Subject: 3 Year Internal Audit Workplan

Report to: Audit Committee

Report date: Monday, February 8, 2021

Recommendations

1. That the three year Internal Audit Workplan **BE APPROVED**.

Key Facts

- The 2021 Internal Audit Plan was developed following consultation with Senior Management and previous interviews with Audit Committee members and other Councillors.
- Internal Audit also conducted a scan of peer municipalities to determine audit trends in formulating this plan.
- The attached plan provides detailed project scope for those audits that will commence in 2021 as well as highlight additional audits that can be considered part of the longer term audit plan.
- The objective of this 2021 Internal Audit Plan is to provide independent, objective assurance and advisory services designed to add value and improve the organization’s operations and system of internal controls.

Financial Considerations

The consulting budget to acquire external support is set at $200,000 with ability to complete follow-up audits internally to ensure all audits are completed within budget.

Analysis

2021 Internal Audits:

1. **IT Cyber Security and Vulnerability Audit:**
   - Access Control - Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

- Data Security - Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.
- Information Protection Processes and Procedures - Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
- Maintenance - Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.
- Protective Technology - Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

2. IT Penetration Detection and Recovery Testing:

- Anomalies and Events - Anomalous activity is detected in a timely manner and the potential impact of events is understood.
- Continuous Monitoring - The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
- Detection Control - Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.
- Communications - Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
- Analysis - Analysis is conducted to ensure adequate response and support recovery activities.
- Mitigation - Activities are performed to prevent expansion of an event, mitigate its effects and eradicate the incident.
- Improvements - Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
- Recovery Planning - Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
- Awareness Training - The organization’s personnel and partners are provided cybersecurity awareness education and are adequately trained to perform

their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.

3. **BioSolids Value for Money (detailed scope to be determined):**
    - Evaluation of the BioSolids program with a focus on efficiency and effectiveness
    - To determine whether the Niagara Region's Wastewater Treatment plants are effectively meeting its Biosolids Management Policy, program requirements, program goals and objectives.

4. **PCard Follow Up Audit:**
    - To determine the impact of management action plans on the control framework supporting the PCard purchasing program.
    - To determine, through limited testing, if PCard procurement issues still exist.

5. **Consulting Assignments Audit:**
    - Review of the procurement, selection, oversight and post evaluation method for consulting assignments
    - Assurance that applicable consulting recommendations have been effectively implemented.

2022 Internal Audits (Planned):

1. Contract Management (Long Term Contracts)
2. Contract Management (Capital Projects)
3. Paramedic Fleet Management
4. Non-Competitive Procurement Follow-up Audit
5. Bridge Management and Inspection Audit
6. Research and Pilot of Continuous Controls Monitoring (CCM)

2023 Internal Audits (Planned):

1. Pothole Repairs
2. Traffic Signals Audit
3. Quality Assurance Audit of Sexual Health Clinics
4. Ontario Works Payment and Contract Management Audit
5. Non-Monetary Grant Programs

Other areas for consideration:

- Housing Programs and Maintenance Management Audit
- IT Governance Review

Alternatives Reviewed

For the majority of audits an external audit firm will be engaged. It is proposed based on available funding that the two follow-up audits be conducted internally by the Manager, Internal Audit.

Relationship to Council Strategic Priorities

Internal Audit along with related audit functions such as Value-for-money (VFM) audits and compliance reviews were identified and approved within the current Council's Strategic Priority – Sustainable and Engaging Government. The goal of this strategic initiative is a commitment to high quality, efficient, fiscally sustainable and coordinated core services through enhanced communication, partnerships and collaborations with the community.

Other Pertinent Reports

- AC-C 16-2020 – 2021 Audit Workplan

Prepared by:
Frank Marcella, MPA, BEd
Manager,
Internal Audit

Recommended by:
Todd Harrison, CPA
Commissioner,
Corporate Services

Submitted by:
Ron Tripp, P.Eng.
Acting Chief Administrative Officer