REPORT NO. 2012-064
DECEMBER 2011

UNIVERSITY OF NORTH FLORIDA

Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

BOARD OF TRUSTEES AND PRESIDENT

Members of the Board of Trustees and President who served during the 2010-11 fiscal year are listed below:

Dr. R. Bruce Taylor, Chair
A. Hugh Greene, Vice Chair
Matthew Brockelman from 4-20-11 (1)
Sitou Byll-Cataria to 4-19-11 (1)
Toni K. Crawford
Wilfredo J. Gonzalez
Ann C. Hicks to 6-21-11 (2)
Wanyonyi J. Kendrick
Joy G. Korman
Oscar Munoz
Joan W. Newton
M. Lynn Pappas from 5-18-11 (3)
Dr. J. Patrick Plumlee from 9-07-10 (4)
Dr. Katherine M. Robinson to 9-06-10 (4)
Kevin M. Twomey to 6-30-11 (5)
Sharon Wamble-King from 6-22-11 (2)

Mr. John A. Delaney, President

Notes: (1) Student body president.
(2) Board member's term ended January 6, 2011, but member continued to serve until position was filled effective June 22, 2011.
(3) Position remained vacant from July 1, 2010, through May 17, 2011.
(4) Faculty association president (equivalent to faculty senate chair referred to in Section 1001.71(1), Florida Statutes).
(5) Board member resigned effective June 30, 2011.

The audit team leader was Melinda G. Jones, CPA, and the audit was supervised by John P. Duffy, CPA. For the information technology portion of this audit was coordinated by Heidi G. Burns, CPA, CISA. Please address inquiries regarding this report to James R. Stultz, CPA, Audit Manager, by e-mail at jimstultz@aud.state.fl.us or by telephone at (850) 922-2263.

This report and other reports prepared by the Auditor General can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 487-9175; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

UNIVERSITY OF NORTH FLORIDA

SUMMARY

Our operational audit for the fiscal year ended June 30, 2011, disclosed the following:

CONSTRUCTION ADMINISTRATION

Finding No. 1: The University should improve its procedures for negotiating and documenting construction-related fees and guaranteed maximum price for construction projects administered by a construction management entity.

INFORMATION TECHNOLOGY

Finding No. 2: Some inappropriate or unnecessary information technology (IT) access privileges existed.

Finding No. 3: The University's security controls related to user authentication and data loss prevention needed improvement.

Finding No. 4: The University had not developed a written IT risk assessment for its business application system and the supporting environment.

Finding No. 5: The University's security awareness program lacked a feature for documenting users' acknowledgement of their security responsibilities.

BACKGROUND

The University of North Florida (University) is part of the State university system of public universities, which is under the general direction and control of the Florida Board of Governors. The University is directly governed by a Board of Trustees (Trustees) consisting of 13 members. The Governor appoints 6 citizen members and the Board of Governors appoints 5 citizen members. These members are confirmed by the Florida Senate and serve staggered terms of five years. The faculty association president and student body president also are members.

The Board of Governors establishes the powers and duties of the Trustees. The Trustees are responsible for setting University policies, which provide governance in accordance with State law and Board of Governors' Regulations. The University President is selected by the Trustees and confirmed by the Board of Governors. The University President serves as the executive officer and the corporate secretary of the Trustees and is responsible for administering the policies prescribed by the Trustees for the University.

The results of our financial audit of the University for the fiscal year ended June 30, 2011, will be presented in a separate report. In addition, the Federal awards administered by the University are included within the scope of our Statewide audit of Federal awards administered by the State of Florida and the results of that audit, for the fiscal year ended June 30, 2011, will be presented in a separate report.

FINDINGS AND RECOMMENDATIONS

Construction Administration

Finding No. 1: Construction Contract Management

Pursuant to Section 1013.45(1), Florida Statutes, on March 10, 2010, the University entered into a contract with a construction management entity (CME) for construction of a new science and humanities building. The project was funded from Public Education Capital Outlay appropriations totaling $40.5 million. Board of Governors Regulation 14.007, *Competitive Negotiation*, requires that a contract for construction related services be negotiated; CME profit, overhead, and direct management costs contractually agreed upon; and a guaranteed maximum price (GMP) established. Under the CME process, the contracted firm is responsible for scheduling and coordinating both the design and construction phases, and is generally responsible for the successful, timely, and economical completion of the construction project. The GMP provision allows for the difference between the actual cost of the project and the GMP amount, or the net cost savings, to be returned or shared with the University.

Our review of the contract with the CME disclosed that the University did not negotiate and agree upon the profit, overhead, direct management costs, and GMP when entering into the CME contract. The CME provided a detailed GMP proposal dated February 18, 2010, with fees and costs totaling $33,629,742; however, the proposal was not, of record, negotiated and incorporated into the March 10, 2010, contract. Instead, the contract provisions relating to the profit, overhead, direct management costs, and the GMP did not specify negotiated percentages or amounts and indicated the provisions would be subsequently negotiated. The University subsequently approved four partial GMP amendments from April 28, 2010, through October 8, 2010, and a final GMP on January 10, 2011, as follows:

Guaranteed Maximum Price Summary

GMP Notice to Proceed Date	GMP Amendments	Description	Amount	Cumulative Contract Amount
4-28-10	Partial GMP 1	Parking Lot Modifications and Off-Site Sewer	$ 829,525	$ 829,525
6-01-10	Partial GMP 2	Civil and Site Utilities	724,755	1,554,280
8-13-10	Partial GMP 3	Building Structure	5,744,572	7,298,852
10-08-10	Partial GMP 4	Structural Steel and Walls	6,727,909	14,026,761
1-10-11	Final GMP (1)	Balance of the Work	20,000,284	34,027,045

Note: (1) Final GMP amount includes minor change orders and alternate bid item.

Our review of the University's procedures for negotiating and contracting with the CME disclosed the following:

- The University did not complete negotiations and agree upon significant contract terms and provisions prior to the start of construction. Board of Governors Regulation 14.007, *Competitive Negotiation*, provides that, should the University be unable to negotiate a satisfactory contract with the CME, considered the most qualified, at a fair, competitive and reasonable price (i.e., GMP), negotiations shall be terminated and then undertaken with the next most qualified firm. However, by starting construction without an approved GMP cap, the University may have limited its ability to evaluate and ensure the overall cost of the project was fair, competitive, and reasonable, and to negotiate with the next most qualified firm should it become necessary.
- The performance and payment bond was incrementally increased with each partial and the final GMP amendment. When a GMP for the entire project is not established before construction begins and a performance and payment bond executed for the full GMP amount, the University is at risk for the portion

of the project not bonded in the event of CME default. A similar finding was noted in our report No. 2010-141.

- Major subcontracts were bid prior to entering into GMP amendments, thereby limiting the CME's risk of the total cost of the project exceeding the GMP amount. Under the construction manager at risk project delivery method, the GMP provision requires a commitment by the CME to deliver the project within the GMP amount. However, when subcontracts are bid prior to establishing the GMP amount, the CME will establish a GMP to recover all subcontract costs and has limited incentive to minimize other project costs to deliver the project within the GMP amount.

- The construction management contract provided that the CME's fee would be a percentage of the cost of the work, converted to a lump-sum amount upon acceptance of the GMP, and that the sum of the cost of the work and the CME's fee would comprise the total GMP. University personnel advised us that the CME's fee (profit and overhead) was negotiated at 4.75 percent; however, the fee rate was not specified in the contract and documentation of rate negotiations was not available. The actual fee rate used by the CME was 4.75 percent of the total GMP (construction cost plus CME's profit and overhead fee), which equates to 4.98 percent of the cost of the work (construction cost before including CME's profit and overhead fee). In these circumstances, it was not evident upon what basis the 4.75 percent rate was negotiated. The difference between the 4.75 and 4.98 percent fee rates represents additional project costs of $79,209. Subsequent to our inquiries, University personnel advised us that the fees were miscalculated due to an arithmetic error and that the University contacted the CME and will receive a credit change order of $79,209 to adjust the fee to 4.75 percent of the cost of work.

- Each GMP amendment included a separate provision for general conditions costs (reimbursable expenses of the CME) totaling approximately $2 million. General conditions include such items as direct and indirect salary costs of project staff; costs of jobsite office space, furniture, equipment, and supplies; and communication and utility costs. The general conditions costs were estimated by the CME, reviewed by University personnel, and converted to a fixed lump-sum amount for billing purposes. Upon inquiry regarding the University's methodology for reviewing and negotiating the detailed support for general conditions proposals, we were advised that the methodology was based on 36 years of experience in negotiation with contractors, to determine what is legal, fair and equitable for the University, and recent negotiations with other builders. However, documentation of the methodology applied and factors considered during the negotiation process for each cost item was not provided and, absent such documentation, University records did not evidence that amounts paid for general conditions were reasonable and appropriate.

Recommendation: The University should evaluate and revise as appropriate, its procedures for contracting with CMEs to ensure that a GMP is established prior to start of the construction project, a performance and payment bond executed for the entire GMP amount, subcontracts are bid after the GMP is established, and CME fees are properly calculated. The University should also establish written policies and procedures addressing negotiation of general conditions and requiring documentation of the methodology used and application of various factors considered in evaluating the reasonableness of such costs. In addition, the University should consider paying documented actual general conditions costs up to a specified maximum amount, rather than agreeing to pay a fixed amount regardless of actual costs, to provide additional opportunities for recovering unspent costs and maximizing cost savings under the GMP.

Follow-up to Management's Response

The University's response indicates that time is always a critical factor in starting and completing a project because of the demand and need for classrooms being ready at the beginning of any semester, and that phasing the construction by negotiating sequential GMP's reduces the amount of time needed to bring a facility on line and resulted in the best negotiated contract to provide value and timely delivery. The University's response also indicates that the University feels strongly in managing a project in a fashion most advantageous to itself, the State and the taxpayers. However, using multiple negotiated GMPs during

the construction phase of the project is contrary to the requirements of Board of Governors Regulation 14.007, and University records did not evidence that using multiple sequential GMP negotiations was more effective or efficient than using one GMP negotiation prior to the start of construction or reduced the amount of time to bring the facility on line. Additionally, University records did not evidence how using multiple GMP negotiations rather than one GMP negotiation resulted in the best value or was more advantageous to itself, the State or the taxpayers.

Information Technology

Finding No. 2: Access Privileges

Access controls are intended to protect data and information technology (IT) resources from unauthorized disclosure, modification, or destruction. Effective access controls provide employees access to IT resources based on a demonstrated need to view, change, or delete data and restrict employees from performing incompatible functions or functions outside of their areas of responsibility. Periodically reviewing IT access privileges assigned to employees promotes good internal control and is necessary to ensure that employees cannot access computer resources that are inconsistent with their assigned job responsibilities.

Our tests of selected access privileges to the finance and human resources applications and the supporting database disclosed inappropriate or unnecessary access privileges, as follows:

- Four Information Technology Services (ITS) employees had update capability to all critical functions within the finance and human resource applications in addition to having database administrator authority. Since clear division of roles and responsibilities between IT staff and functional end users helps preclude the possibility of a single employee subverting a critical process, this access was unnecessary and contrary to an appropriate separation of duties.
- Two ITS programmers had update capability in the business application system with one having update capability to all critical functions in the finance application and the other having update capability to all critical functions in the human resource application. Based on their assigned responsibilities in support of the business application system, this access was unnecessary and contrary to an appropriate separation of duties.
- In addition to the four ITS staff having unrestricted security administrator authority, nine employees from various departments had unrestricted security administrator authority for the business application system. Although the University's practice was to distribute security administration duties to various departments, these nine employees were not responsible for administering security on a global (Universitywide) level and the granting of unrestricted security administrator authority was inappropriate based on their assigned job responsibilities.

These inappropriate or unnecessary application access privileges indicated the need for improved University review of access privileges. Without a comprehensive review, inappropriate access privileges may not be timely detected and addressed by the University, increasing the risk of unauthorized disclosure, modification, or destruction of University data and IT resources.

Recommendation: The University should develop a process for periodically reviewing the appropriateness of IT application access privileges, including those granted database administrator authority, and timely remove or adjust any inappropriate or unnecessary access detected to ensure that access privileges are compatible with employee job responsibilities and enforce an appropriate separation of duties. In addition, the University should avoid granting unrestricted security administrator authority to employees who are not responsible for global level security administration.

Finding No. 3: Security Controls – User Authentication and Data Loss Prevention

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed that certain University security controls related to user authentication and data loss prevention needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising University data and IT resources. However, we have notified appropriate University management of the specific issues. Without adequate security controls related to user authentication and data loss prevention, the confidentiality, integrity, and availability of data and IT resources may be compromised, increasing the risk that University data and IT resources may be subject to improper disclosure, modification, or destruction.

Recommendation: The University should improve its security controls related to user authentication and data loss prevention to ensure the continued confidentiality, integrity, and availability of University data and IT resources.

Finding No. 4: Risk Assessment

Management of IT-related risks is a key part of enterprise IT governance. Incorporating an enterprise perspective into day-to-day governance actions helps an entity understand its greatest security risk exposures and determine whether planned controls are appropriate and adequate to secure IT resources from unauthorized disclosure, modification, or destruction. Documented IT risk assessment, including the identification of risks and the evaluation of the likelihood of threats and the severity of threat impact, help support management's decisions in establishing cost-effective measures to mitigate risk and, where appropriate, formally accept residual risk.

Although the University had considered external and internal risks and identified security controls to mitigate these risks, the University had not developed a written, comprehensive IT risk assessment for the business application system and the supporting IT environment (i.e., the University's network, operating system, database, Web portal, and connection to the University's data center). The absence of a written, comprehensive IT risk assessment for the business application system and the supporting IT environment may limit the University's assurance that all likely threats and vulnerabilities have been identified, the most significant risks have been addressed, and appropriate decisions have been made regarding which risks to accept and which risks to mitigate through security controls.

Recommendation: The University should develop a written, comprehensive IT risk assessment for its business application system and the supporting environment to provide a documented basis for determining how IT-related risks are managed.

Finding No. 5: Security Awareness

A comprehensive security awareness program, which can include training and publications, is to inform users of importance of preserving the confidentiality, integrity, and availability of data and IT resources. Employees must be aware of their responsibilities and the steps the organization is willing to take to ensure security through documentation describing security policies and procedures and acknowledgements of an individual's responsibility.

Although the University's *Network Acceptable Use Policy* provides standards for acceptable uses of University computing and IT resources and provides for the potential consequences to employees determined to be in violation of its provisions, employees are not required to certify that they have reviewed and understand the *Network Acceptable Use Policy*. A similar finding was noted in our report No. 2010-141.

In response to our inquiry, University personnel indicated that the University's network logon screen displays the Web address for a listing of University policies, of which the *Network Acceptable Use Policy* is a part, and includes a statement that the use of the network constitutes consent by the user to all University IT policies. However, the Web address is not a hyperlink to the policies. In addition, employees are able to directly authenticate to the University's business application system accessing resources and data without presentation of the logon screen information.

The University maintains IT systems with significant nonpublic records (such as student record information) and other records that contain sensitive information accessible by employees in the performance of assigned duties. A periodic certification of employees' acknowledgement of their security responsibilities could reduce the risk of University resources being unintentionally compromised by employees while performing their assigned duties and could enhance the University's ability to take disciplinary action, should it be necessary, against employees misusing data or IT resources.

Recommendation: The University should enhance its security awareness program to ensure that employees periodically provide signed (handwritten or electronic) acknowledgement that they have read and understand the University's security policies.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the University had taken corrective actions for findings included in our report No. 2010-141.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental 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 operational audit from February 2011 to August 2011 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.

The objectives of this operational audit were to: (1) obtain an understanding and make overall judgments as to whether University internal controls promoted and encouraged compliance with applicable laws, rules, regulations, contracts, and grant agreements; the economic and efficient operation of the University; the reliability of records and reports; and the safeguarding of assets; (2) evaluate management's performance in these areas; and (3) determine whether the University had taken corrective actions for findings included in our report No. 2010-141. Also, pursuant to Section 11.45(7)(h), Florida Statutes, our audit may identify statutory and fiscal changes to be recommended to the Legislature.

The scope of this operational audit is described in Exhibit A. Our audit included examinations of various records and transactions (as well as events and conditions) occurring during the 2010-11 fiscal year.

Our audit methodology included obtaining an understanding of the internal controls by interviewing University personnel and, as appropriate, performing a walk-through of relevant internal controls through observation and

examination of supporting documentation and records. Additional audit procedures applied to determine that internal controls were working as designed, and to determine the University's compliance with the above-noted audit objectives, are described in Exhibit A. Specific information describing the work conducted to address the audit objectives is also included in the individual findings.

AUTHORITY

Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our operational audit.

David W. Martin, CPA
Auditor General

MANAGEMENT'S RESPONSE

Management's response is included as Exhibit B.

EXHIBIT A
AUDIT SCOPE AND METHODOLOGY

Scope (Topic)	Methodology
Information Technology (IT) security awareness and training.	Determined whether corrective action was taken with regard to employees' signed acknowledgement of University IT security policies.
IT logical access controls and user authorization.	Reviewed selected operating system, database, network, portal, and application security settings to determine whether authentication controls were configured and enforced in accordance with IT best practices.
IT access privileges and separation of duties.	Reviewed procedures for maintaining and reviewing access to IT resources. Tested selected access privileges over the operating system, database, network, and applications to determine the appropriateness and necessity based on employees' job duties and adequacy with regard to preventing the performance of incompatible duties.
IT data loss prevention.	Reviewed written policies, procedures, and programs in effect governing the classification, management, and protection of sensitive and confidential information.
IT security incident response.	Reviewed written policies and procedures, plans, and forms related to the response to and reporting of security incidents.
IT risk management and assessment.	Reviewed the University's risk management and assessment processes and security controls intended to protect the confidentiality, integrity, and availability of data and IT resources.
Social security number requirements of Section 119.071(5)(a), Florida Statutes.	Examined supporting documentation to determine whether the University had provided individuals with a written statement of the purpose of collecting their social security numbers.
Identity theft prevention program (Red Flags Rule).	Reviewed University policies and procedures related to its identity theft prevention program for compliance with the Federal Trade Commission's Red Flags Rule.
Works of art and historical treasures.	Reviewed controls over museum works of art and historical treasures to determine whether the University had established adequate safeguards to protect such assets from theft or loss.
Distance learning fees and excess hour surcharge.	Determined whether distance learning fees and excess hour surcharges were assessed and collected as provided by Sections 1009.24(17) and 1009.286(2), Florida Statutes.
Florida residency determination and tuition.	Tested student registrations to determine whether the University documented Florida residency and correctly assessed tuition in compliance with Sections 1009.21, 1009.24, and 1009.286(2), Florida Statutes, and Board of Governors Regulation 7.005.
Tuition differential fees.	Tested payments from tuition differential fees collected to determine whether the University used the tuition differential fees in compliance with Section 1009.24(16)(a), Florida Statutes.

EXHIBIT A (CONTINUED)
AUDIT SCOPE AND METHODOLOGY

Scope (Topic)	Methodology
Continuing education programs.	Reviewed University policies and procedures to ensure that credit continuing education courses did not compete with, or replace, the regular on campus courses taken by degree seeking or special students.
Overtime payments.	Reviewed University policies, procedures, and supporting documentation evidencing the approval of and necessity for overtime payments.
Purchasing card transactions.	Tested transactions to determine whether purchasing cards were administered in accordance with University policies and procedures. Also, tested former employees to determine whether purchasing cards were timely cancelled upon termination of employment.
Insuring architects and engineers.	Tested major construction projects in progress during the audit period to determine whether the University had obtained evidence of required insurance.
Construction contract administration.	Tested construction contract administration procedures to determine whether guaranteed maximum price construction project costs were negotiated on a competitive basis and closely monitored, included proper approval of change orders by the Board, and timely updates to payment and performance bonds.
Wireless communication devices.	Reviewed policies and procedures to determine whether the University limited the use of, and documented the level of service for wireless communication devices.

EXHIBIT B
MANAGEMENT'S RESPONSE

ADMINISTRATION & FINANCE
Office of the Vice President

UNIVERSITY of NORTH FLORIDA

December 8, 2011

Mr. David W. Martin
Auditor General
State of Florida
111 West Madison Street
Claude Pepper Building, Suite G-74
Tallahassee, FL 32399-1450

Dear Mr. Martin:

In connection with the University of North Florida Operational Audit for the fiscal year ending June 30, 2011, enclosed are the University's responses to the preliminary and tentative audit findings.

Should you have any questions or need additional information, please do not hesitate to contact me.

Sincerely,

Shari Shuman

Shari Shuman
Vice President, Administration & Finance

Enclosure

1 UNF Drive Jacksonville, FL 32224-7699
Tel: 904.620.2002 Fax: 904.620.2010
Equal Opportunity/Equal Access/Affirmative Action Institution

EXHIBIT B (CONTINUED)
MANAGEMENT'S RESPONSE

Reponses to Florida Auditor General's Preliminary Findings dated November 8, 2011

Construction Administration

Finding No. 1:

Recommendation: The University should evaluate and revise as appropriate, its procedures for contracting with CMEs to ensure that a GMP is established prior to start of the construction project, a performance and payment bond executed for the entire GMP amount, subcontracts are bid after the GMP is established, and CME fees are properly calculated. The University should also establish written policies and procedures addressing negotiation of general conditions and requiring documentation of the methodology used and application of various factors considered in evaluating the reasonableness of such costs. In addition, the University should consider paying documented actual general conditions costs up to a specified maximum amount, rather than agreeing to pay a fixed amount regardless of actual costs, to provide additional opportunities for recovering unspent costs and maximizing cost savings under the GMP.

University Response:
The University understands the position and the recommendation and recognizes we were not in full compliance; however we do feel that in this case the project resulted in the best negotiated contract with the CME to provide value and timely delivery. The University feels strongly in managing a project in a fashion most advantageous to itself, the State and the taxpayers. UNF has been selecting a phased approach to the construction of a major facility. This approach precludes having a total GMP for the entire project before construction starts. At the initial meeting with the A/E and CM, the construction budget is divulged and discussed. Both the A/E and the CM are charged with the responsibility to stay within the construction budget as the construction documents are finalized. The Construction Budget is taken to mean the GMP for the project and this item is on the agenda on all subsequent meetings and discussions with the project team.

The University does not request a GMP before construction starts for the following reasons:

- Time is always a critical factor in starting and completing a project because of the demand and need for classrooms being ready at the beginning of any semester. Phasing the construction, which leads to negotiating sequential GMP's reduces the amount of time needed to bring a facility on line.
- Invariably the Site Utilities, Footings and Foundation Packages are ready for pricing long before the rest of the construction documents are complete. Starting with this phase of the work allows for an early start to reduce the time lapse between start and end dates of a project.
- In light of the funding restrictions and cash-flow requirements, The UNF generally agrees to allow the CME to bid sub-trade packages before establishing a GMP to fix a "real" cost to reduce the risk to the UNF. Phasing the project allows for multi-year funding from the State. As stated previously, the subject of the construction budget and the global GMP is always discussed during progress meetings. This assures the University that both the A/E and the CM have this expectation in mind as they develop the project details.

Additionally, UNF conducts a Post construction audit of all project accounts. Absence the accounting personnel to do a monthly audit of CME pay applications through the duration of a project, a post-construction audit seems to be the most expedient and advantageous to the UNF. We have been successful in audits on previous contracts to collect amounts as identified and owed. However, to clarify the issue UNF is currently revising its procedures to ensure that the general condition terms of the contract are negotiated at the beginning of a contract and appropriately documented. Contracts have been amended to include the following statement:

EXHIBIT B (CONTINUED)
MANAGEMENT'S RESPONSE

"Pursuant to the foregoing general right to audit and copy, the Owner, at its option, may conduct a complete post-audit to ascertain the accuracy of all sums invoiced by the Construction Manager for the Work. If any such audit reveals that the Owner has overpaid improperly for any portion of the work, the Construction Manager will reimburse the Owner for any such overpayment or improper payment."

Information Technology

Finding No. 2:

Recommendation: The University should develop a process for periodically reviewing the appropriateness of IT application access privileges, including those granted database administrator authority, and timely remove or adjust any inappropriate or unnecessary access detected to ensure that access privileges are compatible with employee job responsibilities and enforce an appropriate separation of duties. In addition, the University should avoid granting unrestricted security administrator authority to employees who are not responsible for global level security administration.

University Response:
The University will continue to engage in a process of periodically reviewing access controls and processes in the pursuit of improving these areas. Specific to the concerns noted:

Part1: We understand the concerns of limiting the unnecessary and inappropriate control and access privileges of database administrators. As such we will evaluate and restrict where appropriate those access privileges.

Part 2: After a review of the access permissions, the access rights were removed.

Part 3: It is important to note that the staff with security administrator authority are not default roles and cannot be used outside of the Banner Security Environment. It should also be noted that the four I'T'S staff members who have unrestricted security administrator authority also have database owner privileges. Restricting their security administrator authority will not lessen their access to the underlying application and this is appropriate given their roles and responsibilities. We will continue to seek solutions that improve our security posture congruent with business requirements.

Finding No. 3:

Recommendation: The University should improve its security controls related to user authentication and data loss prevention to ensure the continued confidentiality, integrity, and availability of University data and IT resources.

University Response:
The University is always striving to enhance their information security program. We had previously identified this as an area for further investigation. During the past year we engaged with Oracle to guide us through an extensive review of how we store and handle sensitive data. We are also conducting a long-term pilot program using a data loss prevention (DLP) product. As a result of our initial testing, we concluded that a more expansive pilot with a more full featured DLP solution would be worthwhile. We will continue to explore solutions in this area and others as resources and budget allow.

EXHIBIT B (CONTINUED)
MANAGEMENT'S RESPONSE

Finding No. 4:

Recommendation: The University should develop a written, comprehensive IT risk assessment for its business application system and the supporting environment to provide a documented basis for determining how IT-related risks are managed.

University Response:
We agree with the need for a risk assessment process and feel that we have a working process in place. We will continue to enhance our process and document our actions where appropriate.

We submitted two examples of full assessment workups, a data safety monitoring plan and related appendix. These are samples of the types of extensive, formal risk assessments conducted when warranted or required.

We are engaged in security assessments almost daily, beginning in many cases during our initial contract review for shrink-wrapped software, or from the project meetings during custom application and system development. In most cases, the feedback and subsequent decision-making is not formalized to the extent of requiring signed documents. Even so, issues are worked out to stakeholders' mutual satisfaction, or are escalated to higher levels of management for discussion and remediation as required.

Finding No. 5:

Recommendation: The University should enhance its security awareness program to ensure that employees periodically provide signed (handwritten or electronic) acknowledgement that they have read and understand the University's security policies.

University Response:
We currently display a link to all relevant policies during workstation sign-in. The link is: www.unf.edu/anf/its/polproc. As part of the displayed message, we remind everyone that signing in constitutes assent to and compliance with the relevant policies and procedures. One of those policies is the Network Acceptable Use policy. We believe a daily affirmation and reminder is most effective, which led to our choice in this matter.

However, we have added the Network Acceptable Use Policy to the rotation of policies that are periodically presented to employees for specific acknowledgement. The first time we did this was in September, 2008. We did not present this sort of focused policy acknowledgement again until 2010, at which time the Network Acceptable Use Policy was removed from the rotation in favor of the Code of Conduct and Ethics Policy. It has since been added and was most recently presented again in October, 2011.