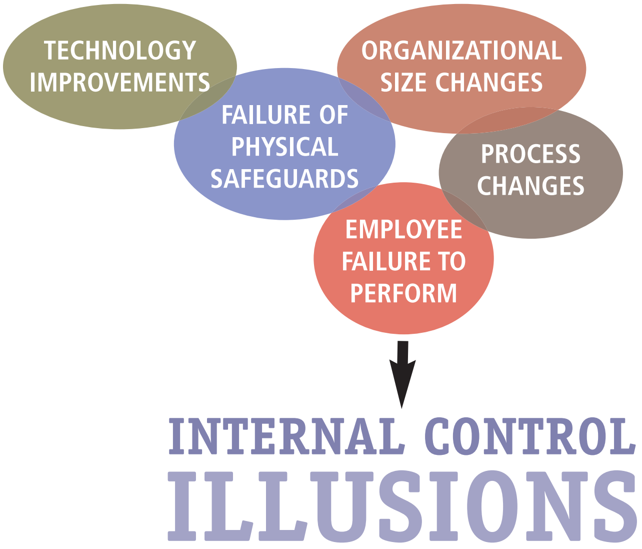
THE ILLUSION OF INTERNAL CONTROLS

By Bill Atwood, CFE, CFF, CPA; Cecily A. Raiborn, CMA, CPA, CFE; and Janet B. Butler, CITP, CGMA

Internal controls (ICs) are the backbone of any thriving, dynamic organization. Chiefly they ensure financial reporting reliability, operational effectiveness and efficiency, and legal/regulatory compliance. Though essential to preventing and detecting internal fraud, ICs are often allowed to deteriorate over time or simply become ineffective because of organizational changes. Either situation generates the perception of internal control protection that, in fact, is an illusion. These illusions can create trouble for management accountants and other financial professionals who must rely on the internal controls system to protect assets, ensure the integrity of financial information, and prevent and detect fraud.

Unless the weaknesses in the IC system are corrected, accountants will perceive that the system is performing as originally intended. Five primary contributors to internal control illusions are organizational size changes, technology improvements, process changes, failure of physical safeguards, and employee failure to perform (Figure 1). Let's examine each of these in more detail.

Figure 1: Primary Contributors to Internal Control Illusions


TECHNOLOGY IMPROVEMENTS
ORGANIZATIONAL SIZE CHANGES
FAILURE OF PHYSICAL SAFEGUARDS
PROCESS CHANGES
EMPLOYEE FAILURE TO PERFORM
INTERNAL CONTROL ILLUSIONS

Organizational Size Changes

Though growth is a positive factor in an organization, it may create problems in a previously effective control system and often generates a need to implement previously unnecessary internal controls. For example, as an organization grows, duties formerly handled by an owner/manager will need to be assigned to other people. The new distribution of duties demands IC adjustments, such as a need for authorization controls, surety bonds, and proper documentation of essential policies and processes. Additionally, restrictions will likely need to be placed on employee access to information. Responsibility for IC compliance may begin to span multiple departments, frequently creating organizational silos and limiting communication. Some internal controls may become illusionary solely based on an "it's the other guy's responsibility" attitude.

If mergers or acquisitions occur, dissimilarities between the different companies' information technology (IT) and IC systems can give rise to internal control illusions. Legacy systems of the companies involved in the transaction may be duplicative, contradictory, or insufficient, causing the ICs to be unreliable or missing entirely. It's common for legacy systems to have been "tweaked" over the years to adapt to the installing company's specific circumstances. As such, even what superficially appears as the same system in two companies might in actuality be two very different systems—with ICs that cancel out each other's effectiveness and leave gaps that provide an opportunity for waste, abuse, or fraud.

An early example of integration problems occurred when USA Waste Inc. acquired Waste Management Corp. in 1998. Neither company's IT system could handle service for the combined organization, and it took almost two years after the acquisition for the expected efficiencies to occur. Even worse, it took JPMorgan about 17 years to fully merge computer operations after purchasing Texas Commerce Bancshares in 1988.

In today's belt-tightening business environment, segregation of duties is often negatively impacted when an organization downsizes and fewer employees assume responsibility for work previously shared among many. In the aftermath of a workforce reduction, management focuses on getting organizational activities accomplished with fewer employees—and it often becomes "easier" to have one person assume responsibility for an entire process, leaving the incompatibility of functions to go unrecognized or ignored, even by the internal accountant or the external auditor. Furthermore, with fewer workers trying to do more in the same amount of time, job descriptions aren't always updated. Though a casual look at such descriptions may lead someone to assume that all duties are adequately segregated, only observation and/or employee interviews will reveal the new process structure and which controls are no longer effective.

Technology Improvements

Multiple controls, such as passwords and time limits on program access, are commonly employed over IT systems. Because such controls have been established and documented, accountants often believe that the controls are being followed and the systems are adequately

Table 1: Examples of Technology Conditions Creating Internal Control Illusions

ILLUSIONARY CONTROL	REALITY
Require computer passwords	Passwords are given to colleagues.
	Password list is in an easily accessible place (such as desk drawer).
Require password changes	Password changes are allowed to be minimal (for example, from XXX1 to XXX2).
	Password change requirements are not enforced.
Require off-site backup	Backup information has never been tested for actual restoration of data.
	Backup is performed on the same schedule (for example, daily or weekly) as prior to going paperless, leaving time gaps in data until the next backup.
	Off-site choice for backup is flawed because it could be affected by similar natural disasters.
Document computer changes and upgrades	System changes and upgrades fail to be documented, creating gaps in the ICs.
Train person on new technology	A "monopoly of knowledge" is created, making a single individual indispensable.
Install encryption system for network	Upgrades are not implemented when security systems advance, leaving the system vulnerable to hacking.
Allow sensitive data access only at specific workstations	Downloading of information onto flash drives (or other similar technology) isn't precluded.

secured. Table 1, however, shows several types of IC illusions related to common technology controls.

Encrypted wireless network systems may be instituted and then not upgraded as security standards advance—leaving the IC system vulnerable. Wi-Fi networks may be left unsecured. Control gaps may lead to organizational data breaches or releases by insiders or external parties (often through hacking) of supposedly secure or sensitive information, such as that related to employees, customers, intellectual property, or product innovations. Breaches may also occur because of basic technology advances. Flash drives, cell phones, and micro-SD cards radically altered the quantity of and time in which proprietary data could be misused or stolen. Unfortunately, accountants may not be fully aware of the challenges created or risks posed by new technology, so they don't address possible IC lapses.

New technology also provides the opportunity for a "technology guru" to develop a "monopoly of knowledge." If only one employee has the knowledge (and, perhaps, the ability to access and use a system), that individual has the opportunity to manipulate the technology and circumvent any internal controls related to it without detection. Yet even if this person is completely trustworthy, the company is also vulnerable if he or she becomes ill or leaves the firm. To the extent possible, technological knowledge should be distributed among everyone who will use or rely on that technology. Accountants should coordinate with the IT department to understand who comprises the foundation of the organizational technology base(s) so that proper offsetting ICs can be implemented.

Process Changes

Over time, organizations typically change the manner in which activities are performed, possibly to reflect employee learning curves, implementation of Just-in-Time inventory or purchasing techniques, single-source procurement, modified value chains, quality control improvements, or outsourcing. Each process change will influence the appropriateness of the internal controls applicable to the assets, policies, and procedures contained within the affected area. Believing that old internal controls will naturally be effective with new processes is an illusion as unwise as the belief that progress will stop if it's simply ignored. More than 400 years ago, philosopher and author Sir Francis Bacon said, "He that will not apply new remedies must expect new evils." In the case of internal controls, those evils will present themselves in the form of organizational fraud, waste, and abuse unless accountants engage in analyzing how the process changes have affected the controls.

Failure of Physical Safeguards

Physical safeguards minimize access to valuable and vulnerable assets, but they're worthless if they aren't employed properly. Locks are left unlocked, or keys are left in easy-to-find places. Video cameras are turned off or left unobserved. Employees can call up documents that should be accessible only to upper management.

An easily overlooked physical safeguard occurs when people leave an organization. Merely collecting the office keys isn't a deterrent to future access because keys—even those using unique blanks or marked Do Not Duplicate—could have been replicated. Companies should investigate what other assets might be held by and need to be recovered from ex-employees. Common possibilities include corporate credit cards, ID cards, laptops, and flash drives containing organizational intellectual property. Additionally, companies often overlook the need to delete such employees from their computer databases, thus dropping their privileges to organizational information. Accountants should periodically run comparisons of employees with IT access and ex-employees' records to ascertain any unauthorized right of entry.

Considering the Human Element

Internal controls are only as strong as their weakest link. At one point or another, controls rely on people—and people are notoriously unreliable. For instance, individuals may

- Believe the policy (and its related task) isn't time effective,
- Be compensating for conflicting IC objectives and policies,
- Trust others to "do the right thing,"
- No longer be able—because of changed conditions—to abide by the policy, or
- Decide (for the right or wrong reasons) to override the policy.

Also, a supervisor may ask employees to violate or override an internal control—for example, not check résumé credentials of an employment candidate because the manager is aware of some untruths contained in the document or perhaps not to perform reconciliations that might uncover theft. Any control that can be overridden through the exertion of management pressure is, by its very nature, illusionary. In some cases, employees responsible for a control may engage (either because their jobs have been made easier or for more nefarious reasons) in considerable sleight of hand to convince other parties (especially auditors) that the control is still effective. Only monitoring will highlight the defects.

As shown in Figure 2, failure to monitor an existing control system for changed circumstances extends the illusion of IC, exposes the system to risk, and ultimately opens the opportunity window for fraud, waste, and abuse.

Lost in the Great Fraud Triangle

The fraud triangle consists of three points: pressure/incentive, rationalization, and opportunity. Pressure and rationalization are individual specific and, as such, can be noted but not controlled. The primary influence on how someone handles pressure and rationalizes certain behaviors reflects personal integrity, but an individual may also be influenced by the organization's culture (in part composed of codes of conduct, the tone at the top, management's attitudes toward ICs, and whistleblower protections). Culture may play a significant role in whether individuals have a higher or lower level of ability to rationalize bad behavior and may encourage or discourage their disclosure of fraud. For instance, why would none of VP of Finance Sujata Sachdeva's employees at Koss Corporation report that she directed them to make fraudulent entries—entries that allowed a $30 million-plus fraud to occur in a company with annual sales of about $40 million to $45 million?

If a company's code of conduct and ethics are aligned with the control system, the system will have been designed to prevent or detect attempts to bypass those controls and, thereby, force compliance. Conversely, unethical management behavior or a lack of a code of conduct can directly impact financial reporting, operational effectiveness and efficiency, or legal compliance. As such, culture elements can indirectly affect the opportunity point of the fraud triangle: When a "damaged" or weak ethical organizational culture exists, there is a higher likelihood that the internal controls system will be flawed and a higher potential for more illusionary controls to exist.

Opportunity is created by failures in the IC system, which is designed to integrate the influences shown in Figure 3. Internal and external organizational changes include previously discussed issues such as growth, downsizing, and technology advances. Organizational size and resources reflect the number of people, technology deployment, and money available to institute and perform control functions. Cost-benefit analysis should be used to estimate the cost of instituting controls and the materiality of any losses (both those that are distinctly quantifiable and those, such as reputational effects, that are more qualitative) that might result from control failures.

Given that the IC system is the primary means of pre-

Figure 2: The Need for Monitoring

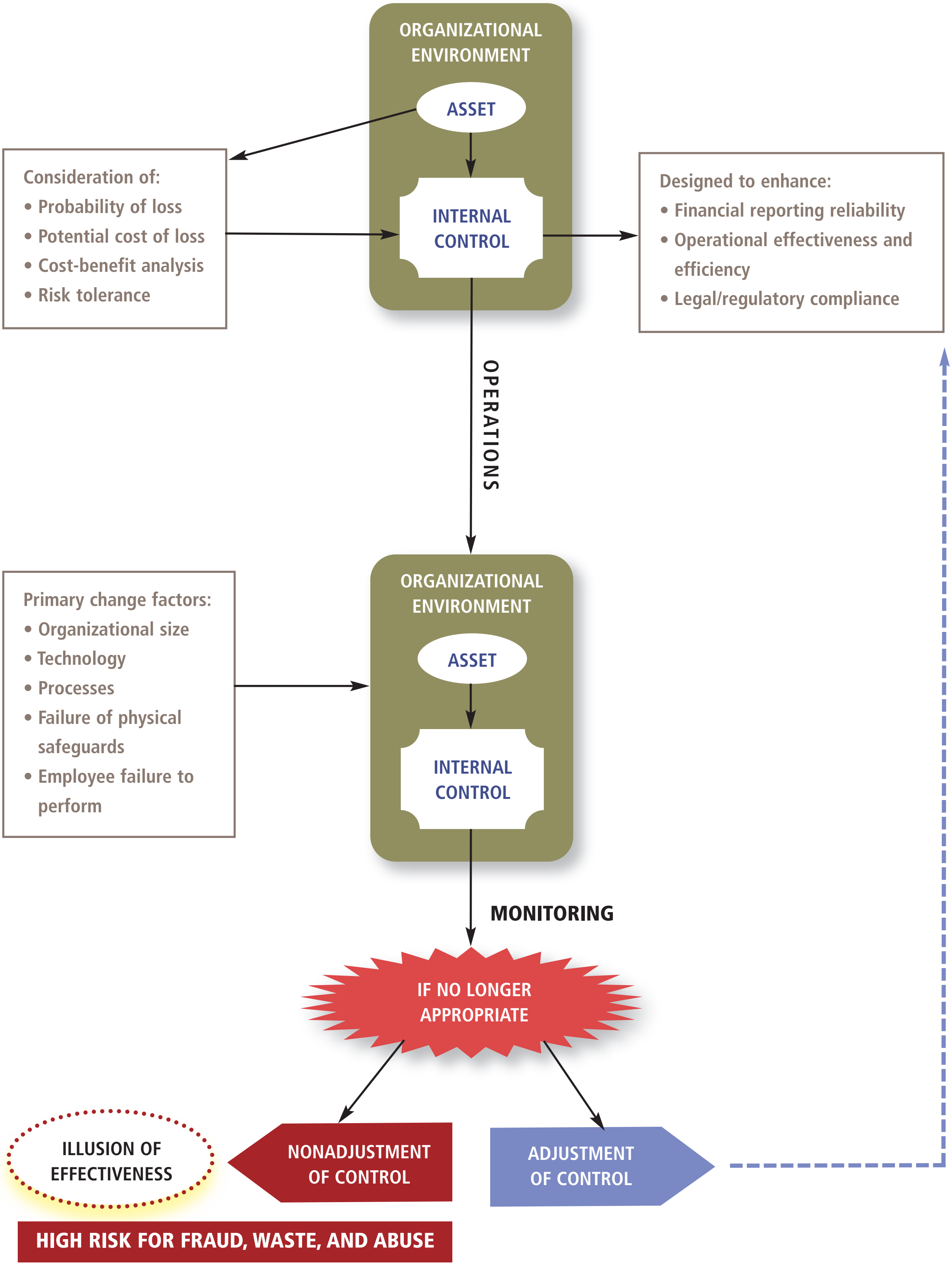
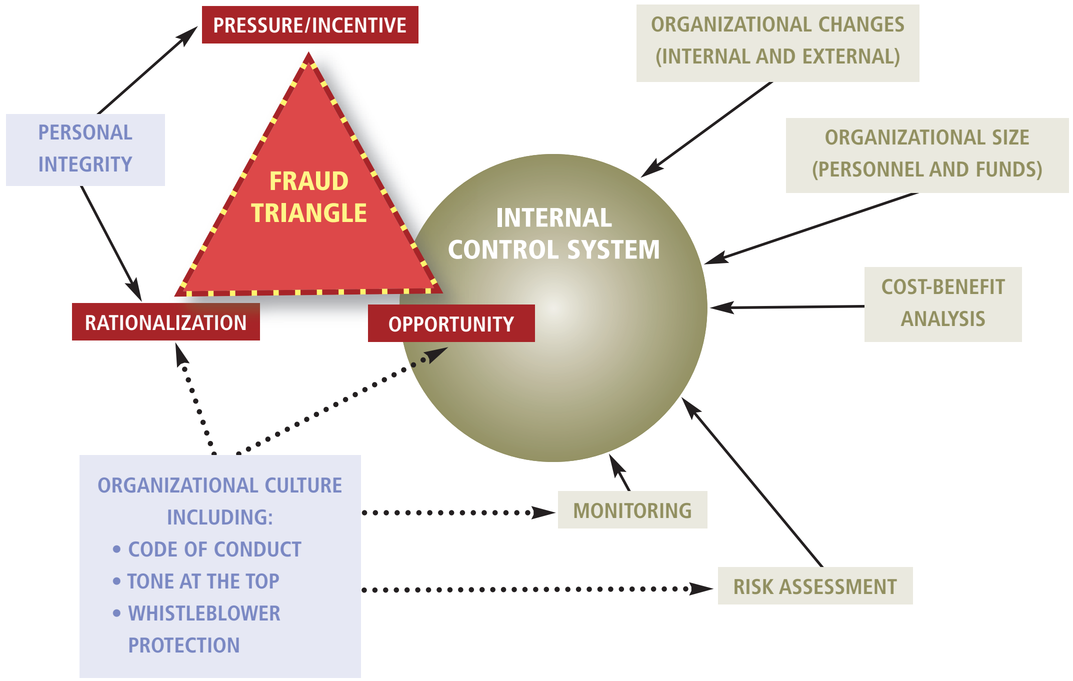


Figure 3: Influences on the Points of the Fraud Triangle



venting, monitoring, and detecting organizational fraud, illusions of effectiveness within that system create a false sense of security. Good companies realize that internal controls will prevent or detect a given issue some percentage of the time, given that 100% protection is cost prohibitive. The expectation is that a breakdown of one control doesn't produce a fatal flaw in the system because the malfunction is within the acknowledged and acceptable risk limits and is usually offset with an alternative control. A failure occurring within an expected range of error is a disappointment; a failure occurring within an expected range of success—which often results from illusionary controls—may be a catastrophe. Only effective monitoring and analysis will prevent reliance on a control that switches between effective and ineffective because of changes in procedures or processes within the operational system.

Preventing Illusions from Becoming Fraud Opportunities

If all humans and machines performed flawlessly and all controls self-corrected for change, then an internal controls system could be designed to effectively guarantee 100% protection from fraud and abuse. But since neither of those conditions exists, the following five factors can improve the IC system and help prevent the complacency that allows the misperceptions of safety to exist, blossom, and become opportunities for fraud.

1. The organization must take a **cost perspective** in designing and making changes to the IC system. Accountants can help compute a cost-benefit analysis to decide how much control is enough and where monitoring controls would be more viable than preventive controls.

2. Management needs to exercise **leadership** by adopting a detailed and workable plan with desired outcomes, supported by operational, tactical, and strategic control components. Without an established plan, the organization will be unsure of which critical elements the IC system needs to protect. Accountants can play a major role in developing this plan by indicating the critical points of "opportunity" that the system needs to minimize.

3. The organization must **enforce** compliance with IC policies and procedures. Enforcement entails involvement by all personnel and oversight (especially by accountants) to ensure that existing controls are active and not simply policies and procedures included in a manual and filed away.

4. Awareness must exist to recognize how changes within the organization may affect the ICs currently in

Figure 4: A CLEAR Plan

C

COST CONSIDERATIONS
Determine the cost constraints under which the organization will be operating.

L

LEADERSHIP
Prepare tactical and strategic plans toward the desired outcome; ascertain critical business factors.

E

ENFORCEMENT
Develop performance measures to motivate employees to perform their functions in accordance with the IC system's policies and procedures.

A

AWARENESS
Monitor changes in the business environment and assess how those changes impact the control system.

R

RISK ASSESSMENT
Determine the implications that might result from asset protection or policy failure.

INTERNAL CONTROL SYSTEM

place. Recognizing the implications of change is essential to effective monitoring and critical to dispersing the illusion that controls are necessarily still viable. Given their ongoing interactions with the IC system, accountants are likely to be primary overseers of change implications.

5. The organization must engage in **risk assessment** to ascertain the potential for failure if specific assets (both hard and intangible) are vulnerable to fraud and abuse. Accountants are especially attuned to understanding the financial repercussions of such exposure. In other words, as shown in Figure 4, organizations must have a CLEAR plan to develop the IC system and to prevent illusions of control safety from becoming sites of fraud opportunity.

Organizations must recognize one critical fact: A fully functioning internal control system is the *only* true stopgap between asset protection and asset loss. No amount of personal integrity or organizational culture will preclude fraud from occurring if pressure on an individual reaches a certain point. The IC system must therefore be designed and enforced to eliminate or subdue the opportunity point of the fraud triangle within the organization's monetary constraints.

Moving in the Right Direction

The internal controls system should be carefully evaluated initially—and continually as changes occur—so that it can provide as much organizational control and security as budgets will allow. Internal and external access, as well as asset susceptibility issues, must be examined, and people must be viewed as a paramount concern in designing the system. An IC system must force compliance throughout the entity—as well as externally among vendors, customers, and financial entities—to provide an acceptable level of defined and quantifiable assurance. But all decisions should include consideration of how internal controls may become illusionary and how to preclude such a transition from functional to nonfunctional.

Although widespread, internal controls deficiencies are often indiscernible because the controls may be *perceived* to be operating as intended when, in fact, they're deficient or have failed. Monitoring of the IC system must be systematic and effective, not random and cursory. For the system to function as expected, organizations—and, most important, their accountants—must stop embracing the illusion of control and begin facing reality with a CLEAR plan that includes **C**ost considerations, **L**eadership, **E**nforcement, **A**wareness, and **R**isk assessment. **SF**

Bill Atwood, CFE, CFF, CPA, is president of Bill Atwood, CPA, LLC, a tax, systems design, and accounting consultancy firm based in Austin, Texas. You can reach him at (512) 965-1790 or bill@Systems-Symmetry.com.

Cecily A. Raiborn, CMA, CPA, CFE, Ph.D., is the McCoy Endowed Chair in Accounting at Texas State University-San Marcos in San Marcos, Texas. Cecily is a member of IMA's Austin Chapter. You can contact her at (512) 245-3878 or CRaiborn@txstate.edu.

Janet B. Butler, CITP, CGMA, Ph.D., is an associate professor at Texas State University-San Marcos and a member of IMA's Austin Chapter. You can reach her at (512) 245-3315 or JButler@txstate.edu.