

# STATE OF NORTH CAROLINA

## OFFICE OF THE INFORMATION TECHNOLOGY SERVICES INFORMATION TECHNOLOGY GENERAL CONTROLS

APRIL 2012

### PERFORMANCE AUDIT

OFFICE OF THE STATE AUDITOR

BETH A. WOOD, CPA

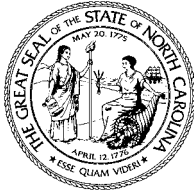
STATE AUDITOR

**OFFICE OF THE INFORMATION TECHNOLOGY SERVICES**

**INFORMATION TECHNOLOGY GENERAL CONTROLS**

**APRIL 2012**

**PERFORMANCE AUDIT**



**Beth A. Wood, CPA**  
State Auditor

STATE OF NORTH CAROLINA

# Office of the State Auditor

2 S. Salisbury Street  
20601 Mail Service Center  
Raleigh, NC 27699-0601  
Telephone: (919) 807-7500  
Fax: (919) 807-7647  
Internet  
<http://www.ncauditor.net>

## AUDITOR'S TRANSMITTAL

---

April 17, 2012

The Honorable Beverly Eaves Perdue, Governor  
Members of the North Carolina General Assembly  
Jonathan Womer, State Chief Information Officer

Ladies and Gentlemen:

This report presents the results of our performance audit of information technology general controls at the State of North Carolina Office of Information Technology Services (ITS). Our audit was performed by authority of Article 5A of Chapter 147 of the *North Carolina General Statutes* and was conducted in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States.

The objectives of the audit were to review the general controls as they pertain to ITS' information technology. The results of our audit disclosed deficiencies that are considered reportable under *Government Auditing Standards*. These items are described in the Audit Findings and Responses section of this report along with your responses thereto, except those regarding access controls which, due to their sensitivity, are reported to you by separate letter and should be kept confidential as provided in *North Carolina G.S. 132-6.1(c)*.

*North Carolina General Statutes* require the State Auditor to make audit reports available to the public. Copies of audit reports issued by the Office of the State Auditor may be obtained through one of the options listed in the back of this report.

A handwritten signature in cursive script that reads "Beth A. Wood".

Beth A. Wood, CPA  
State Auditor

# TABLE OF CONTENTS

---

	PAGE
BACKGROUND .....	1
OBJECTIVES, SCOPE, METHODOLOGY, AND RESULTS .....	3
ORDERING INFORMATION .....	7

[ This Page Left Blank Intentionally ]

## BACKGROUND

---

The General Assembly, “in recognition of the need to better manage the acquisition and use of information technology in general state government” created the Office of Information Technology Services in 1983 (at the time called State Information Processing Services) by consolidating the State Computer Center and similar operations at the Department of Transportation, the Department of Correction, and the Employment Security Commission. Originally placed within the Department of Administration, the Office of Information Technology Services (ITS) was later moved by executive order to the Office of State Controller and the Department of Commerce on March 1, 1987 and April 14, 1997, respectively. Effective November 1, 2000, Senate Bill 1345 of the 1999 Session of the General Assembly transferred ITS from the Department of Commerce to the Office of the Governor as well as expanded its responsibilities to include enterprise management of information technology (IT) assets.

General Statutes (GS) §147-33.83 stipulates, among other things, that ITS shall provide cities, counties, and other local governmental units with access to ITS information resource centers and services. These services are provided through use of mainframe computers, distributed computing servers, and statewide voice, data, and video networks. ITS operates as an internal service fund and, as such, the costs of providing services are recovered through direct billings to clients.

General Statutes (GS) §147-33.76, State Information Technology Management, stipulates the State Chief Information Officer (CIO) shall be responsible for developing and administering a comprehensive long-range plan to ensure the proper management of the State's information technology resources. The State CIO shall set technical standards for information technology, review and approve major information technology projects, review and approve State agency information technology budget requests, establish information technology security standards, provide for the procurement of information technology resources, and develop a schedule for the replacement or modification of major systems. The State CIO is authorized to adopt rules to implement this Article.

[ This Page Left Blank Intentionally ]

## OBJECTIVES, SCOPE, METHODOLOGY, AND RESULTS

---

### OBJECTIVES, SCOPE, AND METHODOLOGY

As authorized by Article 5A of Chapter 147 of the *North Carolina General Statutes*, we have conducted a performance audit at the State of North Carolina Office of Information Technology Services (ITS). The audit was performed as part of our effort to periodically examine and report on the general IT controls for the financial applications hosted by ITS and that are critical to the State of North Carolina Comprehensive Annual Financial Report (CAFR) and the federal single audit.

The objective of this audit was to determine the effectiveness of general controls which influence the overall organization and operation of ITS. Our audit was conducted between February 1, 2011 and September 30, 2011.

The scope of this audit included the financial applications hosted by ITS that are critical to the State of North Carolina Comprehensive Annual Financial Report (CAFR) and the federal Single Audit. The scope of our audit included the following IT general controls categories: general security, access controls, program maintenance, systems software, systems development, physical security, operations procedures, and disaster recovery, which directly affect ITS' computing operations.

To accomplish our audit objectives, we gained an understanding of ITS' policies and procedures, interviewed key ITS administrators and other personnel, examined system configurations, tested on-line system controls, reviewed appropriate technical literature, and reviewed computer-generated reports.

As a basis for evaluating general controls, we applied the guidance contained in *The State of North Carolina Statewide Information Security Manual* as the foundation for information technology security for North Carolina state agencies. It sets out the standards required by G.S. §147-33.110, which directs the State Chief Information Officer (State CIO) to establish a statewide set of standards for information technology security to maximize the functionality, security, and interoperability of the State's distributed information technology assets. The security manual sets forth the basic information technology security requirements for state government.

Additionally, we applied the guidance contained in the *Control Objectives for Information and Related Technology* (CobiT), created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute. CobiT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. CobiT enables clear policy development and good practice for IT control throughout organizations. CobiT emphasizes regulatory compliance, helps organizations to increase the value attained from IT, enables alignment and simplifies implementation of the CobiT framework. CobiT standards state that management should implement controls to ensure that the organization's policies and procedures are designed to adequately protect critical and sensitive data from unauthorized access from both internal and external users.



## **OBJECTIVES, SCOPE, METHODOLOGY, AND RESULTS (CONTINUED)**

---

ITS management, pursuant to North Carolina General Statute §143D-7, bears full responsibility for establishing and maintaining a proper system of internal control which includes information technology (IT) general controls. A proper system of internal control is designed to provide reasonable, rather than absolute, assurance that relevant objectives are achieved. Because of inherent limitations in internal controls, unauthorized access to data, for example, may nevertheless occur and not be detected. Also, projections of our evaluation in this report of general controls to future periods are subject to the risk that, for example, conditions at ITS may change or compliance with ITS' policies and procedures may deteriorate.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

### **RESULTS**

The results of our audit disclosed internal control deficiencies that are considered reportable under *Government Auditing Standards*. The deficiencies noted result from the lack of a current service-level agreement and failure to implement access controls in four critical areas.

#### **Access Controls**

Details about the failure to implement adequate access controls, due to their sensitive nature, were communicated to ITS management in a separate letter pursuant to *North Carolina G.S. 132-6.1(c)*

#### **Service-Level Agreement**

A service-level agreement (SLA) is a negotiated agreement between two parties, where one is the client and the other is the service provider. The SLA records common understanding about services, priorities, responsibilities, guarantees, and warranties. Each area of service scope should have the "level of service" defined.

During our audit, we performed audit procedures that covered the platform supporting the state's human resources and payroll application known as BEACON. The Office of Information Technology Services (ITS) hosts the BEACON application platform for the Office of the State Controller (OSC). Approximately 90,000 state employees are served by the BEACON application. We requested the SLA between ITS and OSC for the BEACON application. ITS provided an SLA with an effective date of February 13, 2009. ITS also provided an unexecuted draft SLA for 2010.

Throughout the audit, ITS continuously responded to questions on specific controls that these concerns were the responsibility of OSC and not of ITS but was unable to provide specific references to the 2009 SLA to support these responses. Best practices established by the

## **OBJECTIVES, SCOPE, METHODOLOGY, AND RESULTS (CONCLUDED)**

---

Control Objectives for Information and Related Technology (CobiT) and ITIL (IT Infrastructure Library) provide that service level agreements should clearly define the roles and responsibilities between the organization and the service provider.

The absence of a current SLA which clearly defines the roles and responsibilities for OSC and ITS in the management and support of the BEACON system could compromise the security of the application or data hosted by ITS. Both OSC and ITS may assume the other party is responsible for managing the application, system configurations, and security of the BEACON system. This could potentially lead to deficiencies in internal control. Annually renewing or updating the SLA will provide both ITS and OSC the opportunity to strengthen and enhance terms and conditions, and clarify and refine the statement of scope and performance requirements.

### **RECOMMENDATION**

We recommend that ITS and OSC annually review and execute the SLA for the services required to manage the BEACON application and infrastructure. The SLA should clearly define the roles, responsibilities of both OSC and ITS and the service levels required of ITS.

### **AGENCY RESPONSE**

ITS, working with the Beacon Project team, created the Operational Expectation Document to define roles and responsibilities of each agency as part of the Beacon implementation. The MOU, including the SLA, was created separately and implemented. ITS will work with the OSC/Beacon team to review, update and confirm roles and responsibilities and to update the SLA as needed on an annual basis. The Operational Expectation Document will be referenced within the SLA. Target for completion is June 15th, 2012.

[ This Page Left Blank Intentionally ]

## ORDERING INFORMATION

---

Audit reports issued by the Office of the State Auditor can be obtained from the web site at [www.ncauditor.net](http://www.ncauditor.net). Also, parties may register on the web site to receive automatic email notification whenever reports of interest are issued. Otherwise, copies of audit reports may be obtained by contacting the:

Office of the State Auditor  
State of North Carolina  
2 South Salisbury Street  
20601 Mail Service Center  
Raleigh, North Carolina 27699-0601

Telephone: 919/807-7500

Facsimile: 919/807-7647