Clay County District Schools

Internal Audit Board Presentation

May 27, 2025

Agenda

01	Top-10 High-Risk Areas of Focus & Suggested Audit Plan
02	Cybersecurity – Internal/External Penetration Testing
03	Contract Administration
04	Timekeeping
05	Estimated Fees

Top-10 High-Risk Areas of Focus & Suggested Audit Plan

Audit Area	FY 2025 – 2026
Cybersecurity – Internal/External Penetration Testing	Recommended by AC
Contract Administration	Recommended by AC
Timekeeping	Recommended by AC
Ad Valorem Millage	
Human Resources – Recruiting and Onboarding	
Internal Accounts	
Purchasing and Procurement Compliance – Noncompetitive Procurement	
Purchasing Cards (“P-Cards”)	
Self-Insurance	
Transportation – Fleet Management	

Cybersecurity – Internal/External Penetration Testing

Internal/External Penetration Testing

Objectives

The objective of this engagement would be to assess the organization's external and internal security posture by simulating real-world cyberattack scenarios. Testing is designed to evaluate the resiliency of network infrastructure, systems, and configurations against a determined attacker, leveraging both manual techniques and automated toolsets in alignment with the Penetration Testing Execution Standard (PTES).

Approach

Procedures may include the following:

Internal Penetration Testing:

- Assess internal network security from the perspective of a compromised external system or insider threat.
- Target infrastructure such as routers, switches, domain controllers, internal applications, and user workstations.
- Test for vulnerabilities including VLAN hopping, ARP poisoning, Active Directory misconfigurations, and privilege escalation paths.
- Evaluate lateral movement techniques and post-exploitation activities to determine potential access to sensitive systems and data.

External Penetration Testing:

- Simulate attacker activity targeting internet-facing systems to evaluate perimeter defenses and identify exploitable vulnerabilities.
- Conduct footprinting and reconnaissance using open- and closed-source intelligence (e.g., DNS lookups, dark web credential searches).
- Perform service and port identification, vulnerability scanning, and targeted exploitation across systems such as firewalls, cloud platforms, and mail servers.
- Include limited social engineering techniques (e.g., spear phishing or vishing) to assess user susceptibility and potential for initial compromise.
- Document vulnerabilities with supporting exploit examples and provide recommendations for remediation.

Contract Administration

Contract Administration

Objectives

The objective of this engagement would be to assess whether the system of internal controls over contract administration is adequate and appropriate for promoting and supporting the achievement of management's objectives for effective contract monitoring and administration.

Approach

Procedures may include the following:

- Select a sample of contracts and obtain background information relevant to each contract.
- Obtain applicable contract documents, contract administrator information, and detail of expenditures under each contract.
- Review each contract to identify areas of heightened risk and develop testing procedures specific to each contract.
- Assess the District's process and controls relevant to identifying unique risks in contracts and ability to develop procedures to mitigate identified risks.
- Assess adequacy and compliance with select terms of the contract, such as the certificate of insurance, performance, District responsibilities, etc.
- Assess the District's process and controls relevant to vendor monitoring and performance assessments.
- Test a sample of invoices for each of the selected contracts to determine whether:
    - Supporting documentation agreed to the payment amount and was mathematically accurate;
    - Payment was made in a timely manner and in accordance with the pricing terms of the contract;
    - Performance (goods / services received) under the contract was properly verified or monitored prior to payment of the invoice.

Timekeeping

Timekeeping

Objectives

The objective of this engagement would be to evaluate whether the internal control structure over time tracking, recording, monitoring, and reporting is appropriately designed and operating effectively to mitigate inherent risk.

Approach

Procedures may include the following:

- Identify and assess segregation of duties and user access controls for proper monitoring and appropriateness over timekeeping functions.
- Assess the location and security of employee records.
- On a sample basis, verify that time and attendance information (overtime, leave, compensatory time, special pay, etc.) agrees to appropriately approved and authorized supporting documentation.
- Determine that the records and documentation for timekeeping are sufficient to establish an audit trail.
- Review appropriateness of individual and overall time approval.
- On a sample basis, verify that hours paid agree to the supporting documentation (timesheets), and is mathematically accurate and reasonable.
- Review the performance and adequacy of pre-payroll monitoring and exception reports.
- Review and assess each department's policies and procedures for timekeeping and determine if they are complete, reflect current practice, and comply with District policies and procedures.

Estimated Fees

Estimated Fees

The table below outlines the estimated budget for each audit area.

Audit Area	Estimated Fee
Cybersecurity – Internal/External Penetration Testing	$ 40,000
Contract Administration	$ 60,000
Timekeeping	$ 60,000
Total	**$ 160,000**

This is our good faith estimate based upon our understanding of the engagement assumptions and the facts and circumstances we are aware of at this time. If the basis of our estimates is inaccurate, the Fees and Expenses may be different from those we each anticipate. If circumstances are encountered that affect our ability to proceed according to the plan outlined above, such as major scope changes, loss of key Client personnel, unavailable information, or undetermined or requested scope changes during our scoping efforts, we will inform you promptly and seek your approval for any changes in scope, timing or Fees that may result from such circumstances.

THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING