University of Alaska
Statewide Audit & Consulting Services
Guidance on Internal Controls During a Pandemic
May 2020

It is not unusual for controls to be quickly modified to adjust to a rapidly changing environment during a pandemic or emergency situation. The information communicated within this document is intended to help departments with critical points to be aware of when controls are temporarily modified or temporarily overridden due to staffing and work environment changes. The information is subject to change and updates as needed to adapt to emerging risk situations.

Maintain or implement controls which:

- Are practical and logical from a safety perspective. Consider the safety of staff, faculty, students, and the public.
- Will permit identification of discrepancies or fiscal misconduct in a reliable manner at a later date. This is commonly accomplished through maintaining adequate segregation of duties. When staffing is reduced or unavailable due to emergency situations, it becomes more critical to determine how management will know who was responsible for custody of an asset at the time it went missing.
    - Examples of fiscal misconduct are theft of assets such as change funds, petty cash, cash receipts (cash, checks, credit card information), blank check stock, and university equipment and recyclable materials, personal use of university procurement cards, and concealment of theft of significant accounting errors.
- Permit spot-checking of transactions and support documentation at later date to evaluate compliance with the expected procedures.
- Result in an adequate cost/benefit ratio. This means the cost of the control should not be greater than the risk it is protecting against.

Controls intended to safeguard finances, such as dual control of assets and verification of funds by a second person, can be difficult to maintain when staff are unavailable due to an emergency or pandemic situation. Therefore:

- Consider the extent for which existing surveillance mechanisms can be utilized.
- Determine how a mix of surveillance mechanisms and electronic signatures on deposit verification forms may be used. Use only university sanctioned electronic signature mechanisms.
- Determine a periodic schedule for managerial review of financial accounts, logs and reports to identify any unusual transactions. Perform surprise checks of documentation, too. Determine the red flags which would alert a manager to the possibility of fraud. For example, nonsequential numbering of receipts, used and unused check stock, or other control documents; missing or incomplete support documentation; unusual dates on documents.
- Check in frequently with staff that retain hands-on interaction with financial instruments and documentation.
- Document the controls that are temporarily modified due to the pandemic or emergency situation.

Specific to banking:

- EFTs (wire transfers, ACH, book transfers, stop payment releases) continue to require wet original signatures – no exceptions. (Call backs will be conducted as needed)
- Banking agreements and contracts which contain a banking component continue to require review and approval by Statewide Cash Management.

Be vigilant in reminding staff, faculty, and students to be particularly alert to:

- Phishing attempts intended to defraud an individual or the university. Remind staff that the university will never request bank account information via email. Make sure to confirm any financial disbursement requests or account change requests directly with the requestor (university staff) via telephone. Do not rely on email confirmation because the individual's email account may be compromised, meaning you could be corresponding with a fraudster instead of a legitimate individual. Examples of requests include:
    a. Change of bank account number for a vendor or employee/faculty payroll direct deposit
    b. Payment via wire transfer to a new vendor
- Other fraud schemes intended to load malware or viruses onto devices and systems. Be alert to emails designed to incite worry or panic to lead an individual to click on links which silently embed malware or viruses.
- Consult with OIT for security tips and resources on:
    a. Securing computing resources in the telework environment.
    b. Use of appropriate settings related to HIPAA, FERPA, PCI, GLBA, GDPR, PII and other compliance requirements necessary to conduct business.
- OIT's mobile device security guidelines.
- General best practices for telework environments:
    a. Use a virtual private network to connect to university computing resources.
    b. Change the wireless network password periodically.
    c. Review the devices connecting to your wi-fi router; verify you recognize them as known devices.
    d. Ensure computer updates (software, anti-virus, etc.) are scheduled to occur automatically.
    e. Be vigilant about verifying links when using any device which is also used for university business.

Fraud Factors

Supervisors should be mindful that the following fraud factors increase during pandemic or emergency situations:

- Relaxed internal controls and revised processes
    - Less visual observation, verification, and documentation
    - Results in **increased opportunities** for fraud
- Disruptive situations, such as pandemics, increase employee stress levels both in their personal and professional lives
    - This can result in uncertainty by employees regarding their health, safety, financial security, and job status or stability

- This can further result in:
  - Increase in rationalization that it is acceptable to take advantage of fraud opportunities, possibly thinking that repayment to the organization will occur once the situation is stabilized or that the organization "owes" the employee
  - Increase in pressure due to unstable personal finances or overextended personal financing compounded by looming job security concerns; this can increase the pressure that fraud is the only way out, usually going hand in hand with rationalizing the fraudulent activity as temporary, necessary, or "owed" to the employee

Maintaining adequate internal controls should assist employers with identifying fraudulent or potentially fraudulent activities and trace it back to a responsible individual.

Questions?

Direct situation-specific questions to your supervisor. Audit and Consulting Services is available to provide assistance, but it's optimal to do so while working through your standard chain of command to ensure all situational facts can be discussed.