OREGON COMMISSION FOR THE BLIND

CLIFTONLARSONALLEN LLP

John Fisher, CPA, CGFM, Partner
3000 Northup Way, Suite 200
Bellevue, WA 98004-1446
425-250-6024 *phone*
John.Fisher@CLAconnect.com

This document and the information contained within is considered Proprietary & Confidential and not to be reproduced, duplicated or disclosed without expressed written consent from Oregon Commission for the Blind

CliftonLarsonAllen
www.cliftonlarsonallen.com

CliftonLarsonAllen LLP
300 Northup Way, Suite 200
Bellevue, WA 98004-1446
425-250-6100| Fax 425-250-6050
www.cliftonlarsonallen.com

November 26, 2013

Ms. Dacia Johnson
Oregon Commission for the Blind
535 SE 12th Ave
Portland, OR 97214

Dear Ms. Johnson,

This report provides you, Oregon Commission for the Blind (“OCB”) leadership, the Commissioners, and members of the Board with the results of the Enterprise-Wide Risk Assessment and a means to prioritize risk mitigation strategies. An enterprise-wide risk assessment is the first step in your risk management program of assessing risks, evaluating risks and controls, reviewing control effectiveness, and implementing strategies to achieve the Board’s acceptable risk level.

The Enterprise-Wide Risk Assessment was performed in accordance with statement on standards for consulting services established by the Institute of Internal Auditors (IIA), Control Objectives for Information Technology (COBIT) standards, and guidelines provided by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

CliftonLarsonAllen (“CLA”) was not engaged by OCB to conduct a financial audit, for which the objective would be the expression of an opinion on the financial statements. Had we been hired to perform an audit of financial information in accordance with U.S. generally accepted auditing standards, other issues may have come to our attention that would have been reported to you. Therefore, we express no opinion on the effectiveness of OCB’s internal controls over all or any part of its financial reporting.

In addition, the procedures performed by CLA are not a substitution for management’s responsibility to maintain a system of controls to mitigate risk. The Enterprise-Wide Risk Assessment was designed to provide OCB with insight to inherent and specific risks throughout the organization. Our procedures alone cannot identify errors and irregularities related to the scope of this project.

We appreciate the opportunity to assist OCB in performing this assessment. Management and staff involved in the process were a pleasure to work with and very open to sharing their opinions and knowledge. This cooperation was invaluable to the outcome of this project. If you have any questions, please feel free to contact us for assistance.

Sincerely,

CliftonLarsonAllen LLP

John Fisher, CPA, CGFM
Partner
425-250-6024
John.Fisher@CLAconnect.com

Table of Contents

Executive Summary

CLA performed an Enterprise-Wide Risk Assessment for OCB. This included identifying and ranking the key financial, operational, and information technology (IT) processes within the organization based on inherent and specific risks. The overall risk for each process was based upon the process's potential impact to the organization and the vulnerability of the risk occurring given the current environment. The risk environment is dynamic and will continue to change; therefore, risk should be assessed on an ongoing basis with a formal Enterprise-Wide Risk Assessment performed periodically.

Documentation for the Enterprise-Wide Risk Assessment consists of an enterprise-wide risk map encompassing the significant functional areas or processes within OCB. The enterprise-wide risk map is a graphical representation of the relative impact and vulnerability of a risk event for each of the key financial, operational, and IT processes. Detailed results are also provided communicating the explanation for the risk ranking and recommendations for addressing the risks.

Approach

With the assistance of OCB management, CliftonLarsonAllen identified 16 key stakeholders in the key functional business areas identified above. Key stakeholders were interviewed for the purpose of assessing the inherent and specific risks associated with each functional business area.

Upon completion of the interviews, the inherent and specific risks identified in each process were prioritized and placed on the enterprise-wide risk map based on the impact of the process to the organization, and the vulnerability of the risk occurring (see Appendix A for further description of the definitions of impact and vulnerability criteria).

What is Risk Assessment?

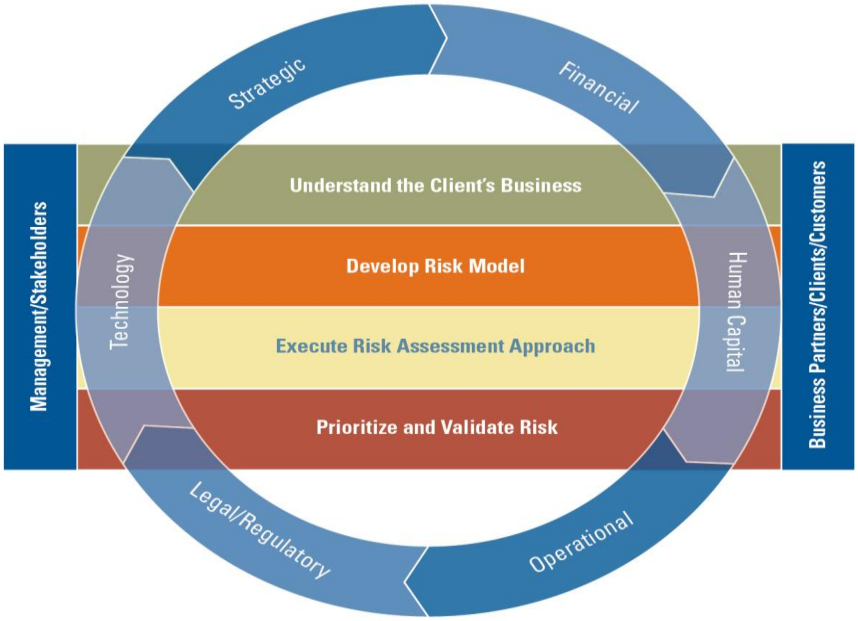
Risk assessment is a systematic process for utilizing professional judgments to evaluate probable adverse conditions and/or events and their potential effects on the company. The process starts with identifying risks associated with business objectives linked through all levels of OCB whether it is entity or process level.

- **Entity level** is the cornerstone for effective control and its objectives provide guidance on what the entity wants to achieve. It should be consistent with budget, strategy, and business plans.

- **Process level** should align with entity level objectives but differ in that they relate directly to goal setting with specific targets and deadlines. It provides guidance for management focus.

Risk Assessment Methodology

The following model illustrates the CliftonLarsonAllen methodology utilized throughout the Enterprise-Wide Risk Assessment for OCB.


Strategic
Financial
Management/Stakeholders
Understand the Client's Business
Develop Risk Model
Execute Risk Assessment Approach
Prioritize and Validate Risk
Technology
Human Capital
Business Partners/Clients/Customers
Legal/Regulatory
Operational

Understand the Client's Business: We begin by understanding OCB's business by gathering the business objectives, goals, and strategies in addition to the key financial, operational, and IT processes. Next, we assess the external and internal risks related to the industry.

Develop Risk Model: We begin by defining risk and creating a risk framework. Risk is an event or condition that can negatively affect the ability of an organization to achieve its objectives. Risks are generally thought to be associated with taking actions; however, risks can also occur when no action is taken in the form of missed opportunities. There are six types of risks:

- **Strategic:** The risk that business objectives will not be met due to poorly defined business strategies, poorly communicated strategies, or OCB's inability to execute these strategies due to inadequate organizational structure, infrastructure or alignment. Strategic risk is managed by appropriate organizational governance. Failure to adequately plan and execute against organizational goals may result in significant damage to OCB's reputation.

- **Financial:** The risk that OCB's financial reporting is inaccurate, incomplete, or untimely due to a variety of factors including the pace of change, the amount of uncertainty, the presence of a large error, or the pressure on management to meet certain expectations.

- **Transactional/Operational:** The risk that OCB's operational processes are not achieving the objectives they were designed for to support the business model. This risk addresses inefficient operations, poor alignment of processes with objectives and strategies, failure to protect assets, etc.

- **Compliance/Legal/Regulatory:** OCB is subject to a variety of federal, state and local laws, regulations and directives, or financial agencies. Failure to follow prescribed directives may result in substantial fines, restrictions, loss of business, and/or legal action taken by regulators.

- **Technology:** This risk considers the level of use, sophistication, complexity, robustness, ease of use and speed, and accuracy of recovery/replacement of systems. This risk addresses the overall importance of technology within OCB and the availability and quality of information OCB can access to support decision making, and the security of key information.

- **Human Capital/People:** This risk addresses the type of behaviors encouraged by management; the methods used to reward employees; the approach to consistently enforce policies and procedures; the selection, screening, and training of employees; and the reason and frequency of turnover. It also includes the length, consistency, and nature of business relationships, including the handling of sensitive or confidential information and the risk that business interruption would seriously impact those relationships.

Next, we define impact and vulnerability criteria applicable to OCB to be utilized as a tool for risk ranking procedures. In determining risk within the financial, operational, and IT processes, we assessed the impact of the process to OCB and the vulnerability that a risk would occur by evaluating the underlying attributes of the process and by assessing the effectiveness of the control environment around that process. The criteria are defined in terms of High, Moderate, and Low. See illustration below for definitions.

Areas of Focus	Criteria
Impact	• Financial • Strategic/Stakeholder • Reputation • Compliance / Legal / Regulatory • Transactions / Operations
Vulnerability	• Control Effectiveness • Speed of Management Response • Process Complexity • Human Capital / People • Operational Efficiency / Policy & Procedure Deficiencies • System Capability / Maturity • Previous Incidents / Findings
Measurement Scale	• High Risk • Moderate Risk • Low Risk

Execute Risk Assessment Approach: We begin by identifying various company participants, including key risk owners and conduct interviews, as applicable. Key risks are gathered during this stage and results are ranked by defined impact and vulnerability criteria.

Prioritize and Validate Risk: Risks identified are prioritized and placed on an enterprise-wide risk map. An enterprise-wide risk map is a graphic tool that assists in plotting the risk's relative impact and vulnerability of a risk event for each of the key financial, operational, and IT processes. Risks are then validated and shared with management, as appropriate. By prioritizing and validating risks, OCB can align and prioritize its resources to manage and mitigate risks appropriately.

Project Overview

Objectives and Scope

The objective of the Enterprise-Wide Risk Assessment was to identify the key financial, operational, and IT processes at OCB and assess the levels of risk within each of the process areas. In addition, provide Management with visibility to process areas that contain the highest potential risk as determined by the risk assessment process.

The scope of the Enterprise-Wide Risk Assessment included the following functional areas / processes within OCB:

Functional Area / Process	Detailed Coverage of Functional Area / Process
Governance	Mergers and acquisitions, business development, senior leadership, commissioners, board of directors, strategic plan, internal policies and procedures, and vendor relationships
Accounting / Finance	Financial close and reporting, accounting operations, budgeting, reconciliation of significant account balances, accruals, estimates and reserves, journal entry review, chart of account maintenance, segregation of duties
Cash Receipts	Cash receipts, accounts receivable management, cash handling, donations/contributions
Grant Administration	Grant identification, grant writing, expense tracking and monitoring, accounting, reporting
Purchase to Pay	Purchasing controls and thresholds, disbursements/accounts payable, payment processing, vendor maintenance, purchasing cards, employee expense reporting
Information Technology	IT infrastructure, security (logical and physical), operations, change management, disaster recovery, data reporting capabilities, hardware and software, applications, servers, wireless networks, and help desk
Programs and Services	Business Enterprise Program, Rehabilitation Services, Orientation and Career Center, Vocational Rehabilitation, Youth Services, Business Services, and Independent Living Services
Compliance	Internal audit, compliance, regulatory requirements, fraud detection and prevention
Human Resources & Payroll	Payroll, benefits, records management, FTE workload, recruiting, hiring, terminations, performance monitoring, new hire integration, employee retention, training and development, incentive program

Conclusions

The overall risk for each process was based upon the process's potential impact to the organization given the current environment without the consideration of controls. As such, all risks identified where based on the inherent impact. The risks identified potentially could have a different risk ranking if the organizations internal controls, policies and/or procedures were also assessed. Based on our risk assessment process we identified a total of 39 identified risks. They consisted of 12 high, 21 moderate and 6 low risk issues. This determination of risk was made based on our review of industry best practices, potential vulnerability and impact, and risk based conversations completed with key OCB stakeholders. The following table summarizes the seven high risk issues CLA identified during our assessment in order of potential risk to OCB. See remaining risks in the "Detailed Results" section below for moderate and low ranked items.

Functional Area / Process	Risk Ranking	Identified Risk
Governance	High	The organization does not have a documented strategic plan to communicate the key business objectives and goals of OCB. In addition, the initiatives currently in place are not linked back to strategic planning.
Governance	High	Comprehensive and documented policies and procedures are not in place to allow for consistent processes across the organization and a documentation trail in the case of personnel turnover. Examples include, but are not limited to, the following: grants, case management, payroll, human resources, programs, inventory, accounts payable, cash receipts, etc. In addition, OCB has not developed an ongoing training plan for all employees related to adherence to policies and procedures.
Grant Administration	High	A grant roster is not maintained to centrally track and monitor completeness and accuracy of current grants as it relates to hours and expense allocations by individual grant. In addition, the roster would also be tracking the grant status and renewal date.
Information Technology	High	The organization does not periodically review all permissions assigned to user accounts and roles assigned to users in System 7 to validate employees and approved business partners continue to have appropriate access based on job responsibilities.
Information Technology	High	An independent review has not been performed addressing exposures and risks of the information technology environment.
Information Technology	High	OCB has not performed an external penetration test or internal vulnerability assessment.
Information Technology	High	Software and infrastructure changes to the System 7 application are not tracked and monitored.
Compliance	High	Processes and internal controls are not consistent and streamlined across the organization. Processes and internal controls should be continually assessed and/or improved to mitigate the potential risk of financial loss, operational/IT inefficiencies and breakdowns, fraud activity and regulatory violations.

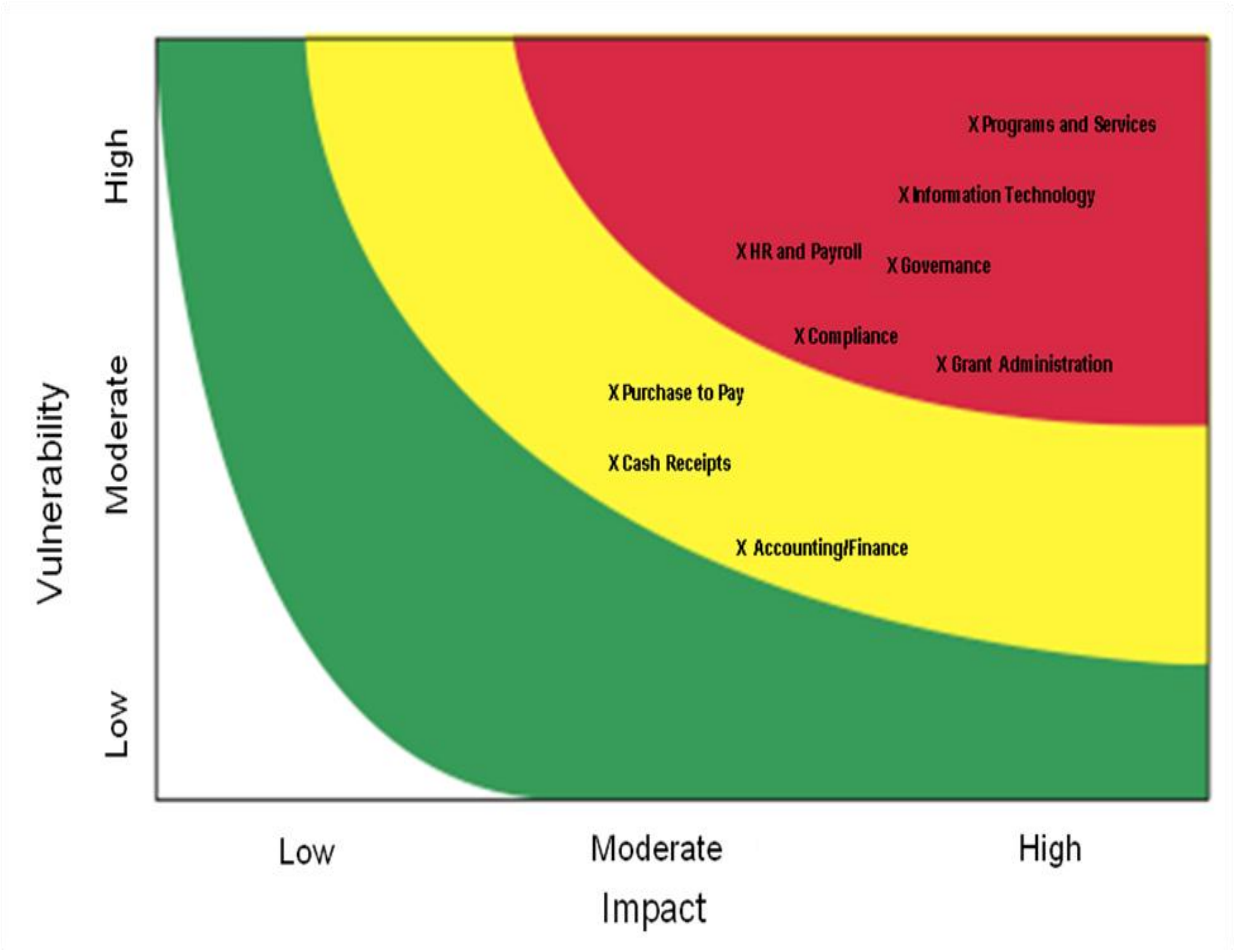
Functional Area / Process	Risk Ranking	Identified Risk
Programs and Services	High	OCB has not performed an in-depth and detailed review of the effectiveness, impact, fiscal spending and potential legal risks to the organization for specific programs that are being offered.
Programs and Services	High	Due to the lack of a formal human resources department, OCB has not consistently executed employee performance evaluations related to all personnel including program management.
Programs and Services	High	Concerns related to the fiscal responsibility of the vendors in the Business Enterprise program. OCB currently does not maintain controls to review and/or validate the accuracy and completeness of vendor's financial statements (profit/loss information) which drives the revenue generation for the program.
Human Resources & Payroll	High	OCB does not have a dedicated HR resource and responsibilities are performed on an ad hoc basis by various individuals within the organization.

Risk Assessment Results

Enterprise-Wide Risk Map

The enterprise-wide risk map communicates the risk results at the functional area / process based on the information obtained during the interviews. The description of the risk map is as follows:

- Green – Low Risk
- Yellow – Moderate Risk
- Red – High Risk



Detailed Results

Per discussions with key stakeholders, CLA identified several processes where specific risks may exist. These risks identified were considered in the overall risk ranking of each key functional business area. The risks identified were based upon discussions with key stakeholders and not based on actual testing of controls. The following is a list of the risks identified by CLA, in addition to the risk ranking and recommendations for addressing the risks.

Functional Area / Process	Risk Ranking	Identified Risk	Proposed Recommendations	Management Response
Governance	High	The organization does not have a documented strategic plan to communicate the key business objectives and goals of OCB. In addition, the initiatives currently in place are not linked back to strategic planning.	Develop a documented strategic plan that outlines specific goals and objectives of the organization and programs. In addition, the strategic plan should include specific initiatives to align with the goals and objectives. The plan should extend to a minimum of 3 years looking forward.	Management agrees with this recommendation. The agency is currently engaged in creating an agency specific management system that will align our key goals and outcomes that will position the Commission to be able to create a data and outcome driven strategic plan that will impact service delivery for Oregonians who are blind.
	High	Comprehensive and documented policies and procedures are not in place to allow for consistent processes across the organization and a documentation trail in the case of personnel turnover. Examples include, but are not limited to, the following: grants, case management, payroll, human resources, programs, inventory, accounts payable, cash receipts, etc. In addition, OCB has not developed an ongoing training plan for all employees related to adherence to policies and procedures.	Review all key business functions of the organization and assess where there appears to be a lack of documented policies and procedures. Develop documented policies and procedures to reflect current practices. In addition, policies and procedures should be reviewed and updated by management on a periodic basis defined by management (i.e. minimum of annually), and communicated to appropriate parties each time an update is made. Finally, develop an annual training plan for key policies and procedures and require employee attendance.	Management agrees with this recommendation. The agency intends to create a consistent enterprise wide approach to policies and procedures to reflect current practices that are reviewed and updated on a periodic basis. Updates and new policies will be communicated to appropriate parties when policies are developed and updated and staff will be trained as appropriate.

Functional Area / Process	Risk Ranking	Identified Risk	Proposed Recommendations	Management Response
	Moderate	There is not a whistleblower policy in place that defines procedures an employee should follow to report inappropriate and/or unethical behavior.	Develop a whistleblower policy that communicates procedures an employee should follow to report inappropriate and/or unethical behavior. The policy should be reviewed and updated by management on a periodic basis defined by management (i.e. minimum of annually), and communicated to appropriate parties each time a policy update is made. In addition, employees should be reminded of the policy at a minimum on an annual basis via formal communication.	Management agrees with this recommendation and the agency complies with statewide policy pertaining to whistleblower protections. We will establish an internal procedure to address this issue and communicate the process with staff.
	Moderate	Due to the lack of a formal human resources department, OCB has not consistently executed employee performance evaluations related to all personnel.	Perform a competency review of all managers in relation to roles, responsibilities, qualifications and capabilities. An assessment should include the following at a minimum: • Assess formal or informal job descriptions or other means of defining tasks that comprise particular jobs. • Adequacy of employee retention and promotion criteria and information-gathering techniques (e.g., performance evaluations). • Management personnel appear to have the appropriate educational background, certifications and ongoing training necessary for their assigned level of responsibility.	Management agrees with the recommendation and this has already been addressed. In August of 2013 the agency entered into an interagency agreement with the Department of Administrative Services Shared Client Services for Human Resource Services.

Functional Area / Process	Risk Ranking	Identified Risk	Proposed Recommendations	Management Response
	Moderate	Several individuals appeared to be concerned about employee morale within the organization. Satisfaction surveys were recently distributed and results appeared to communicate that morale was increasing. However, individuals communicated they were not 100% forthcoming in those surveys. Although the surveys were anonymous, employees were still concerned on whether they would somehow be identified.	Continue to obtain feedback from staff related to tone at the top, culture, morale, etc. In addition, continue to be open and communicate with employees on the business changes with the organization and initiatives and allow employees to take a role in those changes, as deemed appropriate. Employee morale tends to increase if they feel emotional ownership in what they do and where the organization is headed. If specific business functions appear to have more challenges than others, identify the root cause to see if issues can be directly addressed.	Management agrees with this recommendation. In order for the agency to effectively carry out the mission of the organization, we need a highly skilled, engaged workforce. One of our key goals identified in our management system speaks specifically to staff engagement. We are creating outcome and process measures to ensure we are attending to this this key goal.
	Low	IT is currently not presenting a strategic plan or updating the Commission Board members on the current state of the infrastructure and department on a reoccurring basis.	IT should be developing and presenting a technology based strategic plan to the Commission Board as well as providing an executive summary of the current state of the department and infrastructure on a reoccurring basis.	Management agrees with this recommendation. We are currently communicating information technology issues to the Commission and we review the framework and content of the information presented and reviewed to the Commission.
Accounting and Finance	Moderate	Key responsibilities within the accounting and finance departments were identified as having a general lack of cross training resulting in certain positions being sole-sourced.	Determine where additional cross training opportunities could be implemented at each key position to mitigate the risk of only 1 person knowing how to perform various responsibilities.	Management agrees with this recommendation. As we increase our documented policies and procedures, we will better be able to identify the key areas that will benefit from cross training.
	Moderate	Currently, payroll reconciliation between time sheets and payroll reports is not being completed.	Perform a review of payroll reports to determine the completeness and accuracy of time sheet information that was entered.	Management agrees with this recommendation and is currently looking into ways to improve this process using existing statewide resources.
	Low	OCB currently maintains a small store	Perform a cost/benefit to determine if the	Management agrees with this

Functional Area / Process	Risk Ranking	Identified Risk	Proposed Recommendations	Management Response
	🟩	that accepts cash and checks for products sold. Currently there is a lack of audit procedures related to the cash receipts and inventory processes.	store should remain in operation. If yes, formal procedures should be implemented around reconciling cash receipts and inventory.	recommendation. In order to minimize the risk, agency management has significantly reduced the amount and type of products on hand at any time in order to simplify and streamline the store operations.
Cash Receipts	Moderate	OCB currently has a significant outstanding receivables balance that is greater than 30 days past due.	The accounting and accounts receivable departments should perform a review of the past due report to identify the individual vendors that are currently holding past due payments. Collection procedures (phone calls, formal letters and potential legal action) should be enhanced to aggressively work on obtaining outstanding dollar mounts.	Management agrees with this recommendation. This is concentrated in one program within the agency. The program has established a process of collecting back debt and monitoring current payments due in order to prevent this from happening again.
Grant Administration	High	A grant roster is not maintained to centrally track and monitor completeness and accuracy of current grants as it relates to hours and expense allocations by individual grant. In addition, the roster would also be tracking the grant status and renewal date.	Develop a grant roster to centrally track and monitor grants and enhance visibility of the status of all grants and monitor hours and expenses incurred based allowable requirements.	Management agrees with this recommendation and there is a process in place to provide centralized access to grant status. We will explore means to improve our process.
	Moderate	Expenses are not always charged against the appropriate grant due to a potential lack of understanding of the purpose of various grants.	Provide training related to appropriate expenses that are allowable under each grant and enhance monitoring of expenditures charged against grants.	Management agrees with this recommendation and will explore means to provide training and improve our processes to ensure that expenses are charged to the appropriate grant and enhance monitoring of expenditures charged against grants.
	Low	As a result of legislative restrictions, the OCB does not maintain a resource dedicated to identifying grants and other funding source opportunities on	Perform a cost/benefit analysis to determine if it makes good business sense to dedicate additional resources to the grant identification process. In addition,	Management agrees that the agency resources have declined over time due to the economic conditions facing state government in the past several years. In

Functional Area / Process	Risk Ranking	Identified Risk	Proposed Recommendations	Management Response
	🟩	a regular basis.	identifying other funding source opportunities.	order to meet the growing need for services, particularly in the areas of technology and independent living services for Oregonians who are blind, alternate funding sources may need to be considered to the extent they are available.
Purchasing	Moderate	Documentation is not required to be maintained related to a purchase (i.e. purchase order); all purchases are not required to be approved; approval thresholds for purchases have not been established (with the exception of a $5k approval that potentially appears inappropriate as any employee can make a purchase without approval if the purchase is under $5k).	Require all purchases to be approved by a department manager or independent employee regardless of the amount of the purchase.	Management agrees that documentation should be required and maintained to substantiate all purchases. This is our current practice to make sure all expenditures are reasonable and necessary. Currently vocational rehabilitation counselors authorizing services on behalf of clients have independent expenditure authority and agency management does periodic monitoring to ensure expenditures are reasonable and necessary and consistent with rules and regulations. We are open to further testing to determine the right balance between management oversight of all purchases and timely efficient delivery of client services.
	Moderate	Client cases and related expenses are not reviewed by an independent employee to validate purchases appear appropriate, align with client needs, etc.	Implement an expense monitoring process to review client cases and related expenses on a periodic basis. The review should be performed by someone other than the individuals (i.e. counselors) directly involved in the case.	Management agrees with this recommendation. We have implemented independent reviews of client and non-client payments on a periodic basis.
	Moderate	Purchasing limits have not been established for all individuals that have spending capabilities.	Perform a review to identify where specific spending limits have not been established (Management, Counselors and Information Technology). Develop and implement specific dollar thresholds	Management agrees with this recommendation. Although most staff with expenditure approvals are automated in the client case management system. We will review our systems and

Functional Area / Process	Risk Ranking	Identified Risk	Proposed Recommendations	Management Response
			for individuals that are identified to not maintain formal spending authorities.	processes to formalize expenditure authorities for all applicable positions.
	Moderate	A detailed review is not being completed by an independent OCB employee related to individual disbursements for accuracy.	An independent OCB employee should be reviewing all disbursements (AP, travel expenses, client payments) to source documents to validate appropriateness and accuracy.	Management agrees with this recommendation and will review our existing policies and procedures to improve our systems related to disbursements to ensure they are consistent with best practices within other state agencies.
Information Technology	High	The organization does not periodically review all permissions assigned to user accounts and roles assigned to users in System 7 to validate employees and approved business partners continue to have appropriate access based on job responsibilities.	Periodically (i.e. semi-annually) review all permissions and user roles in all systems and applications to ensure permissions are consist with job responsibilities and user roles are assigned appropriately to employees and approved business partners. The review should be documented, including any changes made as a result of the review.	Management agrees with this recommendation. We believe we can build this into our already established Information Technology Inventory Process that takes place.
	High	An independent review has not been performed addressing exposures and risks of the information technology environment.	An information technology general control review should be completed by an independent party to identify potential control weaknesses.	Management agrees with this recommendation and can work with the State Data Center to identify and address any potential control weaknesses.
	High	OCB has not performed an external penetration test or internal vulnerability assessment.	OCB should have a network external penetration test and internal vulnerability assessment performed annually by an independent third-party security firm that was not involved in the initial installation or configuration or currently engaged to manage the network.	Management agrees with this recommendation and can work with the State Data Center to identify and address any potential control weaknesses.
	High	Software and infrastructure changes to the System 7 application are not tracked and monitored.	All software and infrastructure changes should be tracked in a centralized area and have documentation including, but not limited to, the following: Description	Management agrees with this recommendation. There is a centralized issue tracking system that tracks the information outlined in the

Functional Area / Process	Risk Ranking	Identified Risk	Proposed Recommendations	Management Response
			of software or infrastructure change, date of change request, user requesting change, priority of change, approver, test plan documentation, back out plans, etc.	recommendation. Agency management will review the use of the tracking system for consistency and effectiveness.
	Moderate	Password strength and complexity for System 7 and Active Directory does not meet best practices.	Implement, at a minimum, the following end user password settings for System 7 and active directory: • 8 character minimum length • Complexity enabled • 90 day change frequency • Password history of 12 • Invalid login attempts set to 5	Management agrees with this recommendation and will work with the State Data Center to make sure we are utilizing best practices established within state government when available.
	Moderate	Physical security controls related to the server are not appropriate.	Physical security mechanisms (key card or key pad) should be implemented to ensure only current employees and approved business partners have access.	Management agrees with this recommendation and will work with the State Data Center to make sure we are utilizing best practices established within state government when available.
	Moderate	Active Directory and System 7 administrators are not required to have stronger, more complex passwords that non-privileged users.	Develop a dual password policy structure in System 7 and active directory to require administrators technically by the system / application to have stronger, more complex passwords than non-privileged users. If a system limitation is restricting OBC from using dual password policies, administrators should be required administratively via a written policy to have stronger, more complex passwords than non-privileged users. The following settings are recommended for administrators: • 15 character minimum length • Complexity enabled • 60 day change frequency • Password history of 24	Management agrees with this recommendation and will work with the State Data Center to make sure we are utilizing best practices established within state government when available.

Functional Area / Process	Risk Ranking	Identified Risk	Proposed Recommendations	Management Response
			• Invalid login attempts set to 3	
	Moderate	A strategic plan and security policies have not been established and maintained to provide for the overall direction and configuration of information security over new and modified network and communication software, systems software, application systems, data structures and end-user responsibilities.	Review each functional IT area across OCB to determine if sufficient policies and procedures exist. Where deficiencies are identified, develop policy and procedure documents. In addition, review current policies and procedures to determine if changes need to be made. Communication and implementation of new policies and procedures and changes to existing should be consistent. Some examples would be: • Network & Security Device • Workstations • Peripheral Devices • Server(s) & Operating Systems • Password controls • Acceptable usage	Management agrees with this recommendation and will work with the State Data Center to make sure we are utilizing best practices established within state government when available.
	Moderate	OCB does not maintain a formal business continuity or disaster recovery plan.	Formally develop and document a plan that would address how to maintain operations and technology in the event a disaster occurred.	Management agrees with this recommendation and will work with the State Data Center to make sure we are utilizing best practices established within state government when available.
	Moderate	Key responsibilities within the information technology department were identified as having a general lack of cross training resulting in positions being sole-sourced.	Determine where additional cross training opportunities could be implemented to mitigate the risk of only 1 person knowing how to perform various responsibilities.	Management agrees with this recommendation and will work with the State Data Center to make sure we are utilizing best practices established within state government when available.

Functional Area / Process	Risk Ranking	Identified Risk	Proposed Recommendations	Management Response
	Low	Workstations and laptops are not encrypted.	IT should encrypt all laptops and workstations to prevent the potential threat of loss or theft of sensitive data.	Management agrees with this recommendation and will work with the State Data Center to make sure we are utilizing best practices established within state government when available.
	Low	Parameters are not set to technically enforce computers to lock after a set period of time defined by the OCB which could result in inappropriate personnel accessing workstations.	Change the parameters to technically enforce computers to lock after the defined period of time described in the IT Security policy.	Management agrees with this recommendation and will work with the State Data Center to make sure we are utilizing best practices established within state government when available.
Compliance	High	Processes and internal controls are not consistent and streamlined across the organization. Processes and internal controls should be continually assessed and/or improved to mitigate the potential risk of financial loss, operational/IT inefficiencies and breakdowns, fraud activity and regulatory violations.	Perform reviews across key functional areas of the organization to evaluate current internal controls and identify gaps and recommendations for improvements. Based on what was learned from the risk assessment, an internal control review should focus on the following functional processes: • Information technology general controls • Segregation of duties in significant processes • Policy and procedure review for significant processes once developed • Purchasing • Employee expense reimbursements • Grant administration • Accounts payable • Cash receipts • Fleet vehicles • Inventory	Management agrees with this recommendation. The agency has begun to develop an annual internal audit plan that will address the areas of risk identified in this assessment report as well as additional risk concerns based on management's expectations. Internal audit activities will be completed throughout the year by an independent and objective service provider. In addition, the agency will also perform ongoing risk assessment discussions with key stakeholders to validate if there are any changes at the Commission that would require modifications to the annual internal audit plan. Upon completion of each internal audit, a formal report will be issued and communicated to appropriate parties. The report will detail audit objectives, procedures performed, results and detailed recommendations.

Functional Area / Process	Risk Ranking	Identified Risk	Proposed Recommendations	Management Response
	Moderate	OCB has not formalized and implement procedures specific to the protection and processing of non-public data elements including but not limited to: • Medical response information • Social Security Number • Date of Birth • Driver's License Number • Private Health Information	OCB should develop and implement policy statements and controls related to non-public information including: • Definition of non-public data • Protection of non-public data • Appropriate storage • Manual records storage	Management agrees with this recommendation and will review its current policies and procedures related to non-public information, compare those with current state and federal standards and make improvements to our internal policies and controls and needed.
	Moderate	Supporting calculations and reports for regulatory reporting to the local, state, and federal government are not always reviewed prior to submission by someone independent of the person performing the calculation.	All supporting calculations and reports reporting to the local, state, and federal government should be reviewed and approved by someone other than the individual performing the calculations and reporting.	Management agrees with this recommendation and will review our current practices surrounding report completion and submission to see where we may be able to seek and obtain an outside review prior to submission.

Functional Area / Process	Risk Ranking	Identified Risk	Proposed Recommendations	Management Response
Programs and Services	High	OCB has not performed an in-depth and detailed review of the effectiveness, impact, fiscal spending and potential legal risks to the organization for specific programs that are being offered.	OCB should perform an extensive assessment of all programs currently offered. This assessment should include the following: • Is the program providing training and education to blind and disabled individuals to instill confidence and build skills in all aspects of day-to-day life? • Is the program effective by offering the appropriate services and skills that it was originally established for? • Has a cost/benefit analysis been performed to validate that the program is fiscally responsible? • Is the spending appropriate based on the intent of the program and attendance? • Is the program putting the OCB in undue risk? Including, but not limited to, risk of lawsuit due to (1) lack of qualifications and training of program personnel; (2) program personnel not being appropriately licensed; (3) state requirements not being appropriately met/maintained.	Management agrees with this recommendation. The agency is currently engaged in creating an agency specific management system that will align our key goals and outcomes that will position the Commission to be able to create a data and outcome driven management system for the organization. This management system will align to the strategic plan and key goals and outcomes established by the Commission and each program will be responsive to determine how it is performing through specific, targeted measurements and outcomes.
	High	Due to the lack of a formal human resources department, OCB has not consistently executed employee performance evaluations related to all personnel including program management.	OCB should perform and assessment to determine if the current programs personnel's level of commitment and competency is appropriate based on overall roles and responsibilities. Determine if program employees	Management agrees with the recommendation and this has already been addressed. In August of 2013 the agency entered into an interagency agreement with the Department of Administrative Services Shared Client

Functional Area / Process	Risk Ranking	Identified Risk	Proposed Recommendations	Management Response
	🟥		maintain the level of qualifications needed for their specific/particular. Assessment should consist of the following: • Assess formal or informal job descriptions or other means of defining tasks that comprise particular jobs. • Perform an analysis of the personnel knowledge and skills needed to perform jobs adequately. • Review appropriateness of OCB’s organizational structure, and its ability to provide the necessary information flow to manage its activities. • Review adequacy of definition of key stakeholders’ responsibilities, and their understanding of these responsibilities. • Assess the adequacy of knowledge and experience of key personnel and related responsibilities. • Assess the physical demands of the roles and responsibilities. • Adequacy of employee retention and promotion criteria and information-gathering techniques (e.g., performance evaluations). • Do program personnel appear to have the appropriate educational background, certifications and	Services for Human Resource Services.

Functional Area / Process	Risk Ranking	Identified Risk	Proposed Recommendations	Management Response
			ongoing training necessary for their assigned level of responsibility?	
	High	Concerns related to the fiscal responsibility of the vendors in the Business Enterprise program. OCB currently does not maintain controls to review and/or validate the accuracy and completeness of vendor's financial statements (profit/loss information) which drives the revenue generation for the program.	Perform an assessment and/or review of the vendor's financial reports to determine if a formal audit should be performed to validate adequacy and accuracy of information being provided. In addition, assess the need to provide additional training related to fiscal reporting for the program participants.	Management understands this recommendation and will seek to obtain the active participation of the Business Enterprise Consumer Committee (BECC) as to the best way to implement the recommendation and the timing and process of conducting such an assessment.
	Moderate	OCB is currently under staffed to meet the needs of the individual vendors participating in the Business Enterprise program.	Perform an assessment of the employees currently in the Business Enterprise program to determine current status of workload. Based on the assessment, determine if the program should hire additional resources to improve the support level for the individual vendors. In addition, need to assess the current Business Enterprise employees to identify if staffing changes need to be made to improve relationships with licensed customers.	Management agrees with this recommendation. At the present time the agency is seeking to further understand of all of its responsibilities as the state licensing agency. If it is determined that additional staff are required, the increased hiring authority would require legislative action and is not within the control of the agency. The agency is currently working through a process of strategic communications engagement with the managers in the program that we expect will improve and strengthen relationships within the program.
Human Resources & Payroll	High	OCB does not have a dedicated HR resource and responsibilities are performed on an ad hoc basis by various individuals within the organization.	Perform a cost/benefit analysis to determine if an individual dedicated resource should be hired to manage and address personnel, training, recruiting, performance evaluations, etc. An outsourced relationship can also be	Management agrees with the recommendation and this has already been addressed. In August of 2013 the agency entered into an interagency agreement with the Department of Administrative Services Shared Client

Functional Area / Process	Risk Ranking	Identified Risk	Proposed Recommendations	Management Response
	🟥		considered if this appears to be more cost effective for OCB.	Services for Human Resource Services.
	Moderate	Performance evaluations for staff are not consistently completed by all departments and individuals. In addition, there is not an HR dedicated resource to track and monitor the completion of performance evaluations.	Review the processes, timelines, and methods to track and monitor timely completion of performance evaluations with each department across the organization. Determine if changes should be made to enhance the processes, frequency, and monitoring activities of performance evaluations.	Management agrees with the recommendation and this has already been addressed. In August of 2013 the agency entered into an interagency agreement with the Department of Administrative Services Shared Client Services for Human Resource Services.
	Low	Payroll processes are very manual (i.e. Excel spreadsheets are used to calculate and approve sick and vacation time)	The Information Technology group should review the current use of technology for payroll processes to determine if there are additional opportunities to automate the processes for tools that exist and/or could be utilized, and perform a cost/benefit analysis to determine if additional software should be purchased to automate manual processes.	Management agrees with this recommendation and is currently looking into ways to improve this process using existing statewide resources.

Appendix

Impact Criteria

IMPACT CRITERIA					
	FINANCIAL	STRATEGIC/STAKEHOLDER	REPUTATION	COMPLIANCE/ LEGAL / REGULATORY	TRANSACTIONS/ OPERATIONS
HIGH	(1) Asset size (2) Prior negative exposure (3) Rapidly increasing transaction volume	(1) Management and employees affected by process inefficiencies or control breakdowns	(1) Potential adverse issues are known to external parties, such as media and regulatory bodies	(1) Any federal/ state/other action (2) External audit reportable conditions	(1) Current infrastructure cannot support business strategy
MEDIUM	(1) Asset size (2) Major potential cost (3) Transaction volume stable	(1) Management and employees may be affected by process inefficiencies or control breakdowns	(1) Potential adverse issues could impact members	(1) Issues identified by federal/state/ other (2) Issues identified by external audit	(1) Current infrastructure is able to support business strategy with work arounds
LOW	(1) Asset size (2) Minor potential cost (3) Transaction volume stable	(1) No management or employees are affected by process inefficiencies or control breakdowns	(1) Potential adverse issues could impact employees	(1) No issues identified by federal/state/ other (2) No issues identified by external audit	(1) Current infrastructure is able to support business strategy

Vulnerability Criteria

VULNERABILITY CRITERIA							
	CONTROL EFFECTIVENESS	SPEED OF MANAGEMENT RESPONSE	PROCESS COMPLEXITY	HUMAN CAPITAL/ PEOPLE	OPERATIONAL EFFICIENCY	SYSTEM CAPABILITY/ MATURITY	PREVIOUS INCIDENTS/ FINDINGS/ RATE OF CHANGE
HIGH	Controls are not working or do not exist.	No method for anticipating and accessing specific risk events. Issues are not escalated to the appropriate executives effectively.	Manual processes with many data transfer points and owners.	A limited number of staff or current staff has limited competency to manage risk events. Inadequate cross-training exists.	High/unmeasured cost of operations, many quality concerns noted, and unacceptable or unmeasured cycle/process time.	Systems are not operating as designed or design is flawed; very limited controls.	Risk is managed by or directly impacts people, processes, systems, or businesses that have experienced a high rate of change over the last 6 months.
MEDIUM	Controls are detective but not preventative and there may or may not be effective reporting.	A method for anticipating and assessing specific risk events. Issues are not effectively escalated to the appropriate executives.	Automated process encompassing multiple systems and owners.	A limited number of staff and/or staff has moderate competency to manage risk event. Some cross training exists.	Above industry average cost of operation, some quality concerns noted, and below industry average cycle/process time.	Systems are operating as designed, but design can be improved; controls are bolted on top of the system.	Risk is managed by or directly impacts people, processes, systems, or businesses that have experienced a moderate rate of change over the last 6 months.
LOW	Controls are appropriately preventive and detective and there is effective reporting.	A method for anticipating and assessing specific risk events and effectively escalates issues to the appropriate executive.	Automated processes with integrated systems.	Most staff has high competency to manage risk events. Significant cross training exists.	Low/average cost of operations, no quality concerns noted, and cycle/process times within specified standards.	Systems are designed, implemented, and operating effectively; controls are embedded in the system.	Risk is managed by or directly impacts people, processes, systems, or businesses that have experienced a low rate of change over the last 6 months.