Deepwater Horizon Economic Claims Center

Process Review
Financial Controls Report

November 2014

McGladrey

Assurance ▪ Tax ▪ Consulting

McGladrey LLP

1861 International Dr.
McLean, Virginia 22102
O 703.336.6400 F 703.336.6401
www.mcgladrey.com

November 7, 2014

Patrick Juneau
Claims Administrator
Deepwater Horizon Economic Claims Center
935 Gravier Street, Suite 1905
New Orleans, Louisiana 70112

Dear Mr. Juneau:

In accordance with our agreement, effective October 16, 2013, we have performed process review services related to various functions within the Deepwater Horizon Economic Claims Center ("DHECC") and across the Court Supervised Settlement Program ("CSSP"). As part of our engagement, we have completed a process review related to the CSSP financial controls and procedures. This report contains the results of this review, and is divided into the following sections:

- **Executive summary**—provides an introduction to the process review performed, describing our scope and approach, a general description of the manner in which our observations are organized, and some noteworthy positives that we observed in this area.
- **Observations and recommendations**—details our specific observations noted as well as recommendations for DHECC management's consideration.

This report is intended solely for the information and use of DHECC management. This report is not intended to be, and should not be, used by anyone other than DHECC without our express written consent. Notwithstanding the above, DHECC's external auditors, the U.S. District Court for the Eastern District of Louisiana, and regulators may be provided with a copy of this report in connection with fulfilling their respective responsibilities.

We appreciate the cooperation afforded us during this review, and the opportunity to be of continued service to DHECC.

Sincerely,

McGladrey LLP

McGladrey LLP

Table of Contents

Executive summary

Introduction

We have completed an assessment of the financial controls and processes employed by the Deepwater Horizon Economic Claims Center ("DHECC," "Claims Administrator's Office" or "CAO"), as described below. The primary objective of our work was to evaluate the appropriateness and operating effectiveness of the Court Supervised Settlement Program's ("CSSP" or the "Program") system of financial controls. References to the CSSP or the Program broadly include the operation of the Program by DHECC and Program Vendors. Our assessment (the "process review") was conducted in accordance with the applicable American Institute of Certified Public Accountants ("AICPA") consulting standards.

The scope of our review, as outlined in the CSSP Examination Objectives and Scope document included as Exhibit 1 in our agreement, included the following process areas:

- Management controls within the CSSP for budgeting, forecasting, accounting, and financial reporting – *management controls were identified and reviewed for both design appropriateness and operating effectiveness as part of our review of each of the process areas listed below.*
- CSSP compliance with internal procedures, where these exist, or external good practices, including:
    - *Budget procedures* – includes processes to develop and monitor Program-wide budgets, as well as procedures to create and approve re-forecasted information. Due to the organizational design of the CSSP – where the vast majority of operations, and related costs, are driven by several large vendors – we encountered overlap in scope with our Vendor Oversight and Governance review, and will include any duplicative observations and underlying procedures performed in that report.
    - *Travel expense policies* – includes Program-wide processes to submit, support, approve and reimburse travel expenses incurred by CSSP personnel (CAO executive management and vendor employees). This area also includes processes intended to ensure compliance with DHECC's Travel and Entertainment policy.
    - *Procurement procedures* – processes to procure goods and services, including consideration of authorization levels and dollar thresholds, as well as procedures to review, approve, and record vendor invoices and payments.
    - *Cost control and expense management* – processes to understand and manage Program costs, including task order creation and budget monitoring. Other key treasury and cash management functions were also included.
    - *IT security and data protection* – processes to develop and monitor IT security and data protection policies and procedures, including access to and controls around various non-claims systems.
    - *Disaster recovery and business continuity* – processes to implement, maintain, and validate strategies and plans to facilitate the restoration of key operations and resources following a disaster or other disruption.
    - *Policies for safeguarding of assets* – includes the processes to procure, track, dispose of, and secure Program assets.
    - *Compliance with the Code of Conduct and gifts and entertainment requirements* – procedures executed to monitor Program-wide compliance with respective policies, including standardized processes to ensure consistency across all CSSP personnel and CAO-specific compliance with the Code of Conduct.

The following areas were also identified as in-scope processes in Exhibit 1 of our services agreement. However, based on discussions with our client, and duplication of efforts described below, we did not perform any related procedures:

- *Recruiting and vetting of personnel* – processes to identify resource needs, recruit and interview candidates, perform background checks and make offers to individuals. Due to overlap in scope with the court-appointed Special Master, this process area was not included in our review procedures.
- *Use of Management information for identifying process conformance and potential efficiencies* – processes to review vendor performance, evaluate and compare performance to agreed upon tasks orders, and identify and implement opportunities to improve efficiencies or reduce redundancies. We encountered overlap in scope with our Vendor Oversight and Governance review, and will include any duplicative observations and underlying procedures performed in that report.

Approach

We completed the financial controls review procedures in accordance with the CSSP Examination Objectives and Scope document included as Exhibit 1 in our agreement, effective October 16, 2013. The review period covered by this report is CSSP inception through September 30, 2013. Throughout the course of our review, various process changes have occurred. Some of these changes have resulted directly from our work, while others have simply occurred subsequent to the end of our review period. To the extent such changes were deemed to remediate our observations, we have indicated as such in the detail below.

To accomplish our objectives, the following procedures were performed within the respective process areas.

- Performed a risk assessment for each process area to enable a risk-based approach to the review
- Conducted management interviews and walkthroughs in an effort to gain an understanding of processes, procedures, and policies
- Identified risks and risk mitigation strategies, including key controls as well as gaps in risk mitigation strategies (resulting in residual risks to the organization)
- Evaluated and determined the extent to which work prepared by others (such as the DHECC internal audit group) could be relied upon in performing our work
- Developed work programs based on our understanding of process areas and review of relevant documentation
- Obtained and assessed transaction populations for detailed testing and selected samples; requested and obtained supporting documents for samples selected (see Appendix A for additional information pertaining to sampling methodology)
- Executed work programs, developed observations based on exceptions noted, and validated observations with relevant personnel

Throughout our fieldwork, we provided the DHECC with interim reports. Each interim report included those observations that had been identified via supporting documentation and/or discussions with relevant CSSP personnel. As part of this process, recommendations were provided to, and management responses were received from, DHECC management. This report includes observations that have been previously communicated via interim reports.

It should be recognized that internal controls and other risk mitigation activities are designed to provide reasonable, but not absolute, assurance that errors and irregularities will not occur and that procedures are performed in accordance with management's intentions. There are inherent limitations that should be recognized in considering the potential effectiveness of any system of controls. In the performance of most control procedures, errors can result from misunderstanding instructions, errors in judgment, carelessness or other personal factors. Control procedures can be circumvented intentionally by management with respect to the execution and recording of transactions, or with respect to the estimates and judgments required in the processing of data.

Further, the projection of any evaluation of control to future periods is subject to the risk that the procedures may become inadequate because of changes in conditions, and that the degree of compliance with procedures may change over time.

Organization of our observations

During the course of our work, we discussed and validated our observations with management. Our detailed observations and recommendations for improving controls and operations are described in the following section of this report, and are organized by each process area. Within each process area, our observations are classified into three distinct categories, defined as follows:

- Design deficiency ("D") – a business risk has been identified, but no well-designed control or risk mitigation activity exists to properly mitigate the risk.
- Operating effectiveness deficiency ("OE") – a business risk has been identified and a sufficiently designed control or risk mitigation activity exists, but is not operating effectively.
- Process improvement ("PI") – no clear, unmitigated risk exists; however, we see an opportunity to improve the effectiveness or efficiency of the process.

Similarly, we have assigned two ratings to each observation – relative risk and resolution level of difficulty. *Relative risk* is our assessment of the severity of the concern and the potential impact on the operations. *Resolution level of difficulty* is our assessment of the estimated level of difficulty and potential cost to resolve the issue based on our experience and discussions with management. We have assessed both the relative risk and resolution level of difficulty as of the end of our review period. Definitions of the respective ratings are included in the following table:

Rating	Relative risk	Resolution level of difficulty
High	Considered to be of immediate concern and could cause significant operational or financial reporting challenges if not addressed in a timely manner.	Considered to be difficult to resolve and/or will require a significant amount of planning and management involvement/oversight in order to obtain resolution.
Moderate	May cause operational or financial reporting challenges, but does not require immediate attention and should be addressed as soon as practical.	Challenging to resolve and/or does not require a significant amount of planning, but may be time-consuming to implement.
Low	Could escalate into operational or financial reporting challenges, but can be addressed through the normal course of conducting business.	Not complex and/or does not require significant amounts of planning and time to resolve.

Note: Since process improvements are not considered risk mitigation activities, the relative risk of all process improvement observations is indicated as not applicable, or "N/A."

Noteworthy positives

Process review reports are often limited to the identification of areas where the organization is deficient – either due to the lack of a process to appropriately mitigate a risk or an inefficient process to meet the underlying objectives. As a result, such reports often do not inform the reader of areas where the respective organization's internal control environment is sound, or where its processes are efficient. Throughout our process review procedures, we noted various areas of sound business operations, and have summarized several of these below.

Sound internal controls identified

- ✓ Internal controls to mitigate risks related to procurement of goods and services and processing payments are sound. For example, we observed that third party contracts are consistently signed by the Claims Administrator, cash disbursements (non-claims) are properly approved, duties are appropriately segregated in the online banking system, and there are automated controls to prevent the entry of duplicate invoices.
- ✓ Travel & Entertainment expenses incurred by vendor personnel and reimbursed by DHECC are consistently reviewed and approved prior to reimbursement.
- ✓ DHECC management has taken considerable measures in order to establish and demonstrate an ethical tone at the top with respect to its expectations.

Similarly, and sometimes as a result of our process review procedures, we noted areas in which the organization has proactively implemented process changes in an effort to continually improve. The following is a description of some of these noteworthy positives observed:

Process improvements noted

- ✓ Review of invoices, specifically vendor time and expense invoices, has been significantly enhanced, thereby increasing the level of compliance with Travel & Entertainment policy, agreement with contract terms and rates, and frequently resulting in credits back to DHECC.
- ✓ Increased CAO ownership over processes to approve task orders and budgets, and hold vendors accountable for compliance and performance.
- ✓ Through enhancement of the Code of Conduct policy, required acknowledgement by all Program personnel, and implementation of a whistleblower program, DHECC has improved the Program's overall understanding of related expectations.

Observations and recommendations

During the course of our review, we have made a number of observations, which have been discussed with management. Our observations are organized by process area below. Some observations have been included in previously submitted interim reports.

Observation	Type	Recommendation	Management Response
Budgeting, forecasting, accounting, and financial reporting			
1. There is not a formal, routine process for reconciling information among the various systems being used to capture paid-claim data, including: • Claims processing system maintained by BrownGreer • Claim payment system maintained by Garden City Group • Financial reporting system maintained by CAO The lack of reconciliation between these systems increases the risk of incomplete and inaccurate data. *Relative risk: High*	D	Reconcile claim payments per the various systems on a monthly basis. Analyze, explain, and document any reconciling items. Require documented review and approval by the CFO or his designee. *Resolution level of difficulty: High*	We disagree that this is high risk to the Program. All items have been reconciled and no incomplete or inaccurate data was identified. The CAO maintains a check register which is reconciled to GCG's information on a daily basis. Beginning June 2014, the CAO reconciles total payments by claim type, comparing GCG's payment detail to BG's payment table. The CAO coordinates with BG and GCG to identify the cause for any noted variances.
2. During our review period, the budget development process was structured informally and performed inconsistently. As such, there was a risk that the Program and its vendors were not held accountable for their productivity and related expenses. *Relative risk: High*	D	We understand that significant process improvements were made subsequent to our review period. The operating effectiveness of the controls identified should be evaluated in future process reviews. *Resolution level of difficulty: Moderate*	Program budgets are created based on projected activity and utilization rates. Monthly vendor forecasts are approved by the CAO, ensuring resources and production are consistent with CAO modeled expectations. Monthly meetings are held with each major vendor to review actual results in comparison to budget/forecast, and formal task order amendments are required when budget/FTE (s) are exceeded.

Observation	Type	Recommendation	Management Response
3. The processes to prepare and post journal entries in the financial reporting system are not well segregated. During the majority of our review period, the accounting and finance department was limited to two or three individuals. In departments of this size, segregating duties in a manner that sufficiently reduces residual risk to the organization can be difficult. However, without the implementation of mitigating processes (often times detective in nature), there is an increased risk that inaccurate and/or fraudulent transactions will occur. *Relative risk: Moderate*	D	On a monthly basis, review a report detailing all journal entries posted and the user accounts responsible for preparing and posting each entry. Where the same individual completed both tasks, review the supporting documentation for accuracy and reasonableness. *Resolution level of difficulty: Low*	All entries are prepared and subsequently reviewed by different personnel. All activities and monthly reconciliations are performed by the Staff Accountants or Controller. The CFO reviews all journal entries, reconciliations, and resulting trial balance at month end. Since August 1, 2014, all journal entries are now printed with separate preparer and approver sign-offs.
4. The DHECC has not created a process to identify stale checks for purposes of complying with unclaimed property regulation We understand that state escheatment laws are not applicable, since the Program is under the supervision of the US Federal court system. Rather, the Federal court must establish protocols for the treatment of unclaimed property in this case. To date, the courts have not determined the appropriate treatment of unclaimed property. However, without the proper planning and processes in place there is a risk that the organization may incur penalties and fines. *Relative risk: Low*	D	Seek guidance from the U.S. District Court for the Eastern District of Louisiana as to the treatment of unclaimed property. Based on such guidance, create a process that includes the identification of outstanding claim checks that exceed the legal holding period and remittance of such amounts to the appropriate agency. *Resolution level of difficulty: Moderate*	Claims checks are reconciled on a monthly basis including aging tracking. The vendors are currently performing outreach to Payees to validate uncashed checks aging > 90 days. If unsuccessful, checks will be voided with monies returning to the appropriate fund, pending Court decision on the treatment of unclaimed property.

Observation	Type	Recommendation	Management Response
Travel expense policies			
5. It appears that the details of the Travel and Entertainment policy are not well understood throughout the Program. In addition to the exceptions noted in observations #2 through 5 of this section, evidence can be found in the results of rigorous invoice audits performed by the CAO on vendor expense reports and supporting documentation. Lack of understanding increases the risk that improper expenses will be invoiced to, and possibly paid by, the Program. *Relative risk: Moderate*	D	Based on results of invoice audits, develop training or reinforcement activities that are tailored to the challenging areas of each vendor. Evaluate the current Travel and Entertainment policy to determine opportunities for further clarification and simplification. *Resolution level of difficulty: Moderate*	A revised Program Travel & Entertainment policy, which includes additional clarification and specifics concerning documentation requirements for these costs, was distributed in March 2014. Separate follow-up meetings were conducted with the majority of the vendors by the Controller to ensure understanding of the policy requirements and to allow the opportunity for individualized Q&A. In addition, the CAO implemented a more rigorous invoice review process, reducing the risk that improper expenses would be paid by the Program.
6. Section 8.0 of the Travel and Entertainment policy stipulates that personal vehicles may only be used if the use of a rental car is more expensive. We analyzed a sample of ten personal vehicle reimbursement expenses by comparing the amount reimbursed against the estimated cost to rent a vehicle for the same trip. We noted that of the ten reviewed, eight reimbursements appeared to be greater than 20% higher than the equivalent cost of a rental vehicle. These eight reimbursements appear to be in violation of the policy. *Relative risk: Low*	OE	We understand that the CAO has recently implemented a rigorous invoice review process. The design and operating effectiveness of these new controls should be evaluated in future process reviews. *Resolution level of difficulty: High*	In January 2014, The CAO implemented an invoice review process in which the cost of rental cars versus personal mileage is monitored and analyzed. Mileage appearing to be in violation is flagged and elevated to CAO Management for review. If Management deems unreasonable, only the cost equivalent of a rental vehicle is reimbursed. The CFO reserves the right to grant a deviation on a case by case basis if warranted.

Observation	Type	Recommendation	Management Response
7. Section 9.0 of the Travel and Expense policy stipulates that hotel lodging costs should not exceed $170 per night plus applicable taxes. The policy allows for exceptions to the policy if approved by the CFO. Upon review of a sample of invoices, we identified two hotel expense reimbursement reports where the cost of the hotel room was in excess of $170 plus tax without evidence of CFO approval. *Relative risk: Low*	OE	We understand that the CAO has recently implemented a rigorous invoice review process. The design and operating effectiveness of these new controls should be evaluated in future process reviews. *Resolution level of difficulty: High*	In January 2014 the CAO implemented an invoice review process in which the maximum lodging allowance per night is reviewed. Exceptions are flagged and submitted to the vendor. If pre-approval was not obtained, the item will not be paid. The CFO reserves the right to grant a deviation on a case by case basis if deemed warranted.
8. Section 10.1 of the Travel and Expense policy stipulates a per diem schedule for out of town travel. Upon review of a sample of expenses incurred, we noted one expense reimbursement report where per diem rates paid out were in excess of the standards set forth in the Travel and Entertainment policy. The individual was reimbursed for $71/day, rather than the $68/day described in the policy. Additionally, we noted that the full per diem amount was taken for three days of work. However, per review of the invoice, a full day of work was not performed on the third day. Given the employee's 5.5 hour drive back to Houston on the third day, the individual's per diem reimbursement should have been limited to breakfast and lunch, plus a prorata portion of incidentals. In total, the CAO reimbursed the subcontractor $39 more than was appropriate. *Relative risk: Low*	OE	We understand that the CAO has recently implemented a rigorous invoice review process. The design and operating effectiveness of these new controls should be evaluated in future process reviews. *Resolution level of difficulty: High*	The CAO has recently implemented an invoice review process in which the daily per diem allowances are reviewed. For travel via airfare, a copy of the itinerary must be submitted for verification of travel times to determine the per diem application. For ground travel, the hours applied by the employee are analyzed. Full per diem is not permitted on days of travel if labor hours are not equal to or in excess of eight hours.

Observation	Type	Recommendation	Management Response
9. Section 6.3 of the Travel and Entertainment policy states that vendor employees are required to attempt to book the most cost-effective travel by air. In doing so, airline tickets should be purchased at least seven days in advance of the travel date. Upon review of a sample of airline expenses incurred, we noted four instances where individuals purchased airfare within seven days of the departure date. *Relative risk: Low*	OE	We understand that the CAO has recently implemented a rigorous invoice review process. The design and operating effectiveness of these new controls should be evaluated in future process reviews. *Resolution level of difficulty: High*	The DHECC Program strongly encourages contractors to comply with the Lowest Logical Airfare (LLA) provision. We understand that valid business reasons will prevent some travel from being booked 7 days in advance. When travel must occur outside of the LLA provision, CFO pre-approval is required for booking within 48 hours of departure/arrival. The CFO reserves the right to grant a deviation on a case by case basis if deemed warranted.

Observation	Type	Recommendation	Management Response
Procurement procedures			
10. There is a lack of segregation of duties with respect to various aspects of the procurement and payment processes. Specifically, during our review period, the CFO and Analyst II both had access rights that would allow them to perform the following activities: • Create new vendors in Sage • Enter and pay invoices • Access check stock • Reconcile bank statements • Chart of account maintenance Note, the Analyst II had access rights to perform these procedures, but was not trained to do so. During the majority of our review period, the accounting and finance department was limited to two or three individuals. In departments of this size, segregating duties in a manner that sufficiently reduces residual risk to the organization is difficult. However, without the implementation of mitigating processes (often times detective in nature), there is an increased risk that inaccurate and/or fraudulent transactions will occur. There currently exists a review process external to the CAO which serves as a detective control. It is our understanding that BP and the Plaintiff Steering Committee (the "PSC") (collectively, the "Stakeholders") have access to the supporting documentation for all payables transactions, with certain agreed-upon exceptions. See observation 13 below. Further, we understand that BP approves funding of payables prior to disbursements, evidenced via transfer of funds into the operating account. If properly executed, such review procedures would help detect/prevent payment of materially incorrect invoices. *Relative risk: Moderate*	D	Review roles and responsibilities throughout the procurement, fixed assets, and accounts payable processes to ensure appropriate segregation of duties exist. If, due to limited staff within the accounting and finance department, sufficient segregation of duties is not possible, develop monitoring procedures to detect potential abuse of access. While a detective control exists, preventive controls in this area would further enhance the mitigation of these risks. *Resolution level of difficulty: Moderate*	Beginning in March-April 2014, the Finance Department expanded to include additional individuals. Responsibilities have been reviewed and re-assigned to ensure appropriate segregation.

Observation	Type	Recommendation	Management Response
11. There is no formal policy in place that requires the pre-approval of purchases made on behalf of the organization. Due to the nature and structure of the organization, it is unable to obtain credit. Therefore, during our review period, vendors and members of the executive-level management team made purchases using the former CEO's personal credit card. Reimbursement for such purchases was then sought through the expense reimbursement and invoicing process. Similarly, the purchasing process does not require competitive bids to be obtained prior to the execution of transactions greater than a specified threshold (most notably fixed asset purchases). As a result, there is a risk that the organization will incur expenses at a higher cost than necessary. Given the limited volume of purchases made on behalf of the organization, as well as the ability to deny reimbursement for improper or unauthorized purchases, the related risk to the organization was low. *Relative risk: Low*	D	Establish a formal purchase order process and/or credit card in the name of the CSSP to be utilized for all CSSP-related procurement. *Resolution level of difficulty: Moderate*	As of April 2014, a formal policy requiring pre-approval for all purchases made on behalf of the organization has been implemented, including specific levels of authorization requirements based on purchase value. A Purchase Order (PO) form has also been developed, stating the required authorization levels. The PO form must be completed and approved prior to the procurement of goods.

Observation	Type	Recommendation	Management Response
Cost control and expense management			
12. During our review period, invoices submitted by vendors were reviewed in detail by CAO personnel prior to payment. However, in our testing of a sample of invoices paid, it was noted that several vendor invoices were not consistently agreed to supporting documentation (e.g. expense report receipts). Lack of thorough scrutiny over vendor invoices increases the risk that expenses for goods and services will be overpaid. *Relative risk: Moderate*	D	We understand that the CAO has recently implemented a rigorous invoice review process. The design and operating effectiveness of these new controls should be evaluated in future process reviews. *Resolution level of difficulty: High*	Beginning January 2014, the CAO implemented a more rigorous invoice review process. Each line item is traced to the recorded backup provided. All overages are documented, requiring the vendor to seek a formal task order amendment prior to payment issuance. Exceptions are formally documented and distributed to the vendor for resolution. Payment is withheld until all exceptions are addressed.
13. Vendor invoices and supporting documents are not always made available to the Stakeholders in a timely manner. As stated in the Settlement Agreement, the Stakeholders have the right to access invoices and supporting documents submitted to the CAO prior to processing. Exceptions include those invoices that reference claim numbers and agreements related to independent contractors under retainer. To comply with such requirements, all invoices are scanned by the CAO and uploaded to the DHECC SharePoint site for Stakeholder access and review. Upon review of the SharePoint site, we noted that several invoices had not been posted, and did not fall within the parameters of the exceptions described. Lack of a control to make available the required information in a timely manner creates the risk that Stakeholders may not have access to the relevant information. *Relative risk: Low*	OE	Post invoices to the SharePoint site upon receipt and prior to processing by accounts payable. *Resolution level of difficulty: Low*	All invoices not requiring redaction are posted to the Finance SharePoint site and logged onto the weekly AP tracking log within twenty-four hours of receipt, excluding weekends.

Observation	Type	Recommendation	Management Response
14. There is no process to record credits received from vendors into the accounting system. Instead, credits are monitored on a manually maintained spreadsheet. Without entering credits in the system, there is an increased risk that the credits will not be applied timely, if at all, against subsequent invoices. *Relative risk: N/A*	PI	Enter credits into the accounting system when issued. When subsequent invoices are received and entered into the accounting system, ensure that credits have been properly applied. *Resolution level of difficulty: Low*	Since the first quarter of 2014, exception reports are completed documenting any errors resulting in a credit. A copy of the exception report is included with the original invoice and the subsequent invoice containing the credit. These reports are uploaded with the affected invoices on the Finance SharePoint site. All pending reports are reviewed prior to each payment to ensure appropriate credits have been received. If a promised credit is not issued, the CAO can short pay the proceeding invoice utilizing its exception report distributed to the vendor. When credits are applied to subsequent invoices, the credit line items are recorded against the corresponding original account in our financial system.

Observation	Type	Recommendation	Management Response
IT security and data protection			
15. There is no process in place to periodically review physical access to the CAO's data center. The absence of such a review increases the risk that unauthorized access may occur or did occur and that unauthorized access is not detected on a timely basis. *Relative risk: Moderate*	D	Implement a quarterly control for the CAO to review physical access to the CAO's data center to verify that no unauthorized access to the data center has been granted on their behalf and to verify terminated employee access has been removed as expected. Formalize the control to include a process to retain documented evidence that the review was performed as expected and access is as agreed to with the data center manager. *Resolution level of difficulty: Low*	The CAO worked with FOGO Data Centers to formalize who has authority to access the data center. Additionally, a process to review actual and authorized access on a quarterly basis has been developed.
16. A process to deactivate user accounts for terminated personnel within the CAO Active Directory does not exist. Untimely removal or deactivation of user accounts associated with terminated personnel increases the risk that an account can be compromised and unauthorized access could occur. *Relative risk: Moderate*	D	Ensure that the personnel termination process includes removal or deactivation of user accounts. *Resolution level of difficulty: Moderate*	An individual within the CAO is responsible for communicating terminations to the IT department. A process to inform the individual of upcoming terminations was developed and implemented.
17. During our review period, new or modified accounts within the CAO Active Directory, Sage financial reporting, and fixed asset systems were represented to have been informally approved by the Chief Financial Officer; however, such approvals were not documented and retained, increasing the risk of inappropriate access. *Relative risk: Moderate*	D	Formalize the new or modified user account creation process by documenting the approval process. *Resolution level of difficulty: Low*	The CAO has formalized the review process and now requires documentation of new or modified account approvals. The HelpDesk is fully on-line and processes and tracks account requests for all systems.

Observation	Type	Recommendation	Management Response
18. There is no process in place to periodically review the CAO Active Directory user accounts for reasonableness and appropriateness, based on individual roles and responsibilities. The absence of such a review process increases the risk that accounts associated with terminated personnel are not removed in a timely manner, and/or accounts are assigned access that is not necessary for the associated personnel's job function. *Relative risk: Moderate*	D	Create a process to review all user accounts on a quarterly basis. Formalize this process by documenting business management review and approval of user accounts. *Resolution level of difficulty: Moderate*	The CAO has developed a process to review user accounts and will identify the individual(s) responsible for ongoing monitoring. The HelpDesk is fully on-line and processes and tracks account requests for all systems.
19. There is no formal process in place to determine if all relevant system patches have been installed in a timely manner on the CAO server that hosts the Sage financial reporting application. As a result, management did not identify that a critical security patch, MS13-081 released in October 2013 was not installed. By not reviewing vendor supplied operating system and/or application patches in a timely manner, the organization risks unauthorized access or system instability. *Relative risk: Moderate*	D	Revise current patch management process to include verification that critical software patches are being installed in a timely manner. Retain documentation evidencing rationale for uninstalled patches due to lack of applicability or other valid reasons. *Resolution level of difficulty: Low*	The CAO has installed patch MS13-081. The CAO has revised its current patch management process to ensure that critical software patches are installed timely. This process includes appropriate documentation for evidencing rationale for uninstalled patches. In addition, an individual within the IT team will own responsibility for this revised process.
20. Not all CAO Active Directory user account password settings comply with the requirements of the DHECC IT Security Manual. Weakened password configurations increase the risk that an account could be compromised and unauthorized access could occur. *Relative risk: Moderate*	OE	Configure the password setting in Active Directory to require appropriate passwords. If exceptions to the policy are necessary, document the respective business reason and approval. *Resolution level of difficulty: Moderate*	We are aware of certain passwords that are appropriate exceptions to the Policy, and document such exceptions accordingly.

Observation	Type	Recommendation	Management Response
21. The vendor agreements in "Attachment 5" of vendor contracts contain the following requirements for desktops and laptops: • Current and operational anti-virus/malware software. • Installation of personal firewalls, where applicable. • Password-protected screen savers must have a wait period not to exceed thirty (30) minutes. • Critical security patches (i.e., 0/S and applications) must be reasonably current. • Disposal of any desktop/laptop must ensure the complete destruction of all hard drive contents. • Laptops have full disk encryption. As currently written, this wording is fairly high-level and subject to individual vendor interpretation. As a result, risks that this contract language is explicitly trying to minimize may not be appropriately mitigated. *Relative risk: N/A*	PI	Consider amending the contract provisions to more clearly state CAO expectations. Examples include: • Anti-Virus software should be running the most recent security patches and have anti-virus definition files applied within 2 weeks of release, or sooner depending on criticality. • "Where applicable" should be further defined. • Replace reasonably current with "applied within 3 days". • Indicate that destruction should occur using certain standards or guidance, such as the Department of Defense standards. *Resolution level of difficulty:* *Moderate*	We are aware of inconsistencies between our IT Security Policies and the vendor agreements, and have communicated our preferences to the vendors and will work with them to the extent we believe operational changes are needed.

Observation	Type	Recommendation	Management Response
Disaster recovery and business continuity			
22. The Program has not formally established an acceptable disruption period for key systems and business functions, including the operations of all major vendors following a disaster. While it is recognized that the CAO has established Recovery Time Objectives ("RTO"), such RTOs are limited to the CAO's operations, and not the broader DHECC functions that are performed by the various vendors. Without clear RTOs throughout the Program, the sufficiency of the Program's recovery capabilities cannot be determined. *Relative risk: Moderate*	D	Determine the acceptable disruption period for all significant systems and business functions. Establish clear RTOs for each significant system and function. Obtain agreement from all relevant parties regarding the assigned RTOs. Use RTO assignments to determine if current recovery strategies and plans are sufficient across the Program. *Resolution level of difficulty: Moderate*	We disagree that additional actions are warranted. COOP defined RTOs were established by CAO executive management (6/2012), approved by the Claims Administrator and provided to the parties for information and comment. These RTOs were based on what the executive staff established as required to support ongoing CAO and DHECC operations.
23. The Program has not established consistent timeframes and standards for evaluating the adequacy of the claims processing vendors' business continuity plans ("BCPs") and the related recovery planning processes. The CAO has reviewed and approved each key vendor's BCP (or Continuity of Operations Plan, or "COOP"). Specifically, the CAO reviewed the respective vendor COOPs for inclusion of certain elements, but has not reviewed each element for completeness and appropriateness. Additionally, the CAO's COOP was utilized to illustrate the recovery planning expectations of the vendors. However, there is not a clear set of criteria for denoting a vendor's BCP as either sufficient or insufficient. Without a clear set of criteria for assessing the adequacy of the vendors' BCPs, the CAO's evaluation process may be ineffective and significant BCP deficiencies may not be detected. *Relative risk: Low*	D	Establish and communicate specific standards for the evaluation of claims processing vendor BCPs. Include a list of specific elements and considerations that are expected to be addressed within each BCP/COOP, as well as the criteria that would represent satisfying the expectations for each element. Reevaluate vendor BCPs annually. *Resolution level of difficulty: Moderate*	As noted CAO objective was to ensure DHECC vendors had BCP/COOP plans that met or exceeded the current CAO COOP. This evaluation was performed via a review of each vendor's BCP/COOP. The vendors must manage and maintain their plans in a fashion that is effective given their operations and over all companywide standards. The CAO will reevaluate as necessary.

Observation	Type	Recommendation	Management Response
24. The CAO's COOP does not include certain key elements of a BCP. Specifically, it does not outline the resources and processes that would be used to restore each system and resume each business function following a disaster, and does not address key recovery planning topics (including temporary operating procedures and reconstruction procedures). Without a formal and comprehensive BCP, the CAO may encounter unnecessary delays when recovering from a disaster or other business disruption. *Relative risk: Moderate*	D	Develop a comprehensive BCP using the existing COOP and incorporating information on resources used to restore key business systems and processes, as well as temporary operating and reconstruction procedures. *Resolution level of difficulty: Moderate*	The level of recovery documentation was considered to be complete for the most critical operation: communication. Multiple fall back sites, software as a service email system, VOiP Telephany plans, and a MOA exist to ensure the CAO can quickly restore communications. (This is all documented in the COOP). All other business processes provided by the CAO are considered secondary to the Claims Administrator's ability to effectively communicate.
25. Consistent with the current scope of the organization's COOP, the CAO only conducts limited recovery plan testing. Without more thorough testing of the processes that would be used to restore key systems and resume individual business functions following a disaster, the CAO may be unaware of deficiencies in the Program's recovery strategies and/or plans, and key staff may not be sufficiently knowledgeable of their role in a recovery effort. *Relative risk: Low*	D	Expand the organization's COOP testing to encompass additional scenarios and recovery processes, such as: • Situations in which key staff and/or resources are rendered unavailable due to a disaster. • Simulating the actual restoration of key resources and functions after direct impact by an event. *Resolution level of difficulty: Low*	The COOP was updated to include a TT&E (Testing, Training and Exercise) section that incorporates a Simulation Template from NIST.gov.

Observation	Type	Recommendation	Management Response
26. Although the CAO performs regular updates to the organization's COOP, active involvement in such maintenance activities appears to be limited to a small number of individuals, with many key staff members having little or no involvement. As a result, it is difficult to confirm that all required COOP updates are identified and implemented when needed, and there is the potential for certain functional areas and/or individuals to be unaware of the organization's latest recovery plans and strategies. *Relative risk: N/A*	PI	Confirm active participation in the COOP maintenance process from designated individuals across the organization. Require acknowledgement of the receipt of COOP updates as well as confirmation that the latest materials were reviewed for the purpose of identifying content requiring modifications. *Resolution level of difficulty: Low*	The COOP is reviewed twice a year as required by the plan. All executive staff and their direct reports attend these meetings. The CAO has implemented a COOP training program (training is documented by CAO Compliance) to ensure all employees are appropriately trained.
27. The CAO has not identified viable strategies for securing replacement computer equipment following a disaster that impacts the organization's data center. Without viable and defined equipment replacement strategies, the CAO may experience delays acquiring the resources that are required to restore the organization's internal computer systems following a disaster. *Relative risk: N/A*	PI	Identify and establish arrangements to obtain viable equipment to replace the organization's technical equipment following a disaster. *Resolution level of difficulty: Low*	The CAO put a hot-backup server and SAN in place within the FOGO data center to ensure no single point of failure. The CAO has also acquired switches to ensure sufficient capacity for fail-over should an individual switch fail.

Observation	Type	Recommendation	Management Response
28. The CAO has not established a formal program to educate the organization's staff on the COOP and related recovery processes. As the organization increases in size or experiences high turnover, the current informal training and awareness processes may become insufficient, thereby allowing individuals to remain unaware of the CAO's latest recovery plans and strategies, and particularly their role following a disaster or other business disruption. *Relative risk: N/A*	PI	Adopt a formal program to regularly educate the organization's staff on recovery planning concepts and the latest COOP. Consider the following as part of the program: • Provide appropriate COOP information during the new-hire orientation process. • Conduct periodic enterprise-wide training to all staff to maintain and update their understanding of the organization's recovery plans and strategies. *Resolution level of difficulty: Low*	The CAO has implemented a COOP training program (training is documented by Compliance) to ensure that all CAO personnel are provided access to a copy of the most up-to-date COOP and that all CAO personnel are trained on the most up-to-date version of the COOP.

Observation	Type	Recommendation	Management Response
Policies for safeguarding of assets			
29. Limited procedures are in place to monitor and control the purchase, tracking, and disposal of fixed assets. Rather, the CAO and vendors purchase assets as needed and request reimbursement for purchases through the invoicing process. As a result, there is a risk of the following: • Assets are purchased and received without appropriate authorization. • Assets are disposed of inappropriately or without the necessary approvals. • Assets are lost or stolen. *Relative risk: Low*	D	Develop a policy that dictates the following: • Require pre-approval from the CFO for all asset purchases above a specific threshold (e.g. $1,500). • Require pre-approval of all asset disposals. • Perform a periodic physical inventory of assets. • Require approval of adjustments made to the fixed asset schedule as a result of the physical inventory. *Resolution level of difficulty: Moderate*	Policy – vendors must get preapproval for purchases over specific dollar limits per each vendor contract. Physical inventories were performed by vendors in September 2013, and the CAO is performing physical inventories during 2014.
30. In an effort to track all goods purchased on behalf of the CSSP, the CAO has required the tagging of all purchased goods, including those that were or should have been expensed. Tagging of low-cost and/or short-lived goods is unnecessary and inefficient. *Relative risk: N/A*	PI	Require tagging for only those goods that are above the CFO pre-approval threshold (defined above). *Resolution level of difficulty: Low*	Agreed.

Observation	Type	Recommendation	Management Response
Compliance with the Code of Conduct and gifts and entertainment requirements			
31. There is no formal process in place for the CAO to provide guidance to vendors with respect to Code of Conduct training and implementation of a Code monitoring program. The CAO has the responsibility to oversee all vendor Code monitoring programs to ensure each vendor has developed a satisfactory compliance framework. Vendors reviewed had different levels of training, conflict identification systems, monitoring controls and disclosure protocols. Well-trained vendor employees and consistent compliance frameworks will decrease the risk that CSSP personnel operate outside the standards set forth in the Code of Conduct and decrease the risk that the CAO is unaware of potential conflicts of interest or Code of Conduct violations at the vendor level. *Relative risk: Moderate*	D	Develop a minimum standard of vendor activities related to Code of Conduct compliance, including the following areas: • Uniform training program • Conflict identification • Conflict monitoring • Disclosure *Resolution level of difficulty: Moderate*	The CAO developed a uniform training program on the Vendor Code of Conduct requiring the vendors to conduct annual in-person training, with quarterly recertification. The training presentation was distributed to the vendors on 6/10/2014.
32. There is no formal process in place for providing consistent feedback or direction on the treatment, severity, or penalties associated with Code of Conduct violations reported by all vendors. Vendors who disclose potential conflicts of interest and Code violations to the CAO should expect to receive guidance from the CAO on the treatment of the relevant employees. The CAO has historically responded to those potential violations they deemed to be the most severe. The CAO can improve consistency in enforcement of the Code if the CAO recommends a remedy or confirms the Vendor's proposed treatment for trends or conflicts disclosed. *Relative risk: Moderate*	D	Create a process to assess and provide guidance on each conflict of interest or Code of Conduct violation reported. Develop a master listing of all disclosed conflicts of interest and Code of Conduct violations to track each issue's status and remedy. *Resolution level of difficulty: Moderate*	The CAO created a process for providing timely guidance on all potential conflict of interest and Code of Conduct violation disclosures. Vendors report all Code of Conduct violations to the CAO's Chief Compliance Officer who reviews the facts of the violation and either agrees with the vendors' proposed course of action or proposes a new course of action. The CAO developed and maintains a master listing of the aforementioned disclosures to monitor issue status and remedy.

Observation	Type	Recommendation	Management Response
33. The CAO did not have an internal fraud hotline established for the first 18 months of the Program. Without an appropriate forum in which to anonymously communicate unethical behavior, there is a risk that the CSSP was not made aware of Code of Conduct violations. *Risk rating: Moderate*	D	The DHECC *Speak Up* Line, supported by Lighthouse Services, was officially set-up and communicated to all personnel working on the CSSP on January 22, 2014. *Resolution level of difficulty: Low*	Complete - Established in January 2014.
34. A subcontractor of a CAO vendor, responsible for reviewing and scoring grant applications for both rounds of funding, has not signed the Code of Conduct. We noted that the Code of Conduct Version 3.0 states that all vendors, contractors, subcontractors, and consultants are required to abide by the Code. Per discussion with the CAO, they chose not to request that the subcontractor certify the Code of Conduct based on the fact that she does not have access to the claims database and is not involved in the claims process. Our review process confirmed the subcontractor has been involved in the tourism industry in Louisiana for over 20 years, serving in several roles throughout the state. Given her familiarity with the industry and likely connections to local tourism based organizations, instances of conflicts of interest have the potential to arise during the review and scoring of grant applications from organizations within the gulf coast region, and thus the subcontractor should not have been provided an exemption. *Relative risk: Moderate*	OE	Implement a process that validates that all vendors, contractors, subcontractors, and consultants involved in the claims, grant, or other financially related processes have signed the Code of Conduct. Require the subcontractor mentioned herein to disclose all potential conflicts of interest through the CAO's standard on-boarding process. Any disclosed relationships with organizations that applied and/or received grant funding should be reviewed. Consideration should be given to an independent review of grant applications submitted by conflicted organizations and subsequently scored by the subcontractor. *Resolution level of difficulty: Moderate*	The Compliance Officer has met with the subcontractor to ensure she had acknowledged the Vendor Code of Conduct and received training. The Compliance Officer conducted an interview to disclose possible conflicts of interest. A second review of all possible subcontractors was conducted to ensure that all vendors, contractors, subcontractors, and consultants have acknowledged the Code of Conduct. Internal Audit completed its audit of the grant program to ensure that grants have been properly reviewed, scored, and approved.

Appendix A – Standards for consulting services

We performed our work in accordance with the American Institute of Certified Public Accountants ("AICPA") Statement on Standards for Consulting Services ("SSCS"). The SSCS recognizes the difference between attest services and consulting services and that different standards apply to consulting services engagements. These standards recognize that the nature of consulting services work is determined solely by the agreement between the practitioner (McGladrey LLP) and the client (DHECC), and the work is generally performed only for the use and benefit of the client. Consulting services differ fundamentally from the CPA's function of attesting to the assertions of other parties. In an attest service, the practitioner expresses a conclusion about the reliability of a written assertion that is the responsibility of another party, the asserter. In a consulting service, the practitioner develops the findings, conclusions, and recommendations presented. The SSCS are listed below, with a brief description as to how our approach met the respective Standard.

Professional competence*:* The process review team was comprised of individuals with the knowledge, skills, and abilities necessary to execute the procedures in a quality and complete manner. The team consisted of one manager, one senior associate, and one experienced associate. The team was supported by a team of IT specialists, including a director and a manager; a business continuity director; and a code of conduct supervisor. All work was performed under oversight and guidance provided by the engagement partner and an additional manager. Our approach also included review by a quality assurance partner throughout various phases of the engagement.

Due professional care: To execute the process review completely and in a quality manner, and ensure due professional care was instilled in every phase, our project included specific review requirements. Each work program required the review and approval of the engagement partner and team manager after completion of the planning and fieldwork phases. Similarly, a high level review was conducted by the quality assurance partner during the planning and reporting phases.

Planning and supervision: Planning for the process review was performed at the commencement of the engagement. As a result, our approach and engagement schedule was drafted and presented to DHECC points of contact, as well as other relevant stakeholders, for consensus. As needed, additional planning was performed throughout the execution of our work, and amendments to the project planning were communicated and implemented.

Sufficient relevant data: As part of the planning process described above, a sampling methodology was developed and applied to the testing of process controls identified. The sampling methodology is based on a 95% confidence level and 5% tolerable deviation rate. Similarly, as part of the process review approach, documents obtained for purposes of testing process controls were reviewed in a manner that ensured all testing attributes were considered.

Client Interest: We believe that our work was performed with integrity and the necessary objectivity required to satisfy the objectives of the process review. Evidence of such objectivity is found in the observations noted above. Similarly, recommendations have been offered that take into consideration the organization's best interest, including the resources available to it and related risk it faces without implementation.

Understanding with Client: Mutual understanding of the scope of the process review is included in our agreement dated October 16, 2013. During the planning phase of the engagement, our approach and any limitations were more clearly defined and communicated to DHECC points of contact. Throughout execution of the process review, amendments to the approach as well as additional limitations identified were communicated to DHECC points of contact verbally or via formal status reports.

Communication with Client: Throughout all phases of the engagement, we have communicated with DHECC points of contact regarding the scope and approach of our work. Such communication – both formal and informal – included the status of our work, any obstacles or barriers identified and the respective recovery plan, and estimates to complete. Additionally, observations identified were communicated to confirm our understanding for report writing purposes.

www.mcgladrey.com

McGladrey LLP is the leading U.S. provider of assurance, tax and consulting services focused on the middle market, with more than 7,000 people in 75 cities nationwide. McGladrey is a licensed CPA firm and serves clients around the world through RSM International, a global network of independent assurance, tax and consulting firms. McGladrey uses its deep understanding of the needs and aspirations of clients to help them succeed.

For more information, visit www.mcgladrey.com, like us on Facebook at McGladrey News, follow us on Twitter @McGladrey and/or connect with us on LinkedIn.