

APPENDIX M

Louisiana Division of Administration Internal Audit Risk Assessment Questionnaire Fiscal Year Ending June 30, 2016

State of Louisiana

Certification Checklist

Prepared by
Louisiana Office of Community Development/Disaster Recovery Unit

RISK ASSESSMENT QUESTIONNAIRE

Fiscal Year Ending June 30, 2016

Section: OCD/DRU
Completed By: Edwin Legnon

Section Head: Patrick W Forbes, P.E.
Date: August 17, 2015

Directions: Answer each question by selecting the option(s) provided that addresses the appropriate response for your section. After each major section of the questionnaire, please add comments to clarify any of your responses. Include any other information not addressed by this Questionnaire that you feel we should be aware of in Section X - Other.

I. TIME AND RESULTS OF PREVIOUS AUDITS

1. Has your section had an audit or review within the last 2 years? (e.g., LLA, IG, Federal Agency, DOA Internal Audit)

☒ Yes

☐ No

If yes, please name auditor and what they audited or reviewed. (Attach additional pages if necessary)

OCD/DRU provides both the DOA Internal Audit Section and the LLA with all audit reports. HUD-CPD performed a Monitoring Review in June 2015 but it has not been issued to OCD for comment.

2. Frequency of your section's routine external state audits (e.g., LLA, IG, etc.):

☒ Annual audit each fiscal year

☐ Audit every other fiscal year

☐ Had audit more than 2 years ago

☐ Had audit more than 5 years ago

☐ No knowledge of section ever having an audit

3. Frequency of your section's routine non-state audits (e.g., regulatory agencies, insurance companies, outside CPA firms, Federal auditors):

☒ Annual audit each fiscal year

☐ Audit every other fiscal year

☐ Had audit more than 2 years ago

☐ Had audit more than 5 years ago

☐ No knowledge of section ever having an audit

4. Previous audit findings or internal control deficiencies (within last 2 years):

☐ No findings or deficiencies noted

☐ Non-reportable findings (discussion comments only)

☒ Reportable findings*

☐ Not Applicable (had no audit or review within the last 2 years)

*Provide name of auditor, report name, finding titles, and date findings were reported:

DOA Internal Audit is in possession of all audits performed on OCD/DRU.

I. TIME AND RESULTS OF PREVIOUS AUDITS (CONT.)

If you have additional information to provide regarding **PREVIOUS AUDITS**, please include below:

[Click here to enter text.](#)

II. OPERATIONAL CHANGES

1. To what extent have procedures, processes and systems changed (added, removed, or updated) in your section within the past 2 fiscal years?

- ☐ No changes have occurred
☒ Only minor changes have occurred
☒ Substantial changes have occurred*
☐ Major changes have occurred to one or more procedures or processes, or a significant new system has been developed and implemented*

*Please explain:

The Division of Administration has introduced statewide changes to the procurement and accounting systems (ProAct and LaGov) which will substantially change the procedures and processes for OCD-DRU.

2. To what extent has reorganization, budget reductions, management turnover, or employee turnover affected your section within the past 2 fiscal years?

- ☐ No changes
☒ Minimal impact
☐ Moderate impact*
☐ Significant impact*

*Please specify changes and the impact the changes have made:

As our programs are being completed, the budget for OCD-DRU has decreased from approximately 600 million to 360 million in fiscal year 21016.sus

3. To what extent has your section increased or decreased in size as a result of the addition or elimination of services or programs within the past 2 fiscal years? (for example: changes in budget, staffing, or areas of responsibility)

- ☐ No changes
☐ Limited increase or decrease in size has occurred
☒ Moderate increase or decrease in size has occurred*
☐ Significant increase or decrease in size has occurred*

*Please specify the impact these changes have made on your processes and staffing efforts:

As our programs are being completed, the budget for OCD-DRU has decreased from approximately 600 million to 360 million in fiscal year 21016.

If you have additional information to provide regarding **OPERATIONAL CHANGES**, please include below:

Click here to enter text.

III. VOLUME OF FINANCIAL ACTIVITY

1. Volume of financial transactions: What is the annual volume of financial transactions processed by your section? Include the volume of transactions processed on behalf of other organizations. For example, accounts payable processed invoices for other sections.

Volume

- ☐ Zero
☐ 1-50
☐ 51-200
☐ 201-1,000
☒ 1,001-10,000
☐ >10,000

2. Value of financial transactions: What is the annual value of financial transactions processed by your section? Include the value of transactions processed on behalf of other organizations. For example, accounts payable processed invoices for other sections.

Value

- ☐ N/A
☐ \$0-\$25,000
☐ \$25,001-\$100,000
☐ \$100,001-\$500,000
☐ \$500,001-\$5 million
☒ > \$5 million

3. Does your section receive any grants that support one or more operational functions?

- ☐ N/A
☐ One grant
☒ Two - three grants
☐ Four - five grants
☐ More than five grants

4. Does your section monitor any grants for other entities?

- ☐ N/A
☐ One grant
☒ Two - three grants
☐ Four - five grants
☐ More than five grants

5. What is the approximate value of grants received or monitored by your section?

- ☐ N/A
☐ \$1 - \$500,000

- ☐ \$500,001 - \$1,000,000
- ☐ \$1,000,001 - \$5,000,000
- ☒ > \$5,000,000

III. VOLUME OF FINANCIAL ACTIVITY (CONT.)

If you have additional information to provide regarding volume of financial and grant activity, please include below:

[Click here to enter text.](#)

IV. INTERNAL CONTROL ENVIRONMENT

1. Please indicate below the liquidity of the assets managed by your section. Liquidity is the ease of the conversion of assets to cash. Consider all asset types in any dollar amount. More than one answer may be checked. Assets controlled by your section:

- ☐ Non-liquid assets or immobile assets
- ☒ Somewhat mobile, but less easily converted, e.g. office furniture, motor vehicles, etc.
- ☒ Easily convertible for resale or personal use, e.g., laptop computers, tools, etc.
- ☒ Cash or cash equivalents, e.g., checks, money orders, etc., either in physical proximity or within the work process

2. Receipt of cash: Does your section collect cash or cash equivalents for any transactions?

- ☐ No receipts are collected in the section
- ☐ Only credit card charges, or debit card payments are received
- ☒ Credit cards, debit cards and/or checks are received (See question below)
- ☐ Cash, credit cards, debit cards and/or checks are received (See question below)

How are checks and cash equivalents stored or maintained overnight while waiting for further processing?

*Please explain:

Checks are logged in upon receipt- stored in a fire proof safe and then transferred to OFSS for deposit.

3. Does your section have a written cash receipts policy?

- ☒ Yes
- ☐ No

4. Disbursement of funds: Is your section involved with the disbursement of funds for certain activities?

- ☐ No disbursements occur within the section
- ☒ Only purchase cards are used as a means of payment in this section
- ☐ Occasional disbursements are made in this section as acquisitions of goods or services occur
- ☐ Regular disbursements occur as an integral part of this section's operations and processes

5. Petty Cash: Does your section maintain a petty cash and/or imprest fund account?

☐ Yes, if selected please provide the total balance of the fund below.

☒ No

Total petty cash: [Click here to enter text.](#) Total Imprest Fund: [Click here to enter text.](#)

IV. INTERNAL CONTROL ENVIRONMENT (CONT.)

6. How many employees in your section are assigned a LaCarte purchasing card?

☐ None

☐ One to three

☒ Four to six

☐ Seven or more

7. How many employees in your section are assigned a travel card?

☒ None

☐ One to three

☐ Four to six

☐ Seven or more

8. Please indicate which situation below appropriately describes your section's operations as it relates to separation of duties. Separation of duties means that responsibilities are assigned so that no one individual in your section controls all aspects of a process or transaction.

☒ Currently, separation of duties is adequate and prevents errors from occurring; collusion would be necessary for fraud to occur

☐ Some individuals have full control over some transactions; however, there are sufficient mitigating controls that significantly reduce risk, such as subsequent review by another person

☐ Some individuals have full responsibility for transactions; however, there are some mitigating controls over the transactions

☐ Some individuals have full responsibility for transactions and there are little or no mitigating controls over the transactions

9. Are any of your section's processes decentralized?

☐ None

☐ Occasionally some of our activities are sent to another location for validation, processing, etc.

☐ Part of our processing necessitates forwarding and completion by another location, vendor, etc.

☒ A large part of the section's regular processing requires forwarding information/documentation to another location/outside vendor for completion

10. How sensitive or confidential is the information processed by your section?

☐ No sensitive data or information is processed (if selected, skip to Question 12)

☐ Small amounts of sensitive data are processed by this section

- ☒ A significant amount of highly sensitive information is processed or used to process work in this section

11. What is the potential for loss of sensitive data? Rate the potential for loss of sensitive or confidential data by your section:

- ☐ High
☒ Medium
☐ Low

IV. INTERNAL CONTROL ENVIRONMENT (CONT.)

12. Pressure to meet deadlines, goals, or budget: Select the most appropriate description for your section.

- ☐ There are few or no pressures or deadlines that could impact performance or decisions
☐ There are occasional pressures or deadlines that could impact performance or decisions
☒ There are considerable pressures or deadlines that could impact job performance or decisions
☐ There are considerable pressures or deadlines either real or perceived that could seriously impact performance or decisions*

*Please explain:

[Click here to enter text.](#)

13. Are there written policies and procedures, in place to guide the execution of activities within the section?

- ☐ There are no written procedures within the section
☐ Some of the section's processes have written policies and procedures
☐ Most of our processes have written policies and procedures
☒ Each activity is documented through written policies and procedures

14. When your agency updates existing policies or develops new policies, how are policy revisions or new policies communicated to your employees? **(Check all that apply)**

- ☒ Emailed to employees
☐ Hard copy provided to employees
☒ Meeting held to discuss policies with employees
☐ Employees required to sign assuring they have received the policy revisions or new policies.
☐ Other **(Please describe)**

Depending on which policy is being updated, different methods may be deployed which would also include hard copies provided to employees and requiring employees to acknowledge their receipt and understanding by their signature.

15. Do you have procedures or processes in place within your section or agency to ensure DOA policies and procedures are followed?

- ☐ No
☒ Yes **(Please describe. Include any annual certifications, internal reviews/audits, employee acknowledgments, etc. Also include the frequency of when those occur; annually, only upon issuance of new policy or policy revisions)**

Click here to enter text.

16. How often are written policies and procedures for your section reviewed and updated for accuracy?
- ☐ Written policies and procedures are not periodically reviewed for accuracy and updated
 - ☐ Written policies and procedures were reviewed and updated more than 5 years ago
 - ☒ Written policies and procedures were reviewed and updated 1 to 5 years ago
 - ☐ Written policies and procedures are reviewed and updated annually

IV. INTERNAL CONTROL ENVIRONMENT (CONT.)

17. What primary controls are used to monitor operational activities within your section?

More than one item may be checked.

- ☒ Established checks and balances exist within each area of the section
- ☐ Peer review of activities
- ☒ Written policies and procedures
- ☐ Supervisory review and/or management approvals

18. Evaluate job responsibilities of employees with opportunities for unethical conduct and indicate the level of exposure below:

- ☐ Not exposed
- ☐ Occasionally exposed
- ☐ Frequently exposed*
- ☒ Continuously exposed to opportunities for unethical conduct (e.g. contractor selection, procurement, confidential information)*

*Please explain:

Many OCD/DRU employees as well as contractor employees have access to confidential information.

19. Are all the employees in your section in compliance with DOA Personnel Policy 95 "Outside Employment?" Has outside employment been disclosed by employees in your section?

- ☒ Yes
- ☐ No

If you have additional information to provide regarding **CONTROL ENVIRONMENT**, please include below:

Click here to enter text.

V. EXPERIENCE AND TRAINING/COMPLEXITY

1. Skills and training. What level of staff training, in general, is involved in performing and maintaining the functions within this section? (More than one response may be selected)
- ☐ No significant level of knowledge or expertise
 - ☐ Limited training and working knowledge required
 - ☒ Training or experienced working knowledge required; tasks are fairly complex and require personal judgment
 - ☒ Specialized expertise is required; tasks are complex and require involved thought processes and ongoing training to maintain an adequate skill level for the position

V. EXPERIENCE AND TRAINING/COMPLEXITY (CONT.)

2. Types of training offered by management to keep employees adequately trained for their job duties: (Check all that apply)
- ☒ Job specific training offered annually
 - ☐ Job specific training offered less than annually
 - ☒ In-house training offered
 - ☒ Computerized training offered
 - ☐ No training offered
3. Length of time the average employee of the section has been in place:
- ☐ 10 + years
 - ☒ 5 - 10 years
 - ☐ 3 - 5 years
 - ☐ 2 - 3 years
 - ☐ < 2 years
4. Length of time the section head has been in place:
- ☐ 10 + years
 - ☐ 5 - 10 years
 - ☒ 3 - 5 years
 - ☐ 2 - 3 years
 - ☐ < 2 years
5. What is the level of complexity of operations in this section?
- ☐ Limited - simple
 - ☐ Minimal - fairly easy to understand
 - ☐ Moderate - somewhat difficult
 - ☒ Significantly complex
6. Employees have direct contact with those who use this section's services
- ☐ Rarely
 - ☐ Occasionally

- ☐ Frequently
☒ Continuously

If you have additional information to provide regarding EXPERIENCE AND TRAINING/COMPLEXITY, please include below:

[Click here to enter text.](#)

VI. INFORMATION TECHNOLOGY AND DATA PROCESSING SUBSYSTEMS

1. Are the main work processes in your section computerized?
☒ Yes
☐ No
2. Are there procedures in place to review, monitor, and update user access to IT systems as employees are hired or separated from employment within your section or agency?
☒ Yes
☐ No
3. Are necessary changes to user access to IT systems made in a timely manner?
☒ Yes
☐ No
4. Are there customized data processing subsystem(s) used only by this section?
☐ No (if this box is checked, skip to section VII)
☐ Only one minor system that supports non-critical tasks
☐ One system that is critical to our operations
☒ Two or more subsystems that support critical functions
5. Within the last year, has there been any downtime which caused a loss of productivity that was due to system error or malfunction of the subsystem noted in question No. 4?
☒ Yes, downtime has occurred. If yes, indicate approximately how often downtime occurred (select one):
 - ☐ 1 or 2 times a year
 - ☒ Once a month
 - ☐ More than once a month
 - ☐ Once a week
 - ☐ More than once a week☐ No downtime has occurred.
6. Has the subsystem in this section been evaluated through any formal review process for its functionality/utility within the operations of your section?

- ☐ No
 - ☐ Evaluated once when first installed
 - ☐ Is evaluated biannually for system problems/errors
 - ☒ Is evaluated on a regular basis (at least annually) for errors and/or downtime when the system is processing and action is taken to alleviate any problems with the system
7. Is access to your section's subsystems controlled through your section?
- ☒ No, other sections are allowed to grant access to our subsystems
 - ☐ Yes

VI. INFORMATION TECHNOLOGY AND DATA PROCESSING SUBSYSTEMS (CONT.)

8. Is subsystem monitoring done in your section? (Monitoring should be interpreted as: documenting change controls, internal or external reviews, exception reporting, etc.)
- ☒ Yes
 - ☐ No
9. Are there manual or automated checks and balances to periodically test the integrity of the data in your section's subsystems?
- ☒ There are periodic checks to test the integrity of the data
 - ☐ There are no checks to test the integrity of the data.

If you have additional information to provide regarding INFORMATION TECHNOLOGY AND DATA PROCESSING SUBSYSTEMS, please include below:

The prime IT contractor is required to report all subsystem outages in its monthly SLA report. Target availability is 98%; actual available averages >99.9%, and has not fallen below target in 4 years. Subsystem outages are typically resolved in <1 hour. Typical reasons for loss of productivity include the following: a server needs to be re-booted; a spreadsheet load contains a formatting error; a VPN connectivity error occurs; an error occurs in a security device interface; the WAN service provider experiences an outage; or there is a power failure.

VII. DISASTER RECOVERY AND BACKUP SYSTEMS

1. Is there a disaster recovery plan in place within this section?
- ☒ A formalized and regularly updated disaster recovery plan has been created for the section
 - ☐ A limited disaster recovery plan has been designed for most of our critical processes
 - ☐ No disaster recovery plan has been established for the section's critical processes (if this box is checked, go to Section VIII)
2. If there is a disaster recovery plan in place within the section, has the plan been audited by internal or external auditors or another DOA section?
- ☐ Never been audited

- ☐ Audited within the last 10 years
- ☒ Audited within the last 5 years
- ☐ Audited within the last 2 years
- ☐ Audited annually
- ☐ No disaster recovery plan is in place within the section

VII. DISASTER RECOVERY AND BACKUP SYSTEMS (CONT.)

3. Has a remote site been established for the routine back-up of data that is located a reasonable distance in miles from the main computing headquarters? **(This question is only for OTS)**

- ☒ Yes, within 25 miles
- ☐ Yes, approximately 25-50 miles away
- ☐ Yes, approximately 50-75 miles away
- ☐ Yes, greater than 100 miles away
- ☐ Other* **Please explain below:**

Through the use of our backup utility CommVault, all of our main systems and data repositories are backed up regularly and have set retention schedules to ensure our data is accessible in a system failure. In addition, our state data center (ISB) is backed up to the other state data center (DPS) for failover purposes. These sites are approximately 7 miles apart.

If you have additional information to provide regarding DISASTER RECOVERY AND BACKUP SYSTEMS, please include below:

In addition to the backup procedures and offsite backup, OCD/DRU has a Disaster Recovery site at the North Louisiana Venyu Data Center. This is considered a hot site where OCD/DRU would be able to resume operations quickly after a system failure.

VIII. FRAUD RISK FACTORS

1. Has your section developed and implemented any antifraud controls and programs?
- ☐ Antifraud controls and an antifraud program have not been developed **(if this box is checked, skip to question 4)**
 - ☐ Antifraud controls and an antifraud program have been developed, but have not been implemented
 - ☒ Antifraud controls and an antifraud program have been developed and implemented

2. How often are fraud controls assessed and revised in the section?
- ☐ Never, they are not a high priority
 - ☐ They are assessed and revised, as needed, every 5 years
 - ☒ They are assessed and revised, as needed, biannually
 - ☐ They are assessed and revised, on an annual basis
3. If your section has antifraud prevention controls and programs, are employees aware of your section's antifraud prevention controls and programs?
- ☐ Employees are not aware of the existence of antifraud prevention controls and programs within the section
 - ☒ Employees are aware of the existence of antifraud prevention controls and programs within the section
4. Are the codes of conduct and ethics policies enforced throughout your section?
- ☒ The Code of conduct and ethics policies are not enforced throughout the section
 - ☐ The Code of conduct and ethics policies are somewhat enforced throughout the section
 - ☐ The Code of conduct and ethics policies are strictly enforced throughout the section

VIII. FRAUD RISK FACTORS (CONT.)

5. Has the potential for detecting and preventing fraud taken on a lesser priority because of budget reductions?
- ☐ Yes, our priorities are more focused on getting the work out
 - ☒ No, detecting and preventing fraud remains a priority in this section
6. Would most of the section's employees know the signs of fraud in the workplace?
- ☒ Yes
 - ☐ No
7. Have employees in this section had some form of training in the area of recognizing signs of fraud?
- ☒ Yes
 - ☐ No
8. What is the likelihood of employees in your section reporting suspected fraud?
- ☐ Employees are likely to ignore suspected fraud
 - ☐ Employees are likely to report suspected fraud but will report it anonymously
 - ☒ Employees are likely to report suspected fraud
9. Was any fraud/theft identified in your section within the following time frames?
- ☐ Five or more years ago
 - ☐ Two to five years ago

- ☒ Within the last year
☐ None ever identified

10. Approximately how often does your section perform some type of fraud risk assessment to consider ways that fraud and misconduct can occur?

- ☐ A fraud risk assessment is not performed
☐ A fraud risk assessment is performed annually
☐ A fraud risk assessment is performed semi-annually
☒ A fraud risk assessment is performed quarterly

If you have additional information to provide regarding **FRAUD RISK**, please include below:

Fraud Risk Factors are constantly being reviewed, assessed and updated. The degree of documentation and training will depend on the level or inherent risk each program has.

IX. OUTSOURCING INTERNAL CONTROLS THROUGH CONTRACTS

1. What percentage of the section's work processes is done through the use of contracts with outside vendors?

- ☐ None, we do all of our work in the section. (If this answer is checked, please skip all remaining questions in this section.)
☐ Less than 10%
☒ Between 10 - 50%
☐ Greater than 50%

2. What is the number of contractual agreements that your section has with outside vendors?

- ☐ 1 to 3 contracts
☐ 4 to 6 contracts
☒ 7 or more contracts

3. What is the dollar magnitude of the contracts identified in Question #2 above?

- ☐ Less than \$10,000
☐ \$10,000 to \$100,000
☐ \$100,000 to \$500,000
☒ Greater than \$500,000

4. Do any employees within this section have any conflicts of interest, ownership in, or other relations with any contractors or vendors this section does business with as described by the Louisiana Code of Governmental Ethics (R.S. 42:1101)?

☐ Yes, **if selected please explain**

☒ No

[Click here to enter text.](#)

A key internal control is a control that, if it fails, there is at least a reasonable likelihood that a material error in the financial statements would not be prevented or detected timely. In addition, a key internal control may be controls related to information systems, security, or the administration of confidential information.

5. Would you consider any of the contractual agreements that your section has with outside vendors to constitute an outsourcing of a "key internal control" of your section?

☒ Yes

☐ No

IX. OUTSOURCING INTERNAL CONTROLS THROUGH CONTRACTS (CONT.)

When key internal controls are outsourced, a user entity can strengthen the internal controls of its overall operations by requiring the outsourced vendor to undergo a Statement on Standards for Attestation Engagements (SSAE) 16 review of its operations. The result of a SSAE 16 review is the issuance of a Service Organization Control (SOC) report by the independent reviewer (CPA firm, etc.). If the outsourced control is related to financial reporting, a SOC 1 report might be appropriate. If the outsourced control is more operational in nature or relates to an information processing system, a SOC 2 or SOC 3 report will provide a more appropriate review of the security, availability, processing integrity, confidentiality, and privacy of the processing system of the contracted vendor.

6. Do the contracts your section has with outside vendors require a SOC 1, 2, or 3 report?

☐ None of our contracts have a provision for obtaining a SOC report.

☒ Some of our contracts have a provision for obtaining a SOC report.

☐ All of our contracts have a provision for obtaining a SOC report.

7. Do the contracts your section has with outside vendors require other forms of assurance from the outside vendors to determine controls and processes are operating effectively?

☐ None of our contracts have a provision for obtaining additional assurances.

☒ Some of our contracts have a provision for obtaining additional assurances.

☐ All of our contracts have a provision for obtaining additional assurances.

If you have any additional information to provide regarding OUTSOURCING, please include below:

OCD-DRU has determined that two of its contracts do represent outsourced key internal controls. One of the contracts expired on January 15, 2015 and has not been renewed. The second expired on March 15, 2015 and was rebid with requirements to submit to an independent SSAE 16 engagement. In addition, OCD-DRU did have an additional two contracts that represented outsourced key internal controls, however they are now managed by OTS.

X. OTHER

Do you have any other areas of concern, either in your section or anywhere else in the Division of Administration (DOA) that should be considered in the DOA's overall risk assessment? If so, please list the areas and explain below:

This is not really an area of increased risk, but the one function in our office that doesn't really receive substantial external review is the compliance and monitoring group, who perform external review of grantees. It may be helpful to have an internal DOA review of their processes and activities.