

# Fraud Awareness Training

## Internal Control Cheat Sheet

Control Activities assist with prevention, detection, and mitigation of risks – including the risk of fraud – that can impede organizational objectives. Management is responsible for implementing and modifying control activities in their areas of authority. The table below presents some of the most common control activities, some – but not all – risks that these activities mitigate, and tips for effective implementing each control activity.

CONTROL ACTIVITY	MITIGATED RISKS	IMPLEMENTATION TIPS
<p><b>Competent Staff</b>  <i>Ensure employees are qualified to complete job duties effectively.</i></p>	<ul style="list-style-type: none"> <li>• Mishandling of tasks and job duties.</li> <li>• Unrecognized vulnerabilities overlooked during the course of daily business operations.</li> <li>• Unproductive organizational results.</li> </ul>	<ul style="list-style-type: none"> <li>• Properly evaluate job applicants during hiring process.</li> <li>• Provide adequate training to staff to ensure the team has the required knowledge, skills, &amp; abilities.</li> <li>• Document and track employee training completion.</li> <li>• Create and update standard operating procedures to guide employees when completing their duties.</li> <li>• Ensure staff are familiar with and can access organizational policies and procedures.</li> </ul>
<p><b>Employee Supervision</b>  <i>Ensure employees have direction to complete job duties and performance is monitored.</i></p>	<ul style="list-style-type: none"> <li>• Negative work environment.</li> <li>• Overworked, stressed employees.</li> <li>• Reduce risk related to poor quality projects or services.</li> <li>• Delayed and/or over-budget projects.</li> <li>• Lack of accountability.</li> </ul>	<ul style="list-style-type: none"> <li>• Establish employee accountability measures for recognized errors.</li> <li>• Schedule periodic meetings to discuss status, workload, and budget.</li> <li>• Track achievements &amp; goals and provide constructive feedback.</li> <li>• Compare actual performance to planned or expected results throughout the organization and analyze significant differences.</li> </ul>

### Segregation of Duties

*Ensure one employee is not responsible for incompatible parts of a process.*

- Risk of error, inappropriate transactions, stolen funds, or fraud related to processing and executing individual tasks (i.e. accepting cash & preparing deposits).
- Lack of accountability for identified irregularities.
- Mismanagement of critical departmental functions.
- Designate different employees for authorizing, recording, reviewing, and handling any assets related to a transaction.
- Maintain documented procedures detailing each employee's responsibilities.
- Review operations periodically to ensure employees do not have inappropriate tasks.
- Avoid making processes person specific.

### Authorization & Approvals

*Ensure transactions and business activities are properly authorized & approved before they occur.*

- Purchases and decisions made without appropriate supervisor knowledge.
- Occurrence of invalid transactions and activities.
- Business activities that do not adhere to organizational guidelines and objectives.
- Clearly designate which individuals are responsible for approving transactions and their scope of authority (i.e. dollar amount, area or responsibility).
- Maintain records documenting that an activity has been seen, reviewed, and approved by appropriate authority before being processed.

### Support Documentation

*Ensure explanations for transactions or internal services are created and retained.*

- Personal purchases made by employees with City funds.
- Unauthorized or unapproved purchases of goods and services.
- Lack of internal record for transactions and activities.
- Inappropriate reconciliation process.
- Verify that transactions or internal services are for a business purpose.
- Verify that transactions have itemized invoices or receipts that match the transaction.
- Create standard forms or processes to document internal service requests, approvals, or results (e.g. work orders, pick tickets).
- Retain documentation in designated, common repositories (i.e. avoid storing documentation on individual drives, desktops, or email inboxes).

### Access Controls

*Ensure employees' physical and electronic access are appropriate for job duties.*

- Unauthorized access to data and information.
- Reduction of cyber-attack impact in the event an employee credentials are hacked.
- Physical or electronic security breaches.
- Restrict employee access to only activities, applications, or areas needed for their job duties.
- Require dual authentication for access to vulnerable assets.
- Periodically review employee access rights.



### **Inventory Management**

*Ensure City assets are adequately tracked and monitored.*

- Revenue loss due to missing assets.
- Mismanagement and misrepresentation of the quantity and value of City assets.
- Duplicate purchases of assets already acquired.
- Stolen, wasted, or misused assets.
- Limit access to assets to only employees who need it.
- Record assets in use and clearly mark who is responsible for them.
- Periodically check that assets are where they are supposed to be.
- Have clear processes for documenting and approving the disposal of assets.

### **Delivery Confirmation**

*Ensure City-purchased goods and services are received by the City.*

- Payment to vendors for goods or services not provided or for fake invoices.
- Inappropriate or personal purchases go undetected.
- Lost deliveries.
- Restrict delivery of goods or services to only City-addresses.
- Require proof of delivery from the vendor (e.g. receipt, bill of lading – not an invoice).
- Ensure delivered goods match what was ordered upon receipt (i.e. quantity, type).

---

### **Select Policy References:**

The following policies have been referenced here to provide supervisors and managers with additional information about some of the City's internal controls formalized by policy.

- Ethics Policy ([Policy No. 10.00](#));
- Cash Handling Regulations ([Policy No. 403.01](#));
- Warehouse and Central Stores Operations ([Policy No. 407.06](#));
- Centralized Purchasing ([Policy No. 407.10](#)) and [Procurement Policy Manual](#);
- Travel Expenses ([Policy No. 408.01](#));
- Identification Cards / Fobs ([Policy No. 502.03](#));
- User Authorization, Identification and Accountability ([Policy No. 506.02](#)); and
- Fraud Response ([Policy No. 509.01](#)).