STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2017-211
June 2017

UNIVERSITY OF SOUTH FLORIDA

Banner® Enterprise Resource Planning (ERP) System Hosting Operations

Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the period of our audit, Dr. Judy L. Genshaft served as President of the University of South Florida and the following individuals served as Members of the Board of Trustees:

Brian D. Lamb, Chair	Stanley I. Levy
Jordan B. Zimmerman, Vice Chair	Harold W. Mullis, Esq.
Mike Carrere	John B. Ramil
Dr. James Garey [a]	Byron E. Shinn
Stephanie E. Goforth	James Stikeleather
Christopher Griffin [b]	Nancy H. Watkins
Scott L. Hopes	

[a] System faculty council president (equivalent to faculty senate chair referred to in Section 1001.71(1), Florida Statutes).

[b] Student Body President.

The team leader was Rebecca Ferrell, CISA, and the audit was supervised by Heidi Burns, CPA, CISA.

Please address inquiries regarding this report to Arthur Hart, CPA, Audit Manager, by e-mail at arthart@aud.state.fl.us or by telephone at (850) 412-2923.

This report and other reports prepared by the Auditor General are available at:

FLAuditor.gov

Printed copies of our reports may be requested by contacting us at:

State of Florida Auditor General

Claude Pepper Building, Suite G74 • 111 West Madison Street • Tallahassee, FL 32399-1450 • (850) 412-2722

UNIVERSITY OF SOUTH FLORIDA
Banner® Enterprise Resource Planning (ERP) System Hosting Operations

SUMMARY

The University of South Florida (University) provides specific information technology (IT) hosting and services related to the Banner® by Ellucian (Banner®) Enterprise Resource Planning (ERP) system for Florida Gulf Coast University (FGCU), New College of Florida (NCF), and the University of North Florida (UNF). Banner® is used by FGCU, NCF, and UNF for recording, processing, and reporting finance, human resources, and student transactions. This operational audit focused on evaluating selected IT controls applicable to University IT hosting and services. Our audit disclosed the following:

Finding 1: University IT security controls related to user authentication, user account management, logging and monitoring, and service-level agreements need improvement to ensure the confidentiality, integrity, and availability of IT resources related to Banner® ERP system hosting and services and customer data.

BACKGROUND

The University of South Florida (University) Board of Trustees entered into agreements with the Boards of Trustees[1] of Florida Gulf Coast University (FGCU), New College of Florida (NCF), and the University of North Florida (UNF) for hosting and services related to each entity's Banner® by Ellucian (Banner®) Enterprise Resource Planning (ERP) system. Specifically, the agreements provided for the Information Technology Division Data Center Infrastructure, an auxiliary of the University of South Florida Division of Information Technology, to host the Banner® ERP systems and provide selected IT services such as hardware configuration, installation and maintenance of operating systems software, installation and maintenance of databases, and business continuity to these customers.

FINDINGS AND RECOMMENDATIONS

Finding 1: Security Controls – User Authentication, User Account Management, Logging and Monitoring, and Service-Level Agreements

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed that certain security controls related to user authentication, user account management, logging and monitoring, and service-level agreements need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising the confidentiality of customer data and related IT resources. However, we have notified appropriate University management of the specific issues.

[1] The FGCU and UNF agreements were effective September 1, 2016, and the NCF agreement was effective July 1, 2016.

Without appropriate security controls related to user authentication, user account management, logging and monitoring, and service-level agreements the risk is increased that the confidentiality, integrity, and availability of customer data and related IT resources may be compromised.

Recommendation: We recommend that University management improve certain security controls related to user authentication, user account management, logging and monitoring, and service-level agreements for Banner® ERP system hosting and services to ensure the confidentiality, integrity, and availability of customer data and related IT resources.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of educational entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this IT operational audit from February 2017 through April 2017 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 the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our conclusions based on our audit objectives.

This IT operational audit focused on evaluating selected IT controls applicable to University operations for Banner® ERP system hosting and services provided during the period February 2017 through April 2017 to Florida Gulf Coast University (FGCU), New College of Florida (NCF), and the University of North Florida (UNF). The audit included selected IT controls over sensitive application and Web and database server access privileges; sensitive database administration access privileges; sensitive Active Directory access privileges; user authentication applicable to the application and Web and database servers, database management systems (databases), and Active Directory; logging and monitoring of application and Web and database servers, databases, and Active Directory; change management; service-level agreements; and vulnerability management of firewalls and remote access connectivity architecture. The overall objectives of the audit were:

- To determine the effectiveness of selected IT controls in achieving management's control in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

This audit was designed to identify, for the IT systems and controls included within the scope of the audit, deficiencies in management's internal controls; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT systems and controls included within the scope of this audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of the audit; obtaining an understanding of the IT systems and controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This audit included the selection and examination of IT system controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of University management and staff and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting this audit we:

- Interviewed University staff and reviewed documentation applicable to University operations for Banner® ERP system hosting and services to obtain an understanding of:
  - The IT infrastructure and network architecture for platforms hosted by the University.
  - Authentication controls applicable to the University's IT infrastructure, including selected hardware, operating systems, network, and databases related to the customers' Banner® ERP systems.
  - Logical design, administration, and periodic review procedures for logical access privileges granted to selected University IT resources and the customers' servers and databases.
  - Change management controls related to the hosted customers' Banner® ERP systems.
  - University processes for patch management related to the hosted customers' Banner® ERP systems.
  - Organizational structure for management and administration of University resources, including the services offered to customers and the division of responsibilities between University staff and the customers' staff.
- Evaluated the effectiveness of logical access controls, including periodic reviews for the servers, network domain, and databases that support the customers' Banner® ERP systems.
- Examined and evaluated the appropriateness of administrative privileges for the domain used by University staff for University services and operations as of February 27, 2017.
- Examined and evaluated the appropriateness of accounts and associated administrator access privileges granted as of March 1, 2017, to:
  - 80 accounts assigned to 2 application and Web servers for FGCU.
  - 40 accounts assigned to the application and Web server for NCF.
  - 40 accounts assigned to the application and Web server for UNF.

- 72 accounts assigned to the database server for FGCU.
- 49 accounts assigned to the database server for NCF.
- 55 accounts assigned to the database server for UNF.

- Examined and evaluated the appropriateness of services enabled on the application and Web and database servers. Specifically, we examined and evaluated:
  - 65 services on the 4 application and Web servers for FGCU, NCF, and UNF as of March 17, 2017.
  - 49 services on each of the FGCU, NCF, and UNF database servers as of March 1, 2017.
- Examined and evaluated the appropriateness of administrator privileges granted to the 9 University accounts on the FGCU, NCF, and UNF databases as of February 20, 2017.
- Evaluated user authentication controls related to the University's IT infrastructure supporting the customers' Banner® ERP systems.
- Evaluated the effectiveness of the University's logging and monitoring controls related to the hosted customers' Banner® ERP systems.
- Evaluated the effectiveness of the University's change management controls related to the authorization, testing, and approval of Banner® ERP system changes for the customers.
- Evaluated the effectiveness of patch management controls related to the University's IT infrastructure applicable to the hosted customers' Banner® ERP systems.
- Evaluated the adequacy of service-level agreements for ensuring the availability and integrity of customer applications and data.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's response is included in this report under the heading ***MANAGEMENT'S RESPONSE***.

AUTHORITY

Section 11.45, Florida Statutes, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any governmental entity created or established by law. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.

Sherrill F. Norman, CPA
Auditor General

USF UNIVERSITY OF SOUTH FLORIDA.

June 21, 2017

Ms. Sherrill F. Norman, CPA
Auditor General, State of Florida
Suite G74, Claude Pepper
Building 111 West Madison Street
Tallahassee, FL 32399-1450

Dear Ms. Norman:

Please find enclosed the University of South Florida System responses for the audit findings that are included in the USF Banner ERP Systems Hosting Operations prepared by your office.

If you have any questions or require additional information, please contact Alex Campoe, Chief Information Security Officer, at 813-974-1796.

DocuSigned by:
38314EEC39C14A1...

Sidney Fernandes
USF System Vice President/Chief Information

Copy to: President Judy Genshaft, USF System
John Long, Chief Operating Officer and Sr. Vice President, Business and Finance
Alex Campoe, Chief Information Security Officer
Virginia Kalil, Executive Director, University Audit & Compliance

University of South Florida

Responses to Preliminary and Tentative Findings of the

Banner® Enterprise Resource Planning (ERP) System Hosting Operation

Conducted by the Auditor General's Office

Finding 1: Security Controls: User Authentication, User Account Management, Logging and Monitoring, and Service-Level Agreements

Recommendation: We recommend that University management improve certain security controls related to user authentication, user account management, logging and monitoring, and service-level agreements for Banner® ERP system hosting and services to ensure the confidentiality, integrity, and availability of customer data and related IT resources.

Management's Response: As recommended, the University has put measures in place to improve IT security controls related to User Authentication, User Account Management, and Logging and Monitoring. We are currently in the process of addressing concerns raised regarding the Service Level Agreements in conjunction with the hosted Universities.

Expected SLA Implementation:	Dec 15, 2017
Responsible Party:	Alex Campoe, 813/974-1796