VERMONT

VT Dept of Finance & Management
http://finance.vermont.gov/
Volume 4 Issue 4

INTERNAL CONTROL NEWS

DECEMBER 2009

The purpose of this quarterly newsletter is to provide departments with articles on good business practices, internal controls, 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 controls. 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 operation.

Risk Assessment

This is the 3rd in a series of articles on the five internal control standards – **control environment, risk assessment, control activities, communication & information, monitoring -** that comprise the general framework of an internal control system.

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.

Inherent Risks: Focus on those risks that would exist if there were no internal controls in place to prevent or reduce the risk (i.e., uncontrolled environment). Do not eliminate consideration of a risk because of controls that are already in place (e.g., *no one can steal our cash because we lock it in a safe…*the inherent risk is that someone could steal our cash).

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 but 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:

- What can go wrong?
- What is the worst thing that has happened?
- What is the worst thing that could happen?
- What keeps you awake at night?
- What would land us on the TV news or front page of the newspaper?
- Where are we vulnerable?
- How could an employee, vendor or customer commit fraud or steal from us?
- What assets do we need to protect?
- On what information do we most rely?
- On which employees do we most rely?
- What activities are regulated or have the greatest legal exposure?

Some common techniques organizations use to identify risks include:

- Inventory of common events (i.e., what has happened in the past?)
- Routine planning or analysis of a process (e.g., staff meetings, project teams)
- Escalation or threshold triggers (e.g., spike in calls to a help desk)
- Targeted meetings, interviews, and exercises (e.g., risk management teams)
- 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 organizations 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?*)

❖ 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*).

Thanks but No Thanks

Occasionally, particularly during the holiday season, employees make inquiries about the permissibility of accepting gifts from vendors/contractors. The authoritative guidance on this issue is provided by the Dept. of Human Resources' Policy #5.6: Employee Conduct -

Prohibited Conduct

3. Employees are not permitted to solicit or accept any form of compensation from anyone except their employer for activities which are related to their position, unless it is provided for by law or approved by the employer. Prohibited compensation shall include any gift, reward, loan, gratuity or other valuable consideration, including free meals, provided to employees, their immediate family, or business associate(s). Activities related to the position include papers, talks, demonstrations, or appearances connected with the job. However, this prohibition shall not extend to uncompensated activities or compensation received for activities not related to the employees' jobs which are done on their own time.

The most prudent approach is to never accept any type of gift, regardless of value and circumstances. The mere acceptance of a gift could give rise to the appearance of a conflict of interest with the department/employee's official public duties. But sometimes, especially during the holiday season, a "department" receives an unsolicited gift from a vendor. In such cases, and provided the gift is of nominal value, the department head has the decision-making authority to accept the gift or return it. If returning the gift is impractical, the department may decide upon an acceptable alternative such as donating the gift to a local food-shelf or non-profit organization; if doing so, the department should inform the vendor that State policy prohibits accepting gifts and where the donation was made.

Contingency Planning for Mission Essential Functions

As a reminder, please make sure that your risk planning for this flu season includes coverage for the following mission essential functions related to Finance & Management:

- Payroll processing: Employee actions must be processed on time so that employees are paid timely and accurately. Timesheets and Paradox time files must be completed and submitted on time to ensure that employees are paid. Deadlines are posted on the Pay Periods page in the Payroll section of the Finance & Management website. As a reminder, for each pay period, each computer can be used for only one pay group. Please make sure that backup timekeepers have training material and access to Paradox for the specific pay group.
- Payments to vendors: Please make sure that contractual and statutory payments will be made timely and accurately. Ensure that primary and backup users have the correct security to perform necessary duties. For assistance, please refer to the VISION training material on the Finance & Management website or contact the VISION Finance Support Team.
- Bank deposits: Deposits should be entered in VISION within 24 hours of being deposited at the bank. Similarly, deposits should be at the bank consistent with internal control best practices. Ensure that primary and backup users have the correct security to perform necessary duties. For assistance, please refer to the VISION training material on the Finance & Management website or contact the VISION Finance Support Team.
- For those departments who have systems that interface into VISION: Please ensure that your files – those sent and received – are processed in accordance with your deadlines. As a reminder, for those receiving files after an interface cycle, these files are overwritten by the next cycle.

"I Forgot My Password"
Functionality Coming to VISION Financials!

The VISION Finance Support Team and ERP Technical Team are finishing up the work required to provide VISION users with "I Forgot My Password" online help. Once this feature is in Production, users will be able to get password help without having to call or email the VISION Finance Support Team (provided that their VISION accounts have not been locked.)

This functionality works the same way as the "I Forgot My Password" link on the Employee Self-Service login page. In order to use this online help feature, VISION users will need to confirm their email address and set-up their challenge question on the "My System Profile" page. As we get closer to providing this feature in Production, the support team will be letting all users know of this change and will be posting support material to the Finance & Management website.

Operational Guidance - FAQ

Question: An employee has requested to be reimbursed for damage/loss of personal property that occurred while at work. Are such claims allowable and, if so, what are the requirements?

Answer: The specific authorization governing such claims is provided by statute, Title 32 §932a: Administrative Reimbursement for Property Damages. Generally, these types of claims **may** be approved and paid by the employee's department; if the department does not approve the request, the employee may file a claim in small claims court. The relevant sections of the statute are:

(a) In lieu of proceeding under section 932 of this title, a state employee who has a claim against the state for property damages may elect to file a claim under this section, provided the claim does not exceed $1,000.00.

(b) The claim shall be:
  (1) made in writing, under oath, stating the facts relating to the claim;
  (2) filed with the agency, department, or other state entity which employs the claimant; and
  (3) filed within one year after the date the claim accrued.

(c) The state entity with which the claim is filed may approve payment of a claim against the state for property damages sustained by the employee and payment of the claim shall be charged against that entity's departmental appropriation.

(d) If a claim is approved under this section, the commissioner of finance and management shall issue his or her warrant for the amount of the award, the acceptance of which shall be a full discharge of all claims against the state arising out of the matters involved therein. If the claim is disapproved, the person may proceed to file the claim under section 932 of this title.

In addition, the Dept. of Buildings & General Services' Security Division requests that departments report these type of events to BGS by completing an Incident Report form; this form includes several incident types related to "personal property" (re: damaged, lost, missing, stolen, etc.)

Staff Happenings

- The **Payroll Division** has moved to the 3rd floor of the Pavilion Building at 109 State Street, all staff phone numbers and email addresses remain the same.
- **Mary Andes**, former Budget Analyst, is now the Director of Data Analysis & Reimbursement at the VT Office of Health Access.

Internal Control News is published quarterly by the Dept of Finance & Management. Please contact Kevin Gilman with comments or suggestions.