

Deepwater Horizon Economic Claims Center

Process Review Vendor Compliance Report

November 2014

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 vendor compliance with Service Agreements and Task Orders. 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 an overall conclusion as to the adequacy and appropriateness of existing controls 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

Table of Contents

Executive summary	1
Introduction	1
Approach	2
Organization of our observations	3
Observations and recommendations – BrownGreer, PLC	4
Observations and recommendations – The Garden City Group, Inc.	8
Observations and recommendations – HUB Enterprises, Inc.	9
Observations and recommendations – Postlethwaite & Netterville, APAC	11
Observations and recommendations – PricewaterhouseCoopers LLP	13
Other observations	15
Appendix A – Standards for consulting services	21

Executive summary

Introduction

We have completed a vendor compliance review, as described below, for Deepwater Horizon Economic Claims Center (“DHECC,” “Claims Administrator’s Office” or “CAO”). The primary objective of our work was to evaluate compliance of the five major vendors of the Court Supervised Settlement Program’s (“CSSP” or the “Program”) with their respective service agreements and task orders. The five in-scope vendors included BrownGreer PLC, The Garden City Group, Inc., HUB Enterprises, Inc., Postlethwaite & Netterville, APAC, and PricewaterhouseCoopers LLP. The compliance 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:

- *Vendor delivery of tasks identified in the Task Order* – compliance with contract provisions that pertain to the development and delivery of task orders in a timely manner.
- *Vendor invoicing process, including compliance with rate schedules, role descriptions, use of sub-contractors* – compliance with contract provisions related to information required to be submitted to the CAO as part of the invoicing process, agreement with contract rates, and necessary personnel and non-personnel pre-approvals mandated in the contract.
- *Budgeting and forecasting* – compliance with contract provisions related to the timeliness and reasonableness of vendor budgets and forecasts.
- *Compliance with travel and expenses requirements (including "Other Direct Costs")* – compliance with DHECC’s Travel and Entertainment policy, including submission of sufficient documentation for all expenses, conformity with stated thresholds, and appropriate review and approval by a respective manager.
- *Vendor staffing* – compliance with contract provisions that pertain to the knowledge and background of vendor personnel assigned to the Program and receipt of pre-approval from the CAO for changes in staff, if required.
- *Vendor personnel background checking* – compliance with contract provisions mandating the completion of specific background checks for all CSSP personnel, at the expense of the vendor.
- *Disaster recovery and business continuity requirements* – compliance with contract provisions requiring each vendor to implement and maintain disaster recovery and business continuity plans.
- *IT Security and Data Protection requirements* – compliance with the DHECC IT Security Policy and provisions within the Service Agreement, including access to and disposal of personally identifiable information (“PII”).
- *Vendor compliance with the Code of Conduct, gifts and entertainments requirements, and other relevant legislation* – compliance with the DHECC Code of Conduct policy, including processes to report instances of non-compliance to the CAO. Compliance with legislation was reviewed to the extent of contract provisions.

Approach

We completed the vendor compliance 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. Although our review period ended on September 30, 2013, and our observations were valid as of that date, we have included information provided to us by the vendors and the CAO regarding process changes made after that date. No review procedures have been performed to validate remediation of our observations arising out of these process changes.

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

- Obtained and reviewed each vendor's respective service agreement with DHECC.
- Based on scope areas highlighted above, identified the applicable provisions within each contract, noting similarities and differences among vendor contracts, and developed vendor-specific work programs.
- Conducted interviews and walkthroughs with key personnel in an effort to gain an in-depth understanding of processes, procedures, and policies in place to drive contract compliance for each provision reviewed.
- 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).
- Performed detailed testing using the information made available to us by the vendor at the time of our fieldwork.
- Executed work programs and developed observations based on areas of non-compliance, or exceptions, noted.
- Provided each vendor and the CAO an opportunity to review exceptions noted and provide additional information to evidence compliance with contractual requirements noted in our observations. In such cases, we considered the additional information in final determination of our observations.

As part of our approach, we have provided recommendations for each observation made. The recommendations are addressed to CAO management, and include ways in which the CAO can work with the respective vendor to remediate non-compliance or improve processes. For each observation and recommendation, we have included CAO management's responses.

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.

Organization of our observations

During the course of our work, we discussed our observations with the respective vendor management. Our detailed observations and recommendations with respect to non-compliance are organized by vendor and included in the following section of this report. Similarly, throughout the execution of our work, we noted various process improvements that, if implemented, could result in greater efficiencies for either the CAO or vendors. These observations and recommendations are included in the "Other observations" section of this report.

For all major vendors, the effective date of the contract differs from the execution date, with the effective date predating the actual date on which the contract was executed. In order to provide appropriate context with respect to the timing of our observations, where appropriate, we have indicated the number of exceptions that occurred before and after the contract execution date.

Observations and recommendations – BrownGreer, PLC

During the course of our review, we have made a number of observations, which have been discussed with vendor management. Our observations are organized as described above. *Contract execution date: May 13, 2013. Contract effective date: March 8, 2012.*

Observation	Recommendation to CAO	CAO Response
<p>1. Section 12.1 of the service agreement requires that the vendor must, at its own expense, arrange for a background check for each person who will be working on the Settlement Program. Upon review of BrownGreer's processes to perform and review background checks on personnel working on the Settlement Program, we noted the following deficiencies (Agreement Section 12.1):</p> <ul style="list-style-type: none"> • Background checks on three (3) CSSP personnel (two employees, one contractor) were not arranged as of the execution date as defined in the respective vendor's contract. • Results of background checks performed on subcontractors were not reviewed. • Background checks performed by this vendor did not meet all the criteria of the contract. Specifically, motor vehicle checks, military service verification, and credit checks (as defined in the contract) are not performed. Further, this vendor has not determined that the attributes of background checks performed on subcontractors are complete. 	<p>Review the attributes of the background checks performed on all current CSSP personnel for compliance with contractual requirements. Where gaps in criteria exist, obtain the proper information.</p> <p>As part of the on-boarding process, ensure that the appropriate background checks are performed for all new personnel working on the Settlement Program.</p> <p>Consider requiring all vendors to provide a quarterly assertion to the CAO, stating that they are in compliance with all background check requirements.</p>	<p>The CAO will review the identified criteria and work with the vendor to determine what remedial actions may be warranted.</p>

Observation	Recommendation to CAO	CAO Response
<p>2. Section 15 of the service agreement states that "Vendor shall not subcontract any of its obligations to provide Claims Services under this Agreement to any third party, including any Affiliate of Vendor, without the Claims Administrator's prior written approval of the subcontractor". During our review, we selected a sample of contractors and noted that three (3) of the contractors sampled were not pre-approved by the CAO. In addition, in gaining an understanding of the related processes, we learned that seven (7) additional contractors were hired from an agency after the execution date of the contract and were not submitted to the CAO for pre-approval.</p> <p>Of the 10 noted, all exceptions occurred after the execution date of the contract.</p> <p>Per inquiry, CAO approval of these subcontractors has recently been requested by the vendor.</p>	<p>Validate that the vendor's current process, as communicated, remediates exceptions noted.</p> <p>Through the task order process, reinforce requirement to obtain pre-approval from the CAO for new subcontractors.</p>	<p>BG's current practice is to seek and obtain prior approval in writing from the CAO for any subcontractor hired to work on the Program. The CAO has since approved the 10 subcontractors identified.</p>
<p>3. Section 10.2 of the service agreement requires that the vendor maintain insurance that meets the requirements set forth in Exhibit 4. An exception was noted in relation to carrier ratings. Specifically, the ALPS Property & Casualty Insurance Company for Professional Errors and Omissions is not in compliance with the A.M. Best Insurance Rating Requirement of "A" as set forth in the executed services agreement. The ALPS Property & Casualty Insurance Company, which specializes in legal malpractice insurance, has a rating of "A-".</p>	<p>Mandate that the vendor obtain insurance that meets the requirements set forth in the service agreement.</p>	<p>BG undergoes an insurance evaluation every year and has been advised by their insurance broker that the current malpractice carrier is the only one available to BG. The CAO will work with BG to determine the appropriate next steps.</p>

Observation	Recommendation to CAO	CAO Response
<p>4. During our review period, BrownGreer did not have a process to ensure compliance with contractual security standards. We noted that the vendor did not have a control in place to force remote laptop security patches to be applied.</p> <p>The absence of security standards increases the risk that unauthorized access to systems would not be prevented or detected in a timely manner and would compromise the integrity of the data and systems.</p> <p>Per inquiry, the vendor has implemented a process to review potentially uninstalled patches on remote laptops on a monthly basis.</p>	<p>Validate that the vendor’s current process, as communicated, remediates exceptions noted.</p> <p>Define a formal process to protect systems from security vulnerabilities by downloading, installing and validating that critical security patches are applied to all systems within three days of release.</p>	<p>The CAO has verified with BG their current process and compliance with all security patch updates for non-remote and remote laptops. BG pushes Microsoft (MS) security patches to all laptops and desktops on a pre-defined monthly basis using the SCCM tool. BG uses Nessus to scan systems on a monthly basis to look for anything that is not patch compliant.</p>
<p>5. Exhibit 5 of the service agreement states that “Network firewalls and intrusion detection/prevention devices must be implemented and operational.” During our review period, BrownGreer did not have an intrusion prevention or detection system in place to monitor security events on the company network.</p> <p>Per inquiry, BrownGreer purchased an intrusion detection/prevention system in December 2013.</p>	<p>Validate that the vendor’s current process, as communicated, remediates exceptions noted.</p> <p>Mandate compliance with the network firewall and intrusion detection requirements of the vendor agreements.</p>	<p>The CAO has verified that BG is now in compliance with the requirements related to this observation. We would like to clarify that this related to the internal monitoring of BG’s network. In addition, based on best practices, BG made an internal decision to upgrade to an Intrusion Protection System.</p>

Observation	Recommendation to CAO	CAO Response
<p>6. Exhibit 5 of the Vendor contract states "Authentication is handled over secure, encrypted connections using enforced password complexity."</p> <p>On inspection of a sample of 59 password settings for accounts on the BrownGreer network, we identified one user account that did not have the password policy applied. Specifically, the password settings were not configured to force a periodic password reset. Per inquiry, the single item noted has been corrected.</p>	<p>Validate that the vendor's current process, as communicated, remediates exceptions noted.</p> <p>Recommend the periodic review of user accounts to verify the password policy is in effect.</p>	<p>BG has confirmed that they are in compliance with Exhibit 5 of the Vendor contract, because all accounts are handled over secure, encrypted connections using enforced password complexity. BG has an internal process that requires password changes on regular intervals. The one account noted as an observation was given proper approval in accordance with internal procedure to not follow the change interval. This exception has since been removed.</p>

Observations and recommendations – The Garden City Group, Inc.

During the course of our review, we have made a number of observations, which have been discussed with management. Our observations are organized as described above. *Contract execution date: June 18, 2013. Contract effective date: March 8, 2012.*

Observation	Recommendation to CAO	CAO Response
<p>7. Section 6.8 of the service agreement states that “Vendor shall also submit to the Claims Administrator rolling forecasts of the estimated Charges for the next calendar quarter at least ten (10) days prior to the start of such quarter, and as requested by the Claims Administrator from time to time.” For the review period under review, we noted that the Garden City Group did not submit quarterly forecasts of fees and expenses to the CAO.</p>	<p>CAO has recently implemented stricter processes with respect to obtaining and approving task orders and budgets, including withholding payment of outstanding vendor invoices. The design and operating effectiveness of these new controls should be evaluated in future process reviews.</p>	<p>The CAO has received from GCG the information needed on a timely basis. The Program’s major vendors provide monthly rolling forecast updates (typically received by the 15th of the month) with adjustments to their execution plans. This approach exceeds the contractual requirement of at least ten (10) days prior to the start of such quarter.</p> <p>The CAO will continue with its stricter processes with respect to obtaining and approving task orders and budgets, including withholding payment of outstanding vendor invoices.</p>
<p>8. Section 6.3 of the service agreement mandates that vendor expenses are not to be reimbursed in an amount exceeding the limits of the applicable Task Orders and all travel and travel-related expenses shall be in accordance with the DHECC Travel Policy. A sample of 78 expense report line items submitted to the CAO for reimbursement was selected for detailed testing of supporting documentation. Of the 78 reviewed, four (4) included expense items that were not properly supported. The total value of the four exceptions noted was \$800.</p> <p>Of these four exceptions, all occurred prior to the execution date of the contract.</p>	<p>As part of our Financial Controls review, we noted that the CAO recently implemented a rigorous invoice review process. The design and operating effectiveness of these new controls should be evaluated in future process review phases.</p> <p>Based on results of invoice audits, develop training or reinforcement activities that are tailored to the challenging areas at each vendor.</p> <p>Evaluate the current Travel and Entertainment policy to determine opportunities for further clarification and simplification.</p>	<p>GCG has indicated that 3 of the 4 exceptions were valid mileage expenses which lacked MapQuest screenshots as supporting documentation. Given that only one exception had a financial impact, the CAO will continue to monitor and review vendor invoices for potential exceptions.</p>

Observations and recommendations – HUB Enterprises, Inc.

During the course of our review, we have made a number of observations, which have been discussed with management. Our observations are organized as described above. *Contract execution date: February 25, 2013. Contract effective date: May 4, 2012.*

Observation	Recommendation to CAO	CAO Response
<p>9. Section 12.1 of the service agreement requires that the vendor must, at its own expense, arrange for a background check for each person who will be working on the Settlement Program. Specifically, the contract states that “The Background Check will include a check on certain aspects of an applicant’s or employee’s personal and professional background done by a third party vendor for the purpose of determining eligibility for employment.” Upon review of HUB’s processes to perform and review background checks on personnel working on the Settlement Program, we noted the following:</p> <ul style="list-style-type: none"> • Some of the background check criteria required by the service agreement is performed by HUB instead of a 3rd party provider as required in the service agreement. • Of the 30 samples reviewed, nine (9) exceptions were noted wherein the background checks performed did not include educational verification. These nine exceptions apply to the employees who are not licensed as private investigators. • Interpreters or interpretation companies, who have access to personally identifiable information, have not been subject to background checks. <p>Of these exceptions, all occurred after the execution date of the contract.</p>	<p>Review the attributes of the background checks performed on all current CSSP personnel for compliance with contractual requirements. Where gaps in criteria exist, obtain the proper information.</p> <p>As part of the on-boarding process, ensure that the appropriate background checks are performed for all new personnel working on the Settlement Program.</p> <p>Consider requiring all vendors to provide a quarterly assertion to the CAO, stating that they are in compliance with all background check requirements.</p>	<p>The CAO will review the identified errors and work with the vendor to determine what remedial actions, if any are warranted.</p>

Observation	Recommendation to CAO	CAO Response
<p>10. Section 10.2 of the service agreement requires that the vendor maintain insurance that meets the requirements set forth in Exhibit 4. One exception was noted in relation to minimum amounts of coverage. Specifically, insurance coverage for Commercial Crime is below stated requirements found in Exhibit 4 of the services agreement.</p> <p>Commercial Crime</p> <ul style="list-style-type: none"> • Requirement: \$5,000,000 each claim/ aggregate • Actual coverage: \$1,000,000/ occurrence; \$2,000,000/ aggregate <p>Exhibit 4 of the service agreement indicates that the vendor's General Liability policy includes Commercial Crime coverage. Upon review of the insurance certificate, we noted that the vendor's General Liability and Umbrella policies provide limited coverage for specific types of criminal acts. As such, the vendor's insurance limits for these specific types of criminal acts meet the requirements. However, employee theft and other forms of commercial crime are not covered by the General Liability policy. In addition, the Umbrella policy does not provide excess coverage for the Commercial Crime policy and, as a result, the required limit is not met.</p>	<p>Mandate that the vendor obtain insurance that meets the requirements set forth in the service agreement.</p>	<p>The CAO will work with HUB to determine the appropriate course of action going forward.</p>

Observations and recommendations – Postlethwaite & Netterville, APAC

During the course of our review, we have made a number of observations, which have been discussed with management. Our observations are organized as described above. *Contract execution date: February 26, 2013. Contract effective date: May 4, 2012.*

Observation	Recommendation to CAO	CAO Response
<p>11. Section 12.1 of the service agreement requires that the vendor must, at its own expense, arrange for a background check for each person who will be working on the Settlement Program. Upon review of P&N's processes to perform and review background checks on personnel working on the Settlement Program, we noted that of the 78 reviewed, 63 exceptions were noted wherein the background check completed did not meet all requirements per the contract.</p> <p>Of these exceptions, 57 employees were hired before the execution date of the contract, and 6 after.</p>	<p>Review the attributes of the background checks performed on all current CSSP personnel for compliance with contractual requirements. Where gaps in criteria exist, obtain the proper information.</p> <p>As part of the on-boarding process, ensure that the appropriate background checks are performed for all new personnel working on the Settlement Program.</p> <p>Consider requiring all vendors to provide a quarterly assertion to the CAO, stating that they are in compliance with all background check requirements.</p>	<p>The CAO will work with P&N to determine what appropriate next steps, if any are warranted.</p>
<p>12. Section 10.2 of the service agreement requires that the vendor maintain insurance that meets the requirements set forth in Exhibit 4. Exceptions were noted in relation to carrier ratings and existence of all appropriate coverage. Specifically:</p> <ul style="list-style-type: none"> • Two insurance companies that provide general liability and automobile liability as well as umbrella liability have ratings of 'A-', which is below the contract requirement of 'A'. • No Fidelity blanket bond coverage was obtained. Contract requirement is to obtain coverage in the amount of \$500,000. 	<p>Mandate that the vendor obtain insurance that meets the requirements set forth in the service agreement.</p>	<p>The CAO will work with P&N to determine the appropriate course of action going forward.</p>

Observation	Recommendation to CAO	CAO Response
<p>13. Section 6.3 of the service agreement mandates that vendor expenses are not to be reimbursed in an amount exceeding the limits of the applicable Task Orders and all travel and travel-related expenses shall be in accordance with the DHECC Travel Policy. A sample of 78 expense report line items submitted to the CAO for reimbursement was selected for detailed testing. Of the 78 reviewed, four (4) exceptions to the travel and expense section of the vendor contract were identified, relating to missing support and inaccurate per diem charges. The total value of the four exceptions noted was \$20.</p> <p>Of these four exceptions, all occurred after the execution date of the contract.</p>	<p>As part of our Financial Controls review, we noted that the CAO recently implemented a rigorous invoice review process. The design and operating effectiveness of these new controls should be evaluated in future process reviews.</p> <p>Based on results of invoice audits, develop training or reinforcement activities that are tailored to the challenging areas at each vendor.</p> <p>Evaluate the current Travel and Entertainment policy to determine opportunities for further clarification and simplification.</p>	<p>The CAO and P&N have review processes in place and believe these to be isolated issues. Given the materiality of the finding, no changes are planned at this time.</p>
<p>14. Exhibits 2 and 3 of the service agreement include a Service Rate Schedule and Job Descriptions by title, respectively. In accordance with Section 6.5, the invoices submitted after the effective date of the contract must include itemized detail that agrees to the information in both Exhibits (i.e. job title and rate per hour). A sample of eight (8) invoices and 78 line items was selected for detailed testing. Of the 78 items reviewed, one (1) job title and respective rate did not agree to the information included in the Exhibits.</p> <p>The exception noted occurred after the execution date of the contract.</p>	<p>As part of our Financial Controls review, we noted that the CAO recently implemented a rigorous invoice review process. The design and operating effectiveness of these new controls should be evaluated in future process reviews.</p> <p>Evaluate the detailed requirements of the service agreement to determine opportunities for further clarification and simplification.</p>	<p>P&N has a review process in place and both the CAO and P&N believe this to be an isolated issue. The CAO consistently receives detailed invoice information from P&N on a semi-monthly basis. The CAO will continue with its rigorous invoice review</p>

Observations and recommendations – PricewaterhouseCoopers LLP

During the course of our review, we have made a number of observations, which have been discussed with management. Our observations are organized as described above. *Contract execution date: June 17, 2013. Contract effective date: March 8, 2012.*

Observation	Recommendation to CAO	CAO Response
<p>15. Section 6.9 of the service agreement states that “Vendor shall also submit to the Claims Administrator rolling forecasts of the estimated Charges for the next calendar quarter at least ten (10) days prior to the start of such quarter, and as requested by the Claims Administrator from time to time.” For the review period under review, we noted that forecasts were not provided by the deadline noted within the contract. On at least two (2) occasions (out of six quarters), the forecast start date occurred several weeks prior to the date on which the forecast was submitted.</p>	<p>CAO has recently implemented stricter processes with respect to obtaining and approving task orders and budgets, including withholding payment of outstanding vendor invoices. The design and operating effectiveness of these new controls should be evaluated in future process reviews.</p>	<p>The Program’s major vendors provide monthly rolling forecast updates (typically received by the 15th of the month) with adjustments to their execution plans. This approach exceeds the contractual requirement of at least ten (10) days prior to the start of such quarter.</p> <p>The CAO will continue with its stricter processes with respect to obtaining and approving task orders and budgets, including withholding payment of outstanding vendor invoices.</p>
<p>16. Section 6.1 mandates vendor expenses are not to be reimbursed in an amount exceeding the limits of the applicable Task Orders and all travel and travel-related expenses shall be in accordance with the DHECC Travel Policy included in Exhibit 8 of the service agreement. A sample of 60 expense report line items submitted to the CAO for reimbursement was selected for detailed testing of supporting documentation. Of the 60 reviewed, 14 exceptions to the travel and expense section of the vendor contract were identified, relating to flights not booked at least seven days in advance, and lack of evidence of manager approval of expense reports. The total value of the exceptions noted was approximately \$7,300.</p> <p>Of these 14 exceptions, seven (7) occurred before the execution date of the contract and seven (7) after.</p>	<p>As part of our Financial Controls review, we noted that the CAO recently implemented a rigorous invoice review process. The design and operating effectiveness of these new controls should be evaluated in future process reviews.</p> <p>Based on results of invoice audits, develop training or reinforcement activities that are tailored to the challenging areas at each vendor.</p> <p>Evaluate the current Travel and Entertainment policy to determine opportunities for further clarification and simplification.</p>	<p>As indicated, the CAO has implemented and will continue to conduct a rigorous invoice review process.</p> <p>The six exceptions related to early booking of travel (totaling over \$4,800 of the \$7,300) are not exceptions. The policy states contractor “should” book at least seven days in advance. It says “should” because it is anticipated that this cannot always be the case.</p> <p>The eight items related to manager approval have been addressed. Meetings have been conducted with vendors to provide further training and clarification of the current Travel and Entertainment policy.</p>

Observation	Recommendation to CAO	CAO Response
<p>17. Section 6.5 of PwC's contract states that "All invoices submitted after the Effective Date shall be provided and shall contain... (ii) individual timesheets signed by the personnel and designated managers." Of 78 timesheets tested, a total of 11 were not signed by a designated manager.</p> <p>Of the 11 exceptions, three (3) occurred prior to the execution date while eight (8) occurred after the execution date.</p> <p>In reviewing the vendor's invoices, we noted that the engagement partner signs off on the schedule of hours incurred by all team members during the period, evidencing his review and approval.</p>	<p>As part of our Financial Controls review, we noted that the CAO recently implemented a rigorous invoice review process. The design and operating effectiveness of these new controls should be evaluated in future process reviews.</p> <p>Consider allowing for partner sign-off on time billed (i.e. sign-off on the supporting schedules to the invoice) rather than requiring sign-off on individual timesheets.</p> <p>If individual timesheets are preferred, include review of signatures as a review attribute.</p>	<p>As indicated, the CAO has implemented and will continue to conduct a rigorous invoice review process.</p> <p>PwC has confirmed that the appropriate steps have been taken to strengthen the controls in place to make sure timesheets have the appropriate signatures.</p>

Other observations

During the course of our review, we have made a number of observations that do not specifically pertain to a contract provision or requirement; however, an opportunity to improve the effectiveness or efficiency of a process was noted. These observations and recommendations to the CAO are included in the following table. Because such observations are a by-product of our review, and we were not engaged directly by each vendor, we have generalized the information and removed reference to specific vendors.

Observation	Recommendation to CAO	CAO Response
<p>18. In accordance with the United States District Court Eastern District of Louisiana Order regarding the Confidentiality of Claims Information of the Claims Administrator of the Deepwater Horizon Economic and Property Damages Settlement Agreement, vendors are required to certify their understanding of the Order through execution and submission of Appendix B of the Order, "Certification Regarding Confidentiality of Claims Information". As stated in the Order, "An agency or other entity may provide one Certification applicable to all instances in which the agency or entity would be permitted access to Claims Information under this Order." During the course of our review, we noted that the vendors went beyond the requirement and implemented processes to collect an executed Order from each employee assigned to the Program. We then assessed the effectiveness of those processes. As a result, we noted several instances where employees had not signed the Order in accordance with the respective vendor's process.</p>	<p>Provide guidance to vendors on CAO expectations with respect to executing the Order.</p> <p>If execution of the Order by all Program personnel is not deemed necessary, ensure vendors have the necessary processes in place to inform personnel of the Confidentiality requirements contained within.</p>	<p>As indicated above this is not a requirement of the settlement. The CAO and the vendors have agreed to have employees certify and recertify their certification regarding confidentiality on quarterly basis.</p>
<p>19. Section 2.2 of the standard service agreement mandates that each task order and any subsequent changes shall be made in writing and will require approval via signature of the respective vendor and the Claims Administrator. During our review, we noted that various task orders were not approved prior to the period for which the task order was intended. While the service agreement does not require agreement of task orders by a specific deadline, untimely execution creates the risk that tasks will not meet the objectives of the Program.</p>	<p>CAO has recently implemented stricter processes with respect to obtaining and approving task orders and budgets, including withholding payment of outstanding vendor invoices. The design and operating effectiveness of these new controls should be evaluated in future process reviews.</p>	<p>The CAO has implemented stricter processes with respect to obtaining and approving task orders and budgets. Support of these processes and controls will continue to be retained in order to demonstrate the design and effectiveness of the measures taken.</p>

Observation	Recommendation to CAO	CAO Response
<p>20. Manual invoice adjustments prepared by a vendor during its invoicing process lacked evidence of proper supporting documentation and approval. As a result, we could not trace the invoice detail to records retained by the vendor. Additionally, documentation did not exist showing the final approval of the invoice prior to sending the invoice to the CAO.</p>	<p>Propose the implementation of a formal invoice approval process that documents the vendor's review of adjustments into the billing system. Include in the recommendation the retention of a final version of all invoices, including supporting documentation for all adjustments made.</p>	<p>Since the first quarter of 2014, exceptions identified through the invoice review process are included in a formal report documenting the inaccuracies and posted within the same folder as the original invoice along with any additional support submitted by the vendor to clear discrepancies.</p> <p>In all cases, payment is withheld until all exceptions are addressed by the vendor.</p>
<p>21. As a result of mid-month billing rate adjustments, a vendor's invoice included mathematically incorrect detail. Due to this discrepancy and the fact that the vendor was not able to provide supporting documentation, we were unable to verify the accuracy of the invoice.</p>	<p>Ensure invoices are mathematical accurate prior to submission to the CAO.</p> <p>Per inquiry, to prevent such discrepancies, effective August 2012, the vendor no longer allows mid-month rate changes.</p>	<p>Beginning in January 2014, the CAO implemented a more rigorous invoice review process. Each line item is traced to the recorded backup provided. All amounts are recalculated to ensure mathematical accuracy, often utilizing pivot tables against the raw information to verify totals. All labor rates contained within the invoice are validated against the vendor contract rate table. The DHECC Travel & Entertainment Policy is strictly enforced. CIO approval is also sought on all material IT costs. Payment is withheld until all exceptions are addressed.</p>

Observation	Recommendation to CAO	CAO Response
<p>22. A vendor’s service agreement requires the vendor to report results of Quality Assurance / Quality Control procedures to the CAO on a routine basis. We noted that, during our review period, the vendor had not formally reported such results to the CAO. Per conversation with a vendor point of contact, QA/QC information was reported to the CAO throughout the review period via status meetings and ongoing conversation, for which there are no meeting minutes and therefore no audit trail.</p>	<p>Develop a standard QA/QC report and process to obtain such information on a periodic basis (monthly or quarterly).</p>	<p>CAO will work with applicable vendors to establish requirements for formal documentation to be included in task orders by end of 4Q 2014</p>
<p>23. Some vendors have not developed or administered to their employees a formal training program on the Code of Conduct. Although a training program is not required under the terms of the Settlement Agreement, the risk of vendor employees operating outside of the standards in the Code of Conduct increases without training.</p>	<p>Develop minimum standard operating procedures for vendors to use as guidance when creating training and monitoring programs. Review vendor programs for consistency and compliance with standards created.</p>	<p>The CAO has 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 with certification that training had been completed in June 2014.</p>
<p>24. On several occasions, our procedures required the review of periodic or ad hoc reports prepared by the vendor and submitted to the CAO. Throughout the course of our review, we noted that such reports are not always maintained and readily available for retrieval. Failure to maintain all such reports in a central repository creates a risk that information will be lost and reduces efficiencies when the need for retrieval arises.</p>	<p>Propose maintaining a log of all reports requested by and provided to the CAO, as well as the retention of all reports in a central location, with access limited to the appropriate individuals.</p>	<p>The CAO understands the advantages of a central repository for reports and will look into a cost effective mechanism to achieve the related objectives.</p>

Observation	Recommendation to CAO	CAO Response
<p>25. Exhibit 5 of the service agreements state that logical access to relevant networks and systems should be limited to authorized persons. During our review period, a vendor did not have a process to review their network user accounts for reasonableness, appropriateness, and segregation of duty (“SOD”) conflicts on a periodic basis. 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 or consistent with the associated person's job function.</p> <p>Per inquiry, the vendor has implemented a process to review user accounts for reasonableness on a semi-monthly basis.</p>	<p>Validate that the vendor’s current process, as communicated, remediates risks noted.</p> <p>Work with the vendor to perform a baseline review of all active user accounts, taking into consideration roles, responsibilities, and segregation of duties.</p> <p>Propose the creation of a formal process to review all user accounts on a quarterly basis, including the documentation of management review.</p>	<p>BG has procedures to ensure appropriate permission levels are assigned to new employees and to remove terminated personnel timely. BG has implemented and will continue to monitor the appropriateness of access rights on a quarterly basis.</p> <p>Based upon the CAO's recommendation, BG purchased and installed Team Foundation Server, which supports branching, merging and other larger team oriented abilities.</p>
<p>26. A vendor’s software development methodology does not require sufficient comments within program scripts to define the purpose of each procedure. Inclusion of such details is generally accepted as best practice within the industry of software development programming.</p> <p>The absence of sufficient documentation in software development procedures may result in changes to software which have an unknown impact to the function of the application and/or compromise the data and integrity of the application.</p>	<p>Create minimum standards with respect to SQL programs and the inclusion of sufficient explanations to each procedure defining what actions the procedure is performing.</p>	<p>The CAO IT’s Business Intelligence Group has written a series of SQL and Coding standards. This, in addition to the documenting process of the Change Control Board ensures that the CAO is aware of why, what and where all changes to code are made. These same standards are part of the governance work that IBM has worked with the CAO on in the first two quarters of 2014.</p>

Observation	Recommendation to CAO	CAO Response
<p>27. Formal documented policies are not in place defining requirements and processes for monitoring the network and servers at some vendors. Absence of documented policies can result in failures to detect, communicate and report potential fraudulent activities to appropriate management.</p>	<p>Recommend the development of the following policies:</p> <ul style="list-style-type: none"> • A policy that governs the monitoring of the network and servers, which would include the steps that the vendor is already performing, such as monitoring the servers for CPU usage, Server Waits, Memory usage, etc. • A policy governing the procedures to define data load, processing, monitoring and error resolution, which would include the steps that the vendor is already performing. 	<p>The CAO has worked with Garden City Group to define these items in its data center, which the CAO uses. GCG already has a rigorous execution plan for these items in place – the CAO is working to define it for the CAO’s network in particular.</p> <p>The network monitoring and server maintenance of internal resources at other vendors are only subject to Section 5 of the vendor contracts and it would not be appropriate for the CAO to have input beyond the items required under the contract unless they violate one of the CAO’s approved policies which the vendor(s) have agreed to abide by.</p>

Observation	Recommendation to CAO	CAO Response
<p>28. Section 11.4 of the standard service agreement states that "Vendor shall implement and maintain disaster recovery and business continuity plans that are reasonable and appropriate to the Claims Services under this Agreement, all in accordance with generally accepted industry practices and procedures." Through our review procedures, we determined that the major vendors are complying with this provision of the contract. However, we identified areas in which some of the vendors could enhance their business continuity and disaster recovery programs to meet industry good practices. Specifically, we were unable to obtain one or more of the following:</p> <ul style="list-style-type: none"> • Evidence that the vendor has performed sufficient analysis to establish and justify the acceptable outage period or recovery time objective (RTO) of their individual business functions. • Detailed documentation describing how the vendor would resume business operations following a disaster. • Evidence of thorough and consistent analysis of threats that could cause the organization to experience a disaster and the associated disaster risk. • Evidence that the vendor has established a formal process to evaluate the business continuity capabilities of the organization's key suppliers and service providers. • Comprehensive plans describing the steps and resources that would be used to recover key systems. • Confirmation that a succession planning framework has been defined for the organization's DHECC operations. <p>In addition, although continuing to evolve and supported by true activations of the overall Program's recovery plans, we noted that several of the vendors' BCP testing programs and staff trainings are limited.</p>	<p>Evaluate the current business continuity and disaster recovery provisions within the service agreement to determine opportunities for further clarification, simplification, and improvement.</p>	<p>The CAO has already worked with the vendors in this regard. To the extent permitted under the contracts with the vendors this will be done at least yearly as it has been in 2012 and 2013.</p>

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 compliance 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, two senior associates, and two experienced associates. 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 compliance 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 a second partner during the planning and reporting phases.

Planning and supervision: Planning for the compliance 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 contract compliance. The sampling methodology is based on a 95% confidence level and 5% tolerable deviation rate. Based on this sampling methodology, an exception of one was deemed to evidence noncompliance with the contract provision. Similarly, as part of the compliance review approach, documents obtained for purposes of testing contract compliance were reviewed in a manner that ensured all testing attributes were considered.

Client Interest: Our work has been performed with the integrity and objectivity required to meet the objectives of the compliance 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 compliance 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 and gain concurrence 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](#).

© 2014 McGladrey LLP. All Rights Reserved.