VERMONT

DEPARTMENT OF FINANCE AND MANAGEMENT

December 2018 - Internal Control News

The purpose of this quarterly newsletter is to provide departments with articles on good business practices, internal control, and responsibilities. Through articles intended to promote educational and professional development opportunities for employees, this newsletter seeks to raise awareness across state government on the importance of internal control. We hope that by providing this array of information, we can keep you informed of internal control related activities, and help you implement and maintain effective controls in your areas of operations.

http://finance.vermont.gov **Volume 1 Issue 04**

Self-Assessment Internal Control SAIC 2018 Update

In our September quarterly newsletter, we reported that the Department of Finance & Management distributed the 14th Annual SAIC questionnaire to all participating Agencies.

Phase IV: Five Agencies Selected for Review

- The last and final phase of the SAIC review project is the DVR - ***Data Valuation Review***. Five of the Fifty-Six Agencies and Departments were randomly selected for verification of responses from the submitted questionnaires. This was accomplished through the use of the Balancing Mechanism Reporting Agent (BMRA), which randomly selects Agencies based on certain criteria of the questionnaire from the universal pool of all Agencies.
- A detailed SAIC review schedule was developed and all 5 agencies were notified of their selection. Of those selected, the data requested was submitted to F & M by their due dates. The detail review is currently in process. As always, the F & M team appreciates all of the Agencies cooperation during this past year of data collection.

VISION Upgrade 9.2

New and Improved VISION Upgrade coming soon.

VISION Training

- Training classes are being developed for individual module use.
- Updated Manuals and On-line tools will also be available to all Users.

VISION Website Information

- Here is the website that contains important information about the upgrade status. Linkage can be found below:

https://finance.vermont.gov/vision-v9.2-project-home

Delegation of Authority Forms due by January 15th

- In April of 2015, the Secretary of Administration distributed a memorandum regarding the "Delegation of Authority for Signing Documents" as an addendum to Bulletin 3.3: Delegation of Authority. The purpose of the memo was to provide procedures concerning the delegation of authority for signature authorization. Each year, departments must submit an updated and signed copy of the Delegation of Authority form (*located under VISION Security*) to the Department of Finance and Management between January 1st and January 15th. This annual update is required from **every department**, even if there has been no change in the Appointing Authority or their designee(s). Throughout the year, departments need to revise and re-submit the form whenever staff changes occur with the Appointing Authority or their designee(s).

- Please be on the lookout in the new year for the memo from the Secretary of Administration and subsequently send in your form during the submission period. Should you have any questions, please don't hesitate to contact the VISION Support team at: VISION.FinHelpdesk@vermont.gov.

Control Environment (Building Block 1)

This is a **Part 1 of 3 (Part 1 = Control Environment & Risk Assessment) in a series of articles** on the five ***Internal Control Integrated Framework Principles***. Standards include: ***Control Environment, Risk Assessment, Control Activities, Information & Communication, and Monitoring Activities***, which comprises the general framework of an internal control system. Frequently referred to as the "tone at the top", the control environment is the foundation for the other four internal control standards. When management sets a positive tone, leads by example, and cultivates a supportive attitude among its employees then the internal control system is more likely to be strong and effective.

Management establishes and influences the control environment by:

Ethical Values & Integrity

- Provide guidance for proper behavior through policy statements, codes of conduct, and behavior.
- Remove or reduce temptations for unethical behavior and establish methods for reporting ethical violations and consistently enforcing disciplinary practice.

Philosophy & Operating Style

- Acceptance of regulatory control imposed by others and attitude towards accounting and information technology functions.
- Attitude towards internal and external reporting requirements.
- Use of aggressive or conservative accounting principles and support for and responsiveness to internal and external audits and evaluations.

Commitment to Competence

- Hire staff with necessary skills, knowledge, and ensure staff receives adequate training and supervision.
- Provide staff with timely, candid, and constructive performance evaluations.

Structure

- Levels of authority, responsibility, and decision-making are clearly defined for key positions, functions, and Functional sub-units, and relationships are clearly depicted in the organizational structure while understood by all employees.
- Appropriate lines for reporting up-and-down the organizational ladder is established and adhered to policies, procedures, and direct communications ensure employees are aware of their duties, responsibilities, and management's expectations.

Risk Assessment (Building Block 2)

Risk is defined as any event that could jeopardize the achievement of an organization's goals and objectives. Risk assessment is the on-going identification, analysis, and management of risks relevant to the achievement of the organization's goals and objectives. Risks can be both expected and unexpected events from internal and external sources. Internal risk arises from activities within the organization and is usually easier to anticipate and control; examples include technology disruptions, infrastructure malfunctions, changes in key personnel, inadequate or failed processes or systems, fraud, etc. External risk arises from outside the organization and the organization's ability to control or respond to the risk may be constrained; examples include legislative directives, changing public expectations, technological developments, economic changes, social and environmental conditions, natural disasters, fraud, etc.

Key Concepts

- **Start with Goals & Objectives:** Consider the organization's goals and objectives (i.e., what are you trying to accomplish) and then try to identify any risk that could stop or impede the organization from achieving its objectives.

- **Find Root Causes**: Simply identifying "not selling enough widgets" as a risk adds little value to the process, instead focus on the specific causes (e.g., competitor developed a better widget) of not selling enough widgets. Also, do not confuse the impact of a risk with the risk itself; e.g., "losing customers" is not a risk but it may be the impact (or result) to an organization if a risk were to occur.

- **Ineffective Controls are not Inherent Risks**: Identifying ineffective controls or ways that a control may fail is an important process for an organization. Also, assessing control risk is different than identifying the risks that might cause a failure to achieve an objective. For example, if "ineffective training" is a risk, then what's the control to mitigate it – "provide effective training"? **Do Not Ignore Fraud**: The consideration of fraud risk is an important element in the risk assessment process.

Methods to Identify Risks

- Engaging employees at all levels of the organization helps ensure a comprehensive approach. Using question prompts such as the ones below can help frame the discussion and elicit a broad range of responses and some common techniques organizations use to identify risks.

Range of Responses			***Identify Risk Below***
What can go wrong?	How could an employee, vendor or customer commit fraud or steal from us?		Inventory of common events (i.e., what has happened in the past?)
What is the worst thing that has happened?	What assets do we need to protect?		Outline planning or analysis of a process (e.g., staff meetings, project teams)
What is the worst thing that could happen?	What information must we rely on?		Escalation or threshold triggers (e.g., spike in calls to a help desk)
What keeps you awake at night?	Which employees must we rely on?		Targeted meetings, interviews, and exercises (e.g., risk management teams)
What would land us on the TV news or front page of the newspaper?	What activities are regulated or have the greatest legal exposure?		Experience of peers, media reports (i.e., could it happen to us?)

Risk Analysis

- After risks are identified they need be evaluated using a qualitative and quantitative rating system that assesses both the likelihood and impact of the risk. Likelihood is the probability the risk would occur if there were no controls in place. Impact is the measure of magnitude to the organization if the risk were to occur.

Identify Control Activities

- An effective internal control system includes preventive, detective, and monitoring controls designed to confront the risks an organization faces. For each risk, identify the specific control activities the organization is currently utilizing to mitigate the impact and/or likelihood of the risk. Included in this process should be a candid assessment of the actual effectiveness of these control activities (e.g., Are they working as intended? Do employees follow them? etc.)

Risk Response

- After having identified the risks, assessed their impact & likelihood, and evaluated the effectiveness of existing controls, management must then conclude whether the level of risk that remains (i.e., residual risk) is acceptable or not. In deciding its response, management must consider the organization's risk appetite, while evaluating the costs, benefits, and availability of resources to implement additional controls. If existing controls sufficiently mitigate the risk to a tolerable level, then no further action is necessary aside from monitoring for changing conditions or circumstances. If the residual risk that remains is not acceptable, then management should take corrective action.

- Generally, management's response will fall into one of three categories:

  ✓ Mitigate the Risk: Implement new controls or modify existing controls to further prevent or reduce the risk.

  ✓ Accept the Risk: No action taken; the level of residual risk is acceptable, or management has not identified any cost-effective controls to implement to reduce the risk.

  ✓ Avoid the Risk: Eliminate the risk-producing activity or transfer it to another entity (frequently not an option).

F & M Promotion & Retirement:

- Tara Rivet, former VISION Support Specialist II, has resigned from F & M on November 24 to accept a Financial Manager I position with the Treasurer's Office. We wish Tara the best of success.

- Dave Beatty has retired with more than twenty-four years of service to the State, effective November 23, 2018. Dave began work with the State as an Organizations & Operations Analyst in the Agency of Transportation in 1994. Then beginning in 1997, he worked for five years in the Auditor's office before moving on to Finance and Management as a Budget Analyst in 2002. We wish Dave the very best and thank him for his service.

F & M - Internal Control News *is published quarterly by the*

Department of Finance and Management, Statewide Reporting, Internal Control.

Please contact Jeffrey.Montgomery@vermont.gov with comments or suggestions.