STATE OF NORTH CAROLINA

OFFICE OF THE STATE CONTROLLER

BEACON HUMAN RESOURCES AND PAYROLL SYSTEM

INFORMATION TECHNOLOGY GENERAL CONTROLS

JUNE 2012

PERFORMANCE AUDIT

OFFICE OF THE STATE AUDITOR

BETH A. WOOD, CPA

STATE AUDITOR

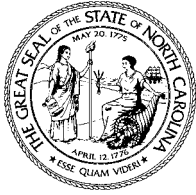# OFFICE OF THE STATE CONTROLLER

BEACON HUMAN RESOURCES AND PAYROLL SYSTEM

INFORMATION TECHNOLOGY GENERAL CONTROLS

JUNE 2012

PERFORMANCE AUDIT

[This Page Left Blank Intentionally]

AUDITOR'S TRANSMITTAL

June 29, 2012

The Honorable Beverly Eaves Perdue, Governor
Members of the North Carolina General Assembly
David T. McCoy, State Controller

Ladies and Gentlemen:

We are pleased to submit the results of our performance audit of information technology general controls at the State of North Carolina Office of the State Controller (OSC) for the BEACON Human Resources and Payroll System (BEACON).

The purpose of our audit was to review information technology general controls as they pertain to the BEACON system.

Our audit was performed by authority of Article 5A of Chapter 147 of the *North Carolina General Statutes* and was conducted in accordance with generally accepted government auditing standards.

The results of our audit disclosed two deficiencies and other recommendations that are considered reportable under *Government Auditing Standards*. These items regarding access controls and security policies which, due to their sensitivity, are reported by separate letter and should be kept confidential as provided in *North Carolina G.S. 132-6.1(c)*. The results of our audit also disclosed the lack of a current service level agreement that is described in the Results section of this report along with your response thereto.

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.

We wish to express our appreciation to the Controller's staff for the courtesy, cooperation, and assistance provided us during the audit.

Beth A. Wood

Beth A. Wood, CPA
State Auditor

TABLE OF CONTENTS

[This Page Left Blank Intentionally]

BACKGROUND

The State of North Carolina Office of the State Controller's (OSC) Human Resources and Payroll System (BEACON) was implemented as the statewide or enterprise technology solution for the human resources and payroll needs of state agencies.

The single integrated human resources and payroll system was intended to leverage best practices and provide updated human resource and payroll functionality including web-based employee and manager self-service functionality. The State decided to leverage the Department of Transportation's purchase and experience implementing an ERP suite marketed by software vendor SAP. The State created a project team consisting primarily of employees of OSC and outside consultants to integrate the SAP software into the state's business processes. The project was branded as BEACON, which stands for Building Enterprise Access for North Carolina's Core Operation Needs. The modules implemented were Organizational Management, Personnel Administration, Time Management, Benefits, Payroll, and some components of Financials.

The BEACON system is currently supported by OSC and the State of North Carolina Office of Information Technology Services (ITS). ITS personnel, supplemented on a very limited basis with SAP consultants when a particular skill or level of expertise is required to manage the application software. OSC is responsible for the help desk operations developed to serve BEACON system users. The OSC BEST Shared Services section performs this function. The BEACON system operates on an infrastructure provided by ITS.

ITS is responsible for the administration of the servers and for providing an operating system for the database management system and the BEACON application. OSC is responsible for maintaining the application software and performing database administration activities. ITS provides the platform for the underlying Oracle database management system that the BEACON system requires, while OSC is responsible for maintaining the "customer" databases that are part of the business application software. A service level agreement between OSC and ITS describes the level of service ITS will provide to OSC as the hosting provider.

OSC is responsible for the internal control that ensures the BEACON application software processes complete, accurate, and valid transactions. ITS is responsible for the technology infrastructure and related internal control upon which the BEACON system operates. State agencies are responsible for end-user processes and related internal controls for employee data and other agency specific master data settings upon which the BEACON system processing rules rely. According to OSC, approximately 90,000 state employees are served by the BEACON system, processing an annual payroll of approximately $3.4 billion.

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 the State Controller (OSC). The audit was performed as part of our effort to periodically examine and report on the general IT controls for the financial applications 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 information technology (IT) general controls for the operation of the OSC Human Resources and Payroll System (BEACON) that were designed, implemented, and operated throughout the period of July 1, 2011 to December 31, 2011. We conducted our audit between February 1, 2012 and June 15, 2012.

As owner of the BEACON application, OSC is responsible for specifying the control objectives, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting controls to achieve the related control objectives. OSC provided us a list of key controls for BEACON application processing.

State agencies (user entities) are responsible for ensuring that data entered into the application is complete and accurate. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

The scope of our audit included the following IT general controls categories: general security, IT governance, program maintenance and change controls, operations procedures, physical security, disaster recovery, and access controls, which directly affect the BEACON system.

To accomplish our audit objectives, we gained an understanding of OSC's policies and procedures, interviewed key OSC administrators and other personnel, examined system configurations, tested system controls, reviewed appropriate technical literature, and inspected computer-generated reports. We performed a gap analysis to identify if key controls were sufficient to achieve the control objectives specified by OSC.

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 *Reporting on Controls at a Service Organization (SOC)*, created by the American Institute of Certified Public Accountants (AICPA). The AICPA's SOC guidance establishes the requirements for reporting on a service organization's description of its system and its controls that are likely to be relevant to user entities' internal control over financial reporting. In addition to financial reporting controls, the AICPA's SOC guidance also establishes the requirements for reporting on a service organization's controls intended to mitigate risks related to security, availability, processing integrity, confidentiality, and privacy (collectively known as the *Trust Services Principles*).

OSC 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 OSC may change or compliance with OSC's 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 two deficiencies and other recommendations that are considered reportable under *Government Auditing Standards*. These items regarding access controls and security policies which, due to their sensitivity, are reported to OSC management by separate letter and should be kept confidential as provided in *North Carolina G.S. 132-6.1(c)*. The results of our audit also disclosed the lack of a current service level agreement that was reported in our "*Office of the Information Technology Services Information Technology General Controls Performance Audit*" dated April 2012.

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. The SLA between OSC and Information Technology Services (ITS) is not current as the effective date is February 13, 2009.

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 OSC continue to cooperatively work with ITS to 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

As noted in your report, the Office of the State Controller (OSC) is currently operating under a service-level agreement with the Office of Information Technology Services (ITS) dated February 13, 2009. OSC and ITS began discussions to update the agreement in April 2010. Although several draft revisions have been reviewed, a new agreement has not been finalized. OSC will continue to work with ITS to update the current service-level agreement. In addition, we will also strive to update the agreement annually.

.

ORDERING INFORMATION

Audit reports issued by the Office of the State Auditor can be obtained from the web site at 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