CLARK SCHAEFER HACKETT
BUSINESS ADVISORS

Internal Controls/Fraud Prevention

Introduction: Amr Elaskary, CPA, CFE

- Amr Elaskary, CPA, CFE, is a University of Toledo graduate with a Bachelor's Degree and a Master's Degree in Accountancy and Finance.
- Amr leads audit engagements under yellow books and single audit requirements for government agencies for nine years.
- In addition, Amr is a Certified Fraud Examiner. As such, he works with clients to extract and analyze data using his knowledge and expertise to detect or prevent fraud.
- Amr has extensive experience in providing actionable recommendations to his clients to help them improve the efficiency and effectiveness of internal controls.
- Amr is a graduate of the AICPA Leadership Academy

Introduction: Cody Mitchell, CPA

- Cody graduated from University of Toledo and joined CSH in September 2018.
- Cody is an audit Senior and serve in the government services Committee at CSH.
- Cody specializes in yellow book and single audits engagement.
- Cody focuses his time on providing quality audit deliverables to clients; supervising interns and staff; and communicating with clients to answer their questions in a timely fashion.
- Cody is Certified Single audit expert by AICPA.

- We brought you a funny video about fraud to start

- There were no funny videos about fraud
- We looked all over the internet

Introduction

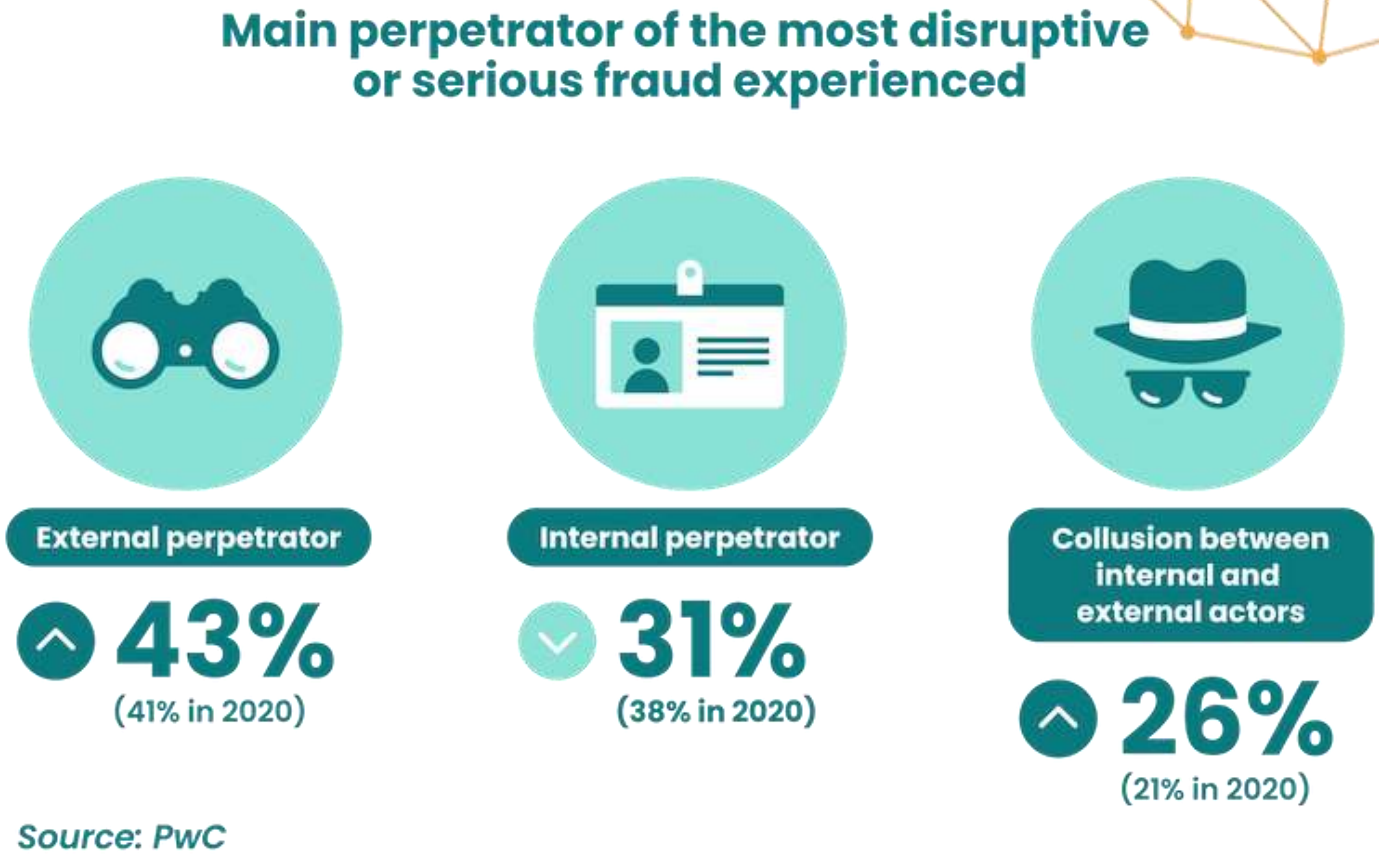
- Fraud cost billions of dollars in damages every year.
- Fraud can be perpetrated by internal and external parties.
- Strong internal controls deter fraud.
- Fraud has many additional costs (see next slide).

Additional Cost of Fraud

- Damage to reputation.
- Lowered employee morale.
- Increased layoffs and cuts.

Who Commits Fraud

- Internal 31%:
  - Employees
  - Board/management
- External 43%:
  - Scammers
- Collusion 26%



Examples of Internal Fraud

- Stealing money
- Stealing inventory
- Fraudulent time
- Fraudulent expense reports
- Adding fake employees
- Adding fake vendors

Examples of External Fraud

- Telephone/ email asks for fraudulent wire payment.
- Telephone/ email asks for fraudulent change in bank account info.
- Ransomware/hack.
- Cryptocurrency fraud.

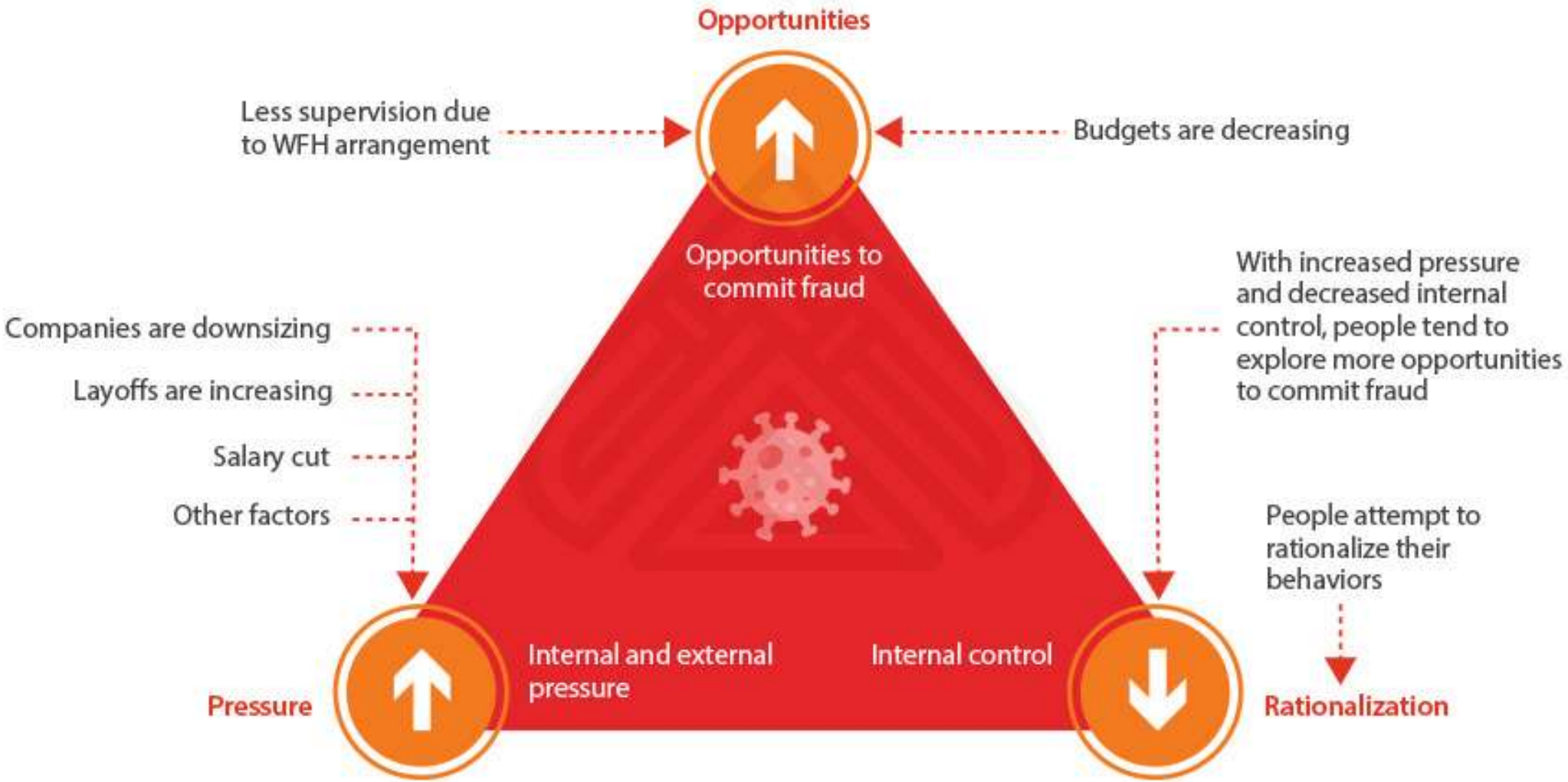
- https://www.youtube.com/watch?v=51dNRSyGpMY

Internal vs. External Fraud

Internal		External
Employee	**Management**	
Stock theft	Lapping	Check forgery
Misappropriation of cash assets	Expense accounts	False insurance claims
Lapping	False financial statements	Credit card fraud
Check forgery	Misappropriation of cash/assets	False invoices
Expense accounts	Unnecessary purchases	Product substitution


COVID-19
AND THE
FRAUD
TRIANGLE

Fraud Triangle in the Context of COVID-19



Graphic© Asia Briefing Ltd.

Pressure

- To support a habit.
- To pay for personal debts.
- To cover for a significant financial loss.
- Pressure to succeed.

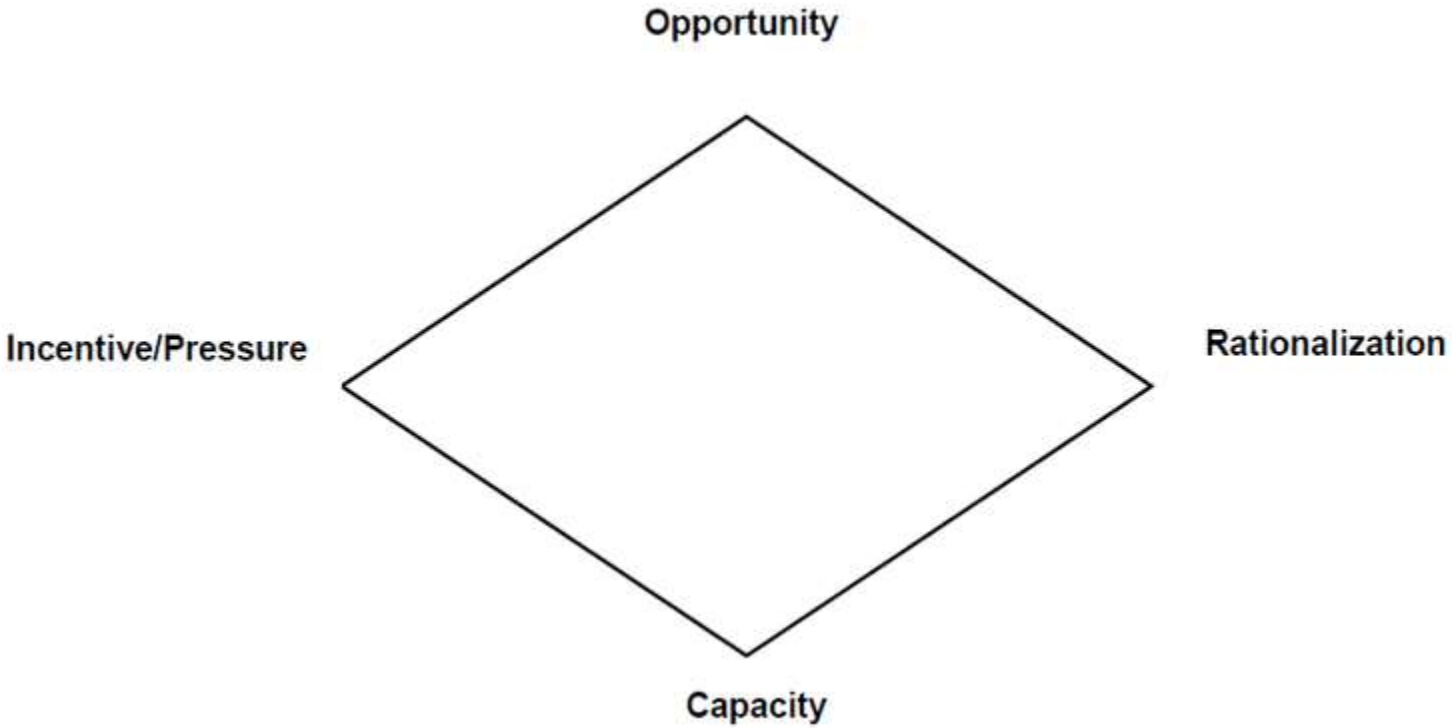
Opportunity

- Poor internal controls.
- Lack of disciplinary action for prior frauds.
- Extreme trust in one individual.

Rationalization

- Only “borrowing” the money and would repay later.
- The company won’t even know this amount is gone because it is not that much.
- I deserve this after the way the organization treated me.
- I’ve been working with this company for 15 years. They owe it to me.

Fraud Diamond



Capacity

- Must have the skills and ability.
- Must recognize the opportunity.
- Must be able to execute the scheme.

Capacity Factors

- Position or responsibilities.
- Expertise and experience.
- Self-Confidence.
- Can coerce others to participate or remain silent.
- Ability to lie fluently and convincingly.
- Can handle stress.

Warning Signs of Fraud


#YOUNGERTV
IT'S FRAUD

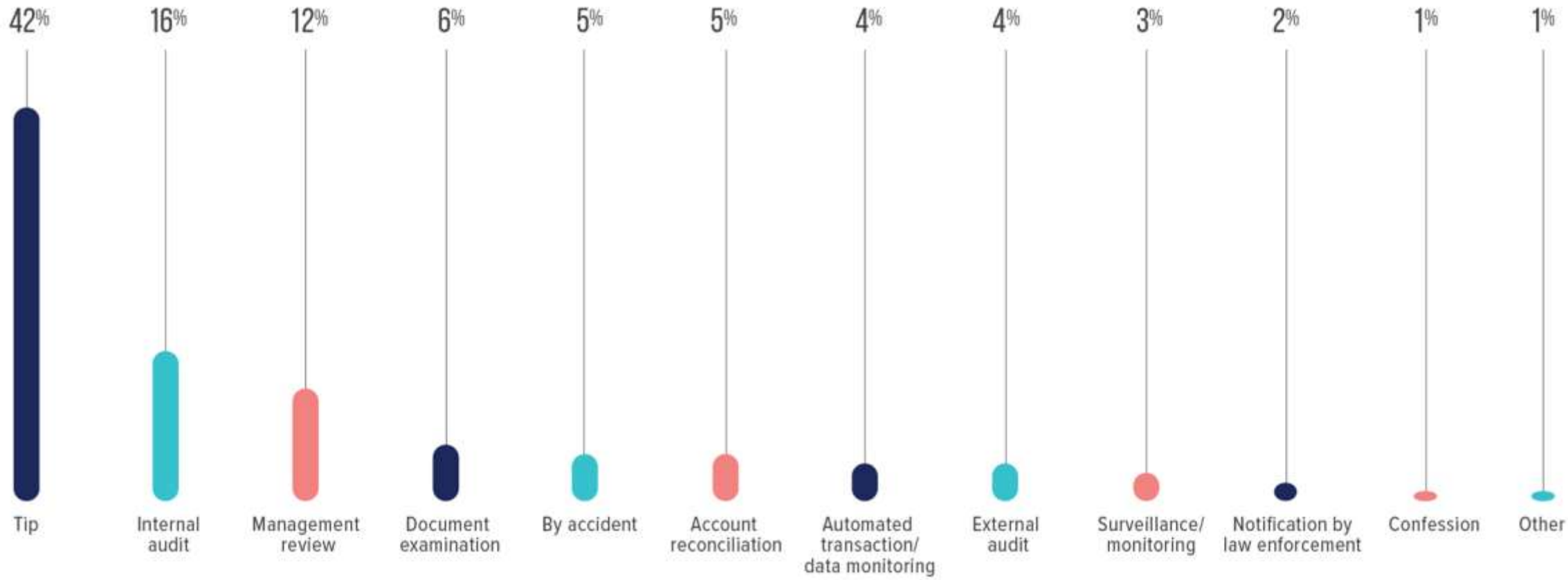
Why Internal Controls are Important

- Safeguard assets.
- Effective and efficient operations.
- Reliable financial reporting.
- Compliance with laws and regulations.

Typical Anti-Fraud Controls by Size of Victim

How do you think fraud is detected?

How is Fraud Initially Detected



COSO Cube


STRATEGIC
OPERATIONS
REPORTING
COMPLIANCE
Internal Environment
Objective Setting
Event Identification
Risk Assessment
Risk Response
Control Activities
Information & Communication
Monitoring

What is the Green Book and how is it used?

Important facts and concepts related to the Green Book and internal control

Internal control and the Green Book

What is internal control?

Internal control is a process used by management to help an entity achieve its objectives.

How does internal control work?

Internal control helps an entity

- Run its operations efficiently and effectively
- Report reliable information about its operations
- Comply with applicable laws and regulations

How is the Green Book related to internal control?

Standards for Internal Control in the Federal Government, known as the Green Book, sets internal control standards for federal entities.

How does an entity use the Green Book?

An entity uses the Green Book to design, implement, and operate internal controls to achieve its objectives related to operations, reporting, and compliance.

Who would use the Green Book?

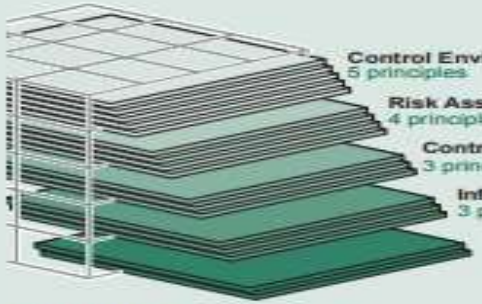
- A program manager at a federal agency
- Inspector general staff conducting a financial or performance audit
- An independent public accountant conducting an audit of expenditures of federal dollars to state agencies
- A compliance officer responsible for making sure that personnel have completed required training

The cube

The standards in the Green Book are organized by the five components of internal control shown in the cube below. The five components apply to staff at all organizational levels and to all categories of objectives.

Principles

Each of the five components of internal control contains several principles. Principles are the requirements of each component.



Attributes

Each principle has important characteristics, called attributes, which explain principles in greater detail.

Page structure

Green Book pages show components, principles, and attributes.

Control Environment

- Set a positive tone at the top.
- Influence on the decisions and activities of the organization.
- Includes the integrity, ethical values, and competence of employees as well as management's philosophy and operating style.

Risk Assessment

- The process of identifying, evaluating, and deciding how to manage risks.

- Questions to ask during risk assessment:
  - What is the likelihood of occurrence?
  - What would be the impact if it occurs?
  - What can we do to prevent or reduce the risk?

Control Activities

- Policies, procedures, and processes that are designed and implemented to help ensure that management directives are carried out.
- Help prevent or reduce the risks.
- Throughout the organization at all levels and in all functions
- Includes approvals, authorizations, verifications, reconciliations, security of assets, reviews of operating performance, and segregation of duties.

Communication and Information

- Information must be captured and communicated on a timely basis.
- Effective systems enable employees to exchange the information needed to conduct, manage, and control its operations.

Monitoring

- Internal controls must be monitored to assess if they are operating as intended.
- Continuous monitoring is necessary to react to changing conditions, so controls do not become outdated or obsolete.
- Should occur during everyday operations.

Controls in Everyday Life

- Lock your house.
- Balance your checkbook.
- Keep copies of important documents.
- Change passwords

Examples of Common Controls

- Segregation of duties.
- Documentation.
- Authorization and approvals.
- Security of assets.
- Reconciliation and review.

Segregation of Duties

- Divide responsibilities between different employees so one individual does not control all aspects of a transaction.

- This reduces the opportunity for an employee to commit and conceal errors or perpetrate fraud.

Documentation

- Policies and procedures set forth the fundamental principles and methods that employees rely on to do their jobs.
- Enables a transaction to be traced from its inception to completion.
- Evidence to substantiate critical decisions and significant events.

Authorization and Approvals

- Document and communicate which activities require approval based on the level of risk to the organization.
- Should only be approved by employees acting within the scope of their authority granted by management.

Security of Assets

- Secure and restrict access to equipment, cash, inventory, confidential information, etc. to reduce the risk of loss or unauthorized use.
- Perform periodic physical inventories.
- Base the level of security on the vulnerability of items being secured, the likelihood of loss, and the potential impact should a loss occur.

Reconciliation and Review

- Examine transactions, information, and events to verify accuracy, completeness, appropriateness, and compliance.
- Base the level of review on materiality, risk, and overall importance to the organization.
- Ensure reconciliation and review is frequent enough to detect and act upon questionable activities in a timely manner.


EXCELLENT
WORK!

Preventive or Detective

- Preventive – Stop an unwanted outcome before it happens.

- Detective – Find the problem before it grows.

Examples - Preventive

- Computer passwords to stop unauthorized access.
- Review and approval process for purchase orders or requisitions to ensure they are appropriate before the purchase.
- Reading and understanding policies and procedures to learn the right way to do something.

Examples - Detective

- Cash counts and bank reconciliations.
- Reviewing payroll reports.
- Inventory counts.
- Monitoring expenditures against budgeted amounts.

What to do if You Suspect Fraud

- Be aware of the warning signs.
- Report if you are ever asked to do anything illegal or unethical.
- Report if you suspect someone no matter the tittle.

Next Steps

- Be an anti-fraud solider
- Review processes
- Start the communication
- Talk with your auditor
- Set the tone at the top

CLARK SCHAEFER HACKETT
BUSINESS ADVISORS

QUESTIONS?

Amr Elaskary
Senior Manager
419.690.9090
aselaskary@cshco.com

Cody Mitchell
Senior
740.513.8971
cmmitchell@cshco.com