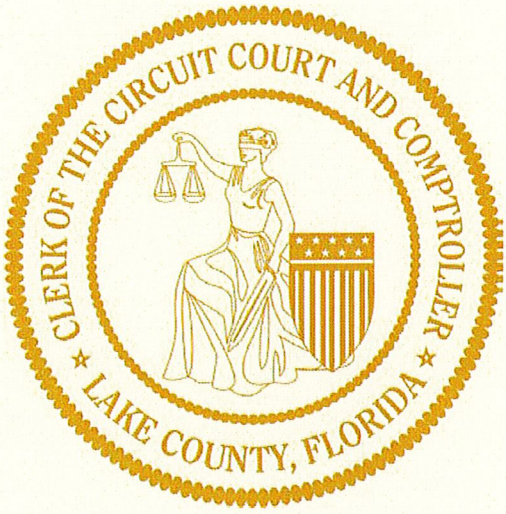


Audit of
BCC Vendor Management Assessment

Division of Inspector General
Gary J. Cooney, Clerk of the Circuit Court and Comptroller
Audit Report

Terri W. Freeman, CPA, CIA, CISA, CRMA
Inspector General

Report No. BCC-173
January 9, 2020

Division of Inspector General
Office of Gary J. Cooney
Clerk of the Circuit Court and Comptroller
550 West Main Street, Post Office Box 7800
Tavares, Florida 32778-7800
Phone: (352) 253-4930 Fax: (352) 742-4534

January 9, 2020

Board of County Commissioners

The Vendor Management Audit that was identified in the 2019 Audit Plan has been completed.

We appreciate the cooperation and assistance provided by everyone during the course of the audit.

Respectfully submitted,

Terri W. Freeman
Inspector General

cc: Gary J. Cooney, Clerk of the Circuit Court & Comptroller
Jeff Cole, County Manager
Jennifer Barker, Executive Director, Administrative Services
Ron Falanga, Director, Office of Procurement Services

VENDOR MANAGEMENT ASSESSMENT

Lake County Board of County Commissioners

January 9, 2020

Table of Contents

Executive Summary

Objective

The objective of the Vendor Management Assessment was to identify gaps in the design effectiveness of the internal controls that could put Lake County Board of County Commissioner (the Organization) data (by type) at risk including:

- Financial Data
- Employee Data
- Intellectual Property

Deficiencies in control design or effectiveness that could negatively impact the confidentiality or integrity of Lake County Board of County Commissioner data or availability of critical systems are identified within this report with recommendations for remediation.

Scope

The scope of this review focused on the following vendors that were selected by the Organization.

- Benefit Focus
- Florida Blue
- Intermedix
- Motorola
- Tri-Star

Approach

Overview

To achieve the project objectives, CLA conducted the Vendor Management Assessment by interviewing staff, reviewing documentation provided by Lake County Board of County Commissioners and reviewing current processes and procedures within the organization.

Best Practice

As a basis for the review, current processes and procedures specific to vendor management within the Organization were compared to Best Practice controls outlined in CLA's Information Technology and Systems Management Work Programs. The work programs were initially developed based on the guidelines of regulatory requirements and have since been revised to incorporate elements of COBIT, COSO, ITIL, and NIST 800-53 Revision 4. Controls proven to be important based on experience of the Information Security Services Group staff within CLA have also been included in the work programs. CLA's controls are categorized as either required, essential or recommended.

- A required control is either stated or implied by regulatory guidance as an expected practice.
- An essential control is stated or implied by other authoritative guidance as expected practice.
- A recommended control is considered by CLA as an industry best practice.

Risk and Control Analysis

Overall risk is determined based on the magnitude of the impact of an event after consideration of the organization's controls and the likelihood that event would negatively impact the organization. Controls specific to each control domain and topic were reviewed, risk was determined as follows:

Inherent Risk – determined based on the probability of the defined risk (threat) risk with subjective consideration of the impact. Inherent Risk is calculated based on the following:

Probability	Impact	Inherent Risk
Low	Low	Low
Low	Medium	Medium
Low	High	Medium
Medium	Low	Low
Medium	Medium	Medium
Medium	High	High
High	Low	Medium
High	Medium	Medium
High	High	High

Control Risk – determined based on the evaluation of each current control's design, effectiveness, strength and likelihood of failure. Control Risk is determined based on the following:

Control Risk	Definition
Critical	Immediate potential to impact availability, integrity or confidentiality *(no control)*
High	Potential to impact availability, integrity or confidentiality *(weak control)*
Medium	Intermittent potential to impact availability, integrity or confidentiality *(control exists but not enforced)*
Low	Controls are in place and operating effectively - however inherent risk exists

Residual Risk – determined by subjectively evaluating the extent Control Risk could reduce Inherent Risk. Residual Risk assumes the organization has not taken action on the Recommended Remediation to reduce the overall risk to the organization. Residual Risk is determined based on the following:

Residual Risk	Definition
Critical	Immediate potential to impact availability, integrity or confidentiality *(Controls cannot be designed appropriately or be effective on a consistent basis)*
High	Potential to impact availability, integrity or confidentiality *(Controls are not designed appropriately or be effective on a consistent basis)*
Medium	Intermittent potential to impact availability, integrity or confidentiality *(Controls are designed appropriately and can be effective on a consistent basis but can be bypassed or overlooked)*
Low	Controls are in place and operating effectively - however inherent risk exists

Remediation Recommendations

As a result of the issue(s) identified, remediation recommendations were provided to improve the position of the Organization related to the defined security or technology management topic. Each recommendation was subjectively assigned an effort that indicates the level of effort associated with implementing the remediation as follows:

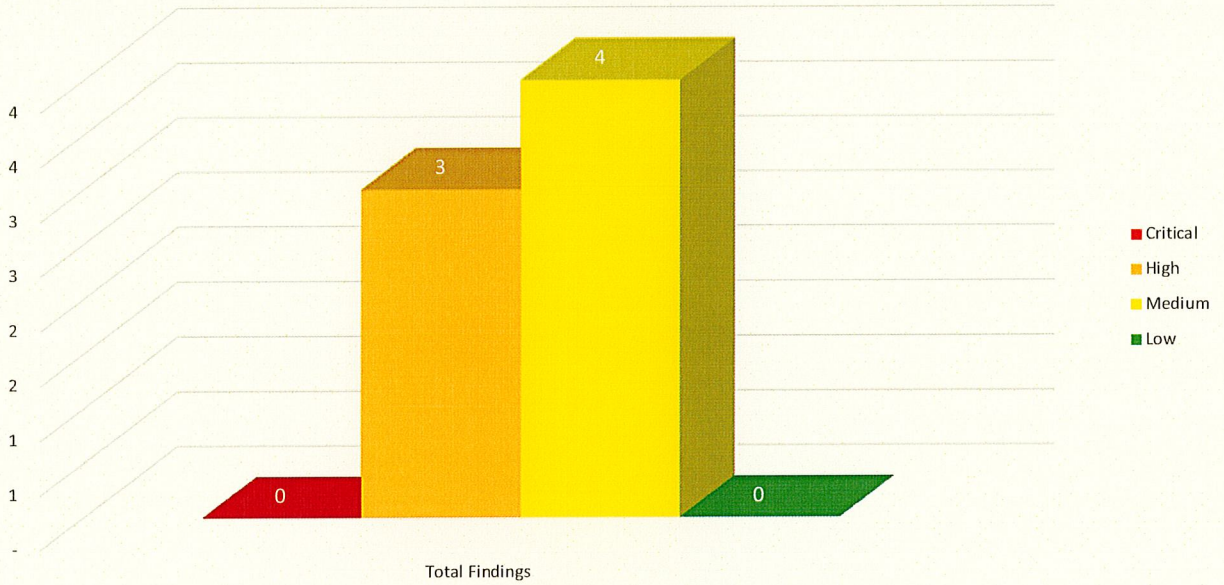
Priority	Review Period	Identification of Mitigating Controls
Critical	Within 10 Days	Within 30 Days
High	Within 30 Days	Within 30 - 60 Days
Medium	Within 90 Days	Within 90 - 120 Days
Low	Within 120 Days	Recommendations are based on "best practice" and can be addressed as time permits to determine if additional controls should be implemented.

Control Results and Benchmarking

CLA evaluated seven controls and rated each control by effectiveness. Effective controls earn 100% of the points, Mostly effective earns 80%, Partially Effective earns 50% and Not Effective controls earn 0. The maturity score by the control domain represents the Organization's maturity in Vendor Management. Score for the Vendor Management control domain is as follows:

Control Domain	Maturity Score
Vendor Management	43.64%

The results of the review process indicated that the following residual risks present within the Vendor Management control domain under review:



Recommendations

Domain: Vendor Management

Best Practice:

The Organization should have a formal Vendor Management Program that includes policies and procedures to outline appropriate due diligence, risk assessments, contracting, and oversight of vendors and business partners. Vendor risk assessments should be performed and all vendors should be risk rated based from both a security and continuity perspective. Vendor due diligence and oversight should be performed timely and include a review of relevant areas based on risk (e.g., vendor security and incident response programs, Business Continuity and Disaster Recovery plans, SSAE18, financial stats, etc.).

Domain: Vendor Management			
Ctl 05.01	**Control Objective**	**Results**	**Priority and Recommendation**
	The Vendor Management Program includes policies and procedures to outline appropriate due diligence, risk assessments, contracting, and oversight of vendors and business partners.	Control Rating: Mostly Effective Inherent Risk: High Comments: Policies and procedures exist for the management of vendors. This includes the processes related to proposals, contract negotiation, purchasing, vendor monitoring and assignment of responsibilities. Policies do not require risk assessments.	Remediation Priority: Low Residual Risk: Low Recommendation: CLA recommends that the vendor management program be updated to specifically require risk assessments.
Ctl 05.02	**Control Objective**	**Results**	**Priority and Recommendation**
	Vendor risk assessments are performed for all vendors. The risk rating should be determined using qualitative ranking methods. The risk assessments determine vendor criticality from both a security and continuity perspective. This criticality then determines the contractual and monitoring requirements for the vendor.	Control Rating: Not Effective Inherent Risk: High Comments: Formal documented risk assessments are not part of the process during vendor selection but the risk assessment itself is not documented so that vendor criticality could be assigned to facilitate monitoring requirements.	Remediation Priority: High Residual Risk: High Recommendation: CLA recommends that vendor risk assessments be regularly performed. Risk assessments should determine vendor criticality from both a security and continuity perspective. This criticality then determines the contractual and monitoring requirements for the vendor. The risk rating (high/medium/low/other) should be determined using a qualitative ranking method.

	Control Objective	Results	Priority and Recommendation
Ctl 05.03	Vendor due diligence is performed prior to vendor selection. Vendor selection criteria is developed and used to effectively compare vendors and solidify the decision for the vendor selected. Documentation should address: - Vendor industry experience - Vendor financial condition and reputation - Vendor references - Vendor service level agreements - Vendor legal and regulatory compliance - Vendor ability to support clients with Business Continuity Plans (BCP) If the vendor will have routine access to protected information documentation should also address: - Review of security controls - Review of BCP controls - Review of controls attestation (such as SSAE 18, SOC 2, etc.) - Incident response plan and cybersecurity event preparedness	Control Rating: Partially Effective Inherent Risk: High Comments: Documented due diligence is not performed prior to vendor selection. The due diligence procedures and activities are not documented.	Remediation Priority: High Residual Risk: High Recommendation: CLA recommends that vendor due diligence evaluate: - Vendor industry experience - Vendor financial condition and reputation - Vendor references - Vendor service level agreements - Vendor legal and regulatory compliance If the vendor will have routine access to protected information documentation should also address: - Review of security controls - Review of BCP controls - Review of controls attestation (such as SSAE 18, SOC 2, etc.) - Incident response plan and cybersecurity event preparedness Vendor due diligence practices verify that vendors in routine custody of non-public personally identifiable information meet specific security criteria established by the organization such as regular patching of systems, limited administrator access, strong authentication, and individual accountability.

	Control Objective	Results	Priority and Recommendation
Ctl 05.04	Vendor contracts should be appropriately reviewed (i.e., legal counsel, business owners, and security personnel) inclusion of all appropriate provisions prior to signing. If the vendor will have routine access to protected information, contracts include appropriate security, confidentiality, and breach disclosure provisions including vendor incident response procedures. Contracts should also address right to audit, subcontracting, Business Continuity Plan testing and Recovery Time Objectives/Recovery Point Objectives, data governance, and communication and update expectations regarding security issues. Contracts should define events that constitute contractual default and provide a list of acceptable remedies and opportunities for curing a default.	Control Rating: Mostly Effective Inherent Risk: Medium Comments: Contracts reviewed that do not address business continuity - Florida Blue Tri-Star	Remediation Priority: Medium Residual Risk: Medium Recommendation: CLA recommends that all vendor contracts address: - Business continuity
Ctl 05.05	Where appropriate, vendor agreements (SLAs) address support of current operating systems and implementation of critical security patches. Vendor agreements specifically define vendor access to internal systems, remote access provisions, individual accountability for access, and access monitoring.	Control Rating: Mostly Effective Inherent Risk: Medium Comments: Contracts reviewed that contain service level agreement - Benefit Focus Intermedix Motorola Contracts reviewed that do not contain service level agreement - Florida Blue Tri-Star	Remediation Priority: Medium Residual Risk: Medium Recommendation: CLA recommends that all vendor contracts address support for current operating systems and the timely deployment of critical security patches for operating systems and applications when applicable. Vendor agreements should specifically define vendor access to internal systems, remote access provisions, individual accountability for access, and access monitoring.

	Control Objective	Results	Priority and Recommendation
Ctl 05.06	For vendors with routine access to protected information, regular and formally documented vendor monitoring is performed at least annually and includes reviewing: - Financial condition - Effectiveness of IT and security controls as represented in a third-party attestation - Effectiveness of Business Continuity Plans (BCP) and testing - Incident response plan and cybersecurity event preparedness	Control Rating: Partially Effective Inherent Risk: High Comments: Formal documented vendor monitoring related to financial condition, IT security controls, Business Continuity and Incident Response are not performed for applicable vendors. CLA understands that this process currently is in being implemented.	Remediation Priority: High Residual Risk: High Recommendation: CLA recommends annual, formally documented vendor reviews including: - Financial condition - Effectiveness of IT and security controls as represented in a third-party attestation - Effectiveness of BCP and BCP testing - Incident response plan and cybersecurity event preparedness
	Control Objective	**Results**	**Priority and Recommendation**
Ctl 05.07	If a critical vendor uses the services of another vendor, vendor due diligence includes a review of a vendor's vendor management practices.	Control Rating: Not Effective Inherent Risk: Medium Comments: Although all contracts reviewed contain language related to subcontracting, vendor due diligence of the subcontractor or vendor is not performed.	Remediation Priority: Medium Residual Risk: Medium Recommendation: CLA recommends that vendor due diligence includes a review of a vendor's vendor management practices.

05.01 The Vendor Management Program includes policies and procedures to outline appropriate due diligence, risk assessments, contracting, and oversight of vendors and business partners.

EFFECTIVENESS RATING: Mostly Effective

REVIEWED: Policies and procedures exist for the management of vendors. This includes the processes related to proposals, contract negotiation, purchasing, vendor monitoring and assignment of responsibilities.

FINDINGS: Policies do not seem to require risk assessments.

RECOMMENDATION: CLA recommends that the vendor management program be updated to specifically require risk assessments.

MANAGEMENT RESPONSE:

Contract Policy is acceptable as written. Contract administration procedure options to be evaluated.

TARGET COMPLETION DATE: January 6, 2020

05.02 Vendor risk assessments are performed for all vendors. The risk rating should be determined using qualitative ranking methods. The risk assessments determine vendor criticality from both a security and continuity perspective. This criticality then determines the contractual and monitoring requirements for the vendor.

EFFECTIVENESS RATING: Not Effective

REVIEWED: Risk assessments are somewhat part of the process during vendor selection but the risk assessment itself is not documented so that vendor criticality could be assigned to facilitate monitoring requirements.

RECOMMENDATION: CLA recommends that vendor risk assessments be regularly performed. Risk assessments should determine vendor criticality from both a security and continuity perspective. This criticality then determines the contractual and monitoring requirements for the vendor. The risk rating (high/medium/low/other) should be determined using a qualitative ranking method.

MANAGEMENT RESPONSE:

Procedure options to be evaluated.

TARGET COMPLETION DATE: January 6, 2020

05.03 Vendor due diligence is performed prior to vendor selection. Vendor selection criteria is developed and used to effectively compare vendors and solidify the decision for the vendor selected. Documentation should address:
- Vendor industry experience
- Vendor financial condition and reputation
- Vendor references
- Vendor service level agreements
- Vendor legal and regulatory compliance
- Vendor ability to support clients with Business Continuity Plans (BCP)
If the vendor will have routine access to protected information documentation should also address:
- Review of security controls
- Review of BCP controls
- Review of controls attestation (such as SSAE 18, SOC 2, etc.)
- Incident response plan and cybersecurity event preparedness

EFFECTIVENESS RATING: Partially Effective

REVIEWED: Vendor due diligence seems to be performed prior to vendor selection.
The due diligence procedure is not documented.
The due diligence activities are not documented.

RECOMMENDATION: CLA recommends that vendor due diligence evaluate:
- Vendor industry experience
- Vendor financial condition and reputation
- Vendor references
- Vendor service level agreements
- Vendor legal and regulatory compliance
If the vendor will have routine access to protected information documentation should also address:
- Review of security controls
- Review of BCP controls
- Review of controls attestation (such as SSAE 18, SOC 2, etc.)
- Incident response plan and cybersecurity event preparedness
Vendor due diligence practices verify that vendors in routine custody of non-public personally identifiable information meet specific security criteria established by the organization such as regular patching of systems, limited administrator access, strong authentication, and individual accountability.

MANAGEMENT RESPONSE:
Procedure options and budget constraints to be evaluated.

TARGET COMPLETION DATE: January 6, 2020

05.04 Vendor contracts should be appropriately reviewed (i.e., legal counsel, business owners, and security personnel) inclusion of all appropriate provisions prior to signing. If the vendor will have routine access to protected information, contracts include appropriate security, confidentiality, and breach disclosure provisions including vendor incident response procedures. Contracts should also address right to audit, subcontracting, Business Continuity Plan testing and Recovery Time Objectives/Recovery Point Objectives, data governance, and communication and update expectations regarding security issues. Contracts should define events that constitute contractual default and provide a list of acceptable remedies and opportunities for curing a default.

EFFECTIVENESS RATING: Mostly Effective

REVIEWED: Contracts reviewed that seem to meet the applicable control objectives -

Benefit Focus
Intermedix
Motorola

Contracts reviewed that do not seem to address business continuity -

Florida Blue
Tri-Star

RECOMMENDATION: CLA recommends that all vendor contracts address business continuity.

MANAGEMENT RESPONSE:
Current contract procedures address business continuity; however, Florida Blue and Tri-Star contracts were used as exceptions as a result of negotiations.

TARGET COMPLETION DATE: N/A

05.05 Where appropriate, vendor agreements (SLAs) address support of current operating systems and implementation of critical security patches. Vendor agreements specifically define vendor access to internal systems, remote access provisions, individual accountability for access, and access monitoring.

EFFECTIVENESS RATING: Mostly Effective

REVIEWED: Contracts reviewed that contain service level agreement: Benefit Focus, Intermedix, and Motorola. Contracts reviewed that do not contain service level agreement: Florida Blue and Tri-Star.

RECOMMENDATION: CLA recommends that all vendor contracts address support for current operating systems and the timely deployment of critical security patches for operating systems and applications when applicable. Vendor agreements should specifically define vendor access to internal systems, remote access provisions, individual accountability for access, and access monitoring.

MANAGEMENT RESPONSE:
Current contract procedures address service level agreements; however, Florida Blue and Tri-Star contracts were used as exceptions as a result of negotiations.

TARGET COMPLETION DATE: N/A

05.06 For vendors with routine access to protected information, regular and formally documented vendor monitoring is performed at least annually and includes reviewing:
- Financial condition
- Effectiveness of IT and security controls as represented in a third-party attestation
- Effectiveness of Business Continuity Plans (BCP) and testing
- Incident response plan and cybersecurity event preparedness

EFFECTIVENESS RATING: Partially Effective

REVIEWED: Performance monitoring is performed on an ongoing basis but formal documented vendor monitoring related to financial condition, IT security controls, Business Continuity and Incident Response are not performed for applicable vendors. This process currently is in being implemented with obtaining vendor SOC reports.

RECOMMENDATION: CLA recommends annual, formally documented vendor reviews including:
- Financial condition
- Effectiveness of IT and security controls as represented in a third-party attestation
- Effectiveness of BCP and BCP testing
- Incident response plan and cybersecurity event preparedness

MANAGEMENT RESPONSE:
Procedure options to be evaluated.

TARGET COMPLETION DATE: January 6, 2020

05.07 If a critical vendor uses the services of another vendor, vendor due diligence includes a review of a vendor's vendor management practices.

EFFECTIVENESS RATING: Not Effective

REVIEWED: Although all contracts reviewed contain language related to subcontracting, vendor due diligence of the subcontractor or vendor is not performed.

RECOMMENDATION: CLA recommends that vendor due diligence includes a review of a vendor's vendor management practices.

MANAGEMENT RESPONSE:
Procedure options to be evaluated.

INTERNAL RESPONSE:
Applicable vendors using sub-contractors will be required to submit vendor's management practices concerning due diligence of sub-contractor(s) prior to execution of any contract. Documentation will be electronically stored in Performance Log on the Procurement Services Admin intranet site.

TARGET COMPLETION DATE: January 6, 2020

References

NIST Special Publication 800-30 Risk Management Guide for Information technology Systems, September 2012

NIST Special Publication 800-39 Managing Information Security Risk, March 2011

NIST Special Publication 800-171 Revision 1 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, December 2016

NIST Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations, January 2015

Center for Internet Security Controls Version 7.1, April 2019