PAYROLL PROCESS, LAWS AND INTERNAL CONTROLS

Tax Collectors and Treasurers Association of New Jersey
Spring Conference 2019
Marc Pfeiffer, Assistant Director
Bloustein Local Government Research Center,
Rutgers University

RISKS OF THE PAYROLL CYCLE

- Timekeeping: incorrect records
- Controls: mitigates risk, requires attention and routines
- Access to information: segregation of duties
- Adherence to regulations: high level of compliance tax calculations and timing of deposits, for both federal and state requirements

RISKS PRESENT IN TIME-KEEPING AND ELECTRONIC PAYROLL SYSTEMS

- Time sheet fraud
  - Caused by manual entry errors, calculation mistakes or from faults within the computer system. Often resolved by biometric machines.
  - Swipe card fraud
  - These inaccuracies may create a single incorrect paycheck, or they could result in an insufficient accrual of wages for all employees.
- Ghost/Fictitious (fake) employees added to the payroll
- Misclassification – contractors as employees or employees as contractors
- Insider risk: payroll staff colludes with employee to cheat
- Tech driven risks
  - Changes driven by email communications
  - Spoofed directions to bank
  - Payroll vendor-based risks

IRS EXPECTATIONS FOR INTERNAL CONTROLS

- Manage worker misclassification
- Records are secure and available and match to payroll (i.e., deductions)
- Withholding payments are made accurately and timely

TIMEKEEPING SYSTEMS: REVIEW OF INTERNAL PHYSICAL AND ELECTRONIC CONTROLS

- Overtime approval process reviews and audits
- Controls for buddy punching/swiping (when no biometics)
- Expense trend lines: OT problems
- Restrict access to records and system
- Use system reports for manager reviews and verifications of hours

PAYROLL SYSTEMS: REVIEW OF INTERNAL PHYSICAL AND ELECTRONIC CONTROLS

- Segregation of duties: worst case, need management set of eyes over payroll person; other separate prepare, authorize, payments
- External audit reviews: correct calculations, individual verification. Record accuracy
- Change authorizations are written and confirmed; either by employee or management originated
- Need for management process to verify and check actions
- Match payroll register to subsidiary documents

PAYROLL SYSTEMS: REVIEW OF INTERNAL PHYSICAL AND ELECTRONIC CONTROLS

- Specific confirmation of email and phone requests
- IT system
  - Change tracking log reviews; manual entry reviews
  - Access rights reviews; payroll staff cannot have access control rights
  - Strong cyber hygiene practices
  - Error tracking
  - Control of access to timekeeping machines
- Move to direct deposit, otherwise, use address matching and document controls for checks

REQUIREMENTS OF NJAC 5:30-17 AND THIRD PARTY DISBURSEMENTS

- DLGS References for Electronic Disbursement Controls for Payroll Purposes: http://go.rutgers.edu/inxgq9vh
- Provides the authority to delegate tasks to a third party to process payrolls and manage payroll funds. Governing body approval is required. Allows it to:
  - To prepare the necessary payment documentation and execute disbursements from the local unit's bank account on behalf of the local unit;
  - To prepare payment documentation, take possession of local unit funds, and make such disbursements itself on behalf of a local unit; or
  - Any combination of the two.
  - This includes practices those payroll service providers that use their own customized programming process to execute disbursements for the local unit; and those who use a third-party processor to execute disbursement for the local unit.

REQUIREMENTS OF NJAC 5:30-17 AND THIRD PARTY DISBURSEMENTS

- The requirement to take an enabling action is not required when:
  - Payroll service providers perform payroll calculations and do not control the disbursement of payroll funds; and
  - For tax pay and file service payroll service providers that are certified users of the various electronic filing programs of the federal and state government, where the agency does not release, transfer or otherwise execute disbursements of the local unit.
- Key points:
  - Vendor never has access to general fund accounts: only a payroll agency account if they make the deposits to agency accounts on your behalf
  - If vendor touches funds it must have a SOC-1 or SOC-2 report.
  - And make sure they are doing business with other local units and talk to people from that organization

REVIEW OF EMPLOYEE VS. INDEPENDENT CONTRACTOR STATUS

- IRS Publication # 1779
  - Form SS-8, Determination of Worker Status for Purposes of Federal Employment Taxes and Income Tax Withholding.
  - Publication 15-A, Employer's Supplemental Tax Guide, provides additional information on independent contractor status.
- Lots of different circumstances: IRS looks at:
  - Behavioral control
  - Financial control
  - Relationship of the parties
- Why is this a problem?
  - IRS wants to make sure people who you call contractors are not really employees – wage and benefit theft issues
  - NJ political environment gave benefits to employees who are really contractors. We've tried to stop that since 2007.

CHECKLISTS OF CRITICAL CONTROL AND RISKS

- General: from www.accountingtools.com
  http://go.rutgers.edu/1itvmale
- Government detailed: from State of Idaho
  http://go.rutgers.edu/m841iuii
- Technology Controls: 2018 GFOA-NJ Presentation (17 min. video)
  http://go.rutgers.edu/g9z23ehc

ELEMENTS OF FINANCIAL FRAUD

- **Financial fraud resolves around**
  - Operations
  - Compliance
  - Financial communications
- **Where financial fraud is targeted**
  - Receipt of goods and services
  - Vendor activities (procurement)
  - Payroll
  - Receipt of funds
- **Technology creates vulnerability**

COMMUNICATION FRAUD/BUSINESS EMAIL COMPROMISE HAPPENS…

- When email, as well as fax or phone approaches are used to commit fraud:
  - Emails with fraudulent and malware loaded attachments
  - Directed wire transfers
  - W-2 information requests
  - ACH/Direct Deposit payment information changes
  - Lien assignee changes
  - Unauthorized purchases

SOURCES OF TECH ENABLED FRAUD

- **Email addresses and phone numbers can be spoofed**
- Hacker or insider unwarranted escalation in privilege authorization
- Malware activated by employee action or network insecurity
- Can be simple or sophisticated – need to be suspicious of the unexpected

NEW THREATS = NEW CONTROLS

- Core cyber hygiene practices: **do not open attachments from someone you don't know or were not expecting**
  - Plus regular cyber hygiene training on new threats
- **Establish principle of a "trusted source"** for ACH payment assignments or account changes
  - Obtain separate independent verification of actions that change something
  - Independent phone calls, fresh email confirmations
- Strong and enforced password policies for financial transactions
- Dedicated banking computer to avoid machine based threats from keystroke loggers/man in the middle attacks

MORE NEW CONTROLS

- Review procurement controls: verification of non-standard requisitions, purchase orders, and sign-offs; verification of outlier transactions
- Periodic testing of routine transactions
- Controls on PII and PHI – affirmative, individual signoff to put it "in motion" or new access privileges
  - Encrypt any MS office files that have PII/PHI
  - Don't use obvious file names
- Outsource credit card transactions