE calculation is:  $500 \times .10$  divided by 2080 = .02 FTE (rounded).

 ***Business Application Inventory***

**Q58: Explain what you classify as a "business application"?**

**A:** An application is a set of computer programs related to a business function which allows the business to achieve operational goals. Please complete a sheet for each Business Application your agency uses.

**Q59: Who is an Application Business Owner?**

**A:** The Business Owner is an individual stakeholder (usually an executive) who serves as the primary customer and advocates for the applications and technology that support their business functions and that establishes and funds the agency's/business units' strategic objectives.

**Q60: What is a subprogram?**

**A:** For budgeting purposes OPB divides an agency's functions into "programs" based on its strategic goals and objectives. If necessary these programs are

subdivided based on more specific strategic goals and objectives into "subprograms". These program and subprograms have associated budgets. Business applications support one or more programs and/or subprograms within an agency. For each application, provide the name/s of the program/s and/or subprogram/s that are supported by this application

**Q61: What is a Program Code (PeopleSoft Financial Code)?**

**A:** The General Ledger designation used to track expenditures for the program.

**Q62: How essential is this application to the agency's core business ?**

**A:** *Critical* - Agency goals would not be met if application did not function.  
*Important* - The agency could operate but may not meet its critical goals if the application did not function.  
*Supportive* - The application only supports basic agency functions and is not necessary to achieve goals.

**Q63: What is an Application Security Plan?**

**A:** An application security plan is an application specific section of the system security plan.

**Q64: Who is the Application Data/Business Owner?**

**A:** The Business Owner is the individual 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. See Enterprise Standard SA-10-001.01 at [Placing Applications into Production Standard](#)

**Q65: What is the hardware platform and operating system hosting the application?**

**A:** Platform" is the type of computing hardware the application is running on. "Operating" System is the core system software running on a hardware platform.

**Q66: Are you asking whether or not a customer satisfaction survey was conducted on our applications during this fiscal year?**

**A:** Yes. Answer NO if the survey was done prior to FY 2012.