❖ INTERNAL CONTROLS

→ For more information, refer to **Internal Control Standards – Guide for Managers**
http://finance.vermont.gov/policies-and-procedures/internal-controls

✓ What is Internal Control?

Internal control is the integration of the activities, plans, attitudes, policies, and efforts of the people of an organization working together to provide reasonable assurance that the organization will achieve its mission.

More simply- Internal controls are what an organization does to see that the things they want to happen **will** happen and the things they don't want to happen **won't** happen.

✓ Why Internal Controls?

An effective internal control system helps an organization to:

- Promote orderly, economical, efficient and effective operations.
- Produce quality products and services consistent with the organization's mission.
- Safeguard resources against loss due to waste, abuse, mismanagement, errors and fraud.
- Promote adherence to statutes, regulations, bulletins and procedures.
- Develop and maintain reliable financial and management data, and accurately report that data in a timely manner.

✓ Internal Control Framework

Five inter-related components that apply to all aspects (administrative, financial and programmatic) of an organization's operations:
Control Environment - **Risk Assessment** - **Control Activities** - **Communication & Information** - **Monitoring**

✓ Who's Responsible?

Internal controls are the responsibility of all employees but the greatest responsibility resides with management for establishing and monitoring the organization's internal control system.

✓ Tone at the Top

Executive management needs to set the organization's direction regarding internal control. If executive management does not establish strong, clearly stated support for internal control, the organization as a whole will most likely not practice good internal control.

✓ Risk Assessment

Simply put a **risk** is anything that could happen to threaten the achievement of goals & objectives.

- **Identify:** Process owners and subject matter experts identify (*brainstorm*) what could possibly go wrong within their operations (breakdowns, fraud, material errors, what keeps you awake at night, single point of failure, past experience, natural disasters, etc). In attempting to identify fraud risks it's often necessary to "**think like a thief**".

- **Analyze:** Assess the risk in terms of **likelihood** (*what are the chances it will happen?*) and **impact** (*what are the ramifications if it does happen?*)...*impact* may be measured in various terms such as health & safety, financial, reputation, legal, disruption to operations, etc.
- **Manage:** Evaluate whether the internal controls already in place adequately address the risk or if not what controls or business process changes must be implemented to reduce the risk. The level of controls necessary should be directly related to the likelihood and impact of the risk.

Two circumstances that typically represent increased risk and deserving of more attention:

- **Change**- Changes in technology, regulatory environment, key personnel, organizational structure, rapid growth or expansion of operations, etc. expose an organization to increased risk.
- **Inherent Risk**- Certain activities or situations such as the presence of cash, high-degree of complexity, prior history of internal control weaknesses, beneficiaries with cash or cash equivalent benefits from State programs, de-centralized operations, etc. have an inherently greater potential for fraud, waste, asset misappropriation, unauthorized use, regulatory non-compliance, etc.

✓ Control Activities

Control activities are what most people generally associate with the term "internal controls".

- **Preventative Controls** (i.e., prevent or deter a 'risk' from occurring): Documented policies & procedures, separation of duties, approvals & authorizations, physical security over assets, supervision, system passwords, safety clothing & equipment, anti-virus software, cross-training, continuity of operations plan, reference & background checks, etc.
- **Detective Controls** (i.e., detect an undesirable event after-the-fact, or as it occurs, enabling prompt corrective action): Reconciliations, verifications, financial monitoring, audits & inspections, rotate job duties, anonymous tip lines, performance evaluations, physical inventory counts, security alarms & cameras, smoke detectors, etc.

✓ Monitor It

Organizations must routinely monitor (formally and informally) their internal control system to ensure it is operating as intended. This is a responsibility of each organization, not external auditors. **"Trust but verify."**

✓ Reasonable Assurance

No matter how well designed and operated, internal controls provide only reasonable assurance regarding the achievement of objectives. All internal control systems are limited by the realities of human frailty in decision-making and the potential failure to anticipate certain risks. Attempting to achieve *absolute assurance* would most likely be cost prohibitive (cost vs. benefit) and/or result in inefficient operations.

✓ Absence of Failure

Benefit of internal control is difficult to quantify because the measure of its success is the absence of failure. For example, organizations must resist the inclination of "nothing is ever wrong so why do we keep doing *it"*….since it's very possible that the reason nothing has gone wrong is because you ARE doing *it*.

SELF-ASSESSMENT of INTERNAL CONTROL

✓ What is Self-Assessment?

Management tool used to assure key stakeholders, both internal and external, that an organization's internal control system is reliable. In certifying the self-assessment, the appointing authority is attesting to the status of their organization's internal control system.

✓ Tone at the Top

To be most effective, the self-assessment process must extend outside the walls of the business office. While financial managers are most often the point person, send a clear message that demonstrates your support of the process and the clearly expected cooperation and engagement of all staff.

✓ Why Self-Assessment?

- Greatest intended benefit is to the individual organizations by providing a framework to evaluate their internal control system.
- Requires the involvement of management & staff (i.e. the process owners) in the assessment of risks and internal controls relating to the operations within which they work.
- An effective self-assessment process will involve communications between financial staff, program staff and management, providing greater assurance to both senior management and external auditors that the organization's internal controls are operating effectively.
- Method to evaluate and document business practices and serves as a primary filter through which senior management can make informed decisions (e.g., *where do we need to improve?*).
- Expectation is that most employees want to do the right thing and perform well in their jobs…the self-assessment provides a collection ("one-stop-shopping") of the various financial related policies, best practices and control activities to assist employees and organizations.
- The importance or relevancy of specific controls can vary by organization, requiring professional judgment to know when it's necessary to expand upon those areas where greater risk exists.
- The level of effort that an organization puts into completing the self-assessment is directly related to the benefit derived from it. **"You get out of it, what you put into it."**
- Positive influence on the control environment; as staff buys into the process, control consciousness increases and when employees become more attuned to internal controls they begin identifying and correcting issues and deficiencies as they occur. Encourage completion of the self-assessment as a group exercise.
- Deliberate, documented and iterative process that functions as an incentive for continuous improvement.

❖ FRAUD PREVENTION

→ For F&M Newsletter articles on Fraud go to: http://finance.vermont.gov/reports-and-publications/internal-control-newsletters/article-index#fraud

✓ **Tone at the Top:** Establish a clear message that fraud, waste and abuse will not be tolerated, nor will any attempt to conceal fraudulent activity.

✓ **Reduce the Opportunity:** In nearly all fraud cases these 3 elements ("fraud triangle") are present:
1. Pressure - A motivation (typically economic) that prompts an individual to consider an illegal act;
2. Rationalization - Frame of mind that allows the individual to justify their dishonest actions;
3. Opportunity - Circumstances within an organization that enable an individual to perpetrate a fraud (generally through weak internal controls).

The only element of the triangle that organizations have significant influence over is through strong internal controls that minimize an individual's **opportunity** (re: preventative controls) to commit and conceal fraud.

✓ **Perception of Detection:** Let employees know that someone is watching them…those who perceive they will be caught engaging in fraud or other inappropriate acts are less likely to commit them. Foster an environment in which employees expect that dishonest acts will be detected by management, monitoring techniques, other employees, or the auditors.

✓ **Separation of Duties:** This is the most important control activity for minimizing the risk of fraud and the concealment of errors. Ensure no single employee controls all key aspects of a transaction or event; ideally no one person should be able to initiate, authorize, record and reconcile a single transaction. With proper separation of duties it is expected that at least one individual involved in the process will identify and/or prevent a transaction processing error, misappropriation or fraud from occurring. Examples of duties to be performed by different employees:

- **Cash Receipts:** Receiving the Cash – Processing the Deposit – Posting to the Accounting Records
- **Purchasing:** Initiate the Requisition – Authorize the Purchase – Receive the Goods – Process Payment
- **Fixed Assets:** Asset Custodian – Performing Physical Inventory – Maintenance of Accounting Records

✓ **Professional Skepticism:** A healthy dose of professional skepticism (i.e., a questioning mind, critically evaluating, not accepting at face value) can be an effective fraud deterrent…ask tough questions, request additional back-up or explanations, challenge why something was done (or not done), perform surprise audits/inspections, etc.

✓ **Red Flags:** Red flags are warning signs (*prove nothing)* that could indicate something is wrong, warranting further investigation, observation, etc.

- **Behavioral Red Flags:** Defensive to reasonable questions from managers or auditors, refusal to take vacations or accept promotions, reluctance to share workload or provide specific details on job duties, "new found" wealth, erratic behavior, substantial personal financial pressures, etc.

✓ **Fraud Happens:** Managers must acknowledge (i.e., belief & awareness) that fraud can occur and is most often committed by those in positions of trust; denial and willful blindness are often contributing factors in significant fraud cases. **"Trust is an emotion, not a control."**