Audit of Information Technology Security Controls
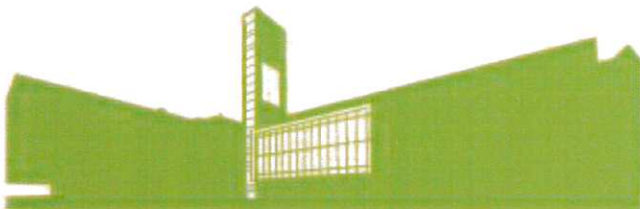# Finance, Administration and Audit Committee

December 8, 2015

VAUGHAN
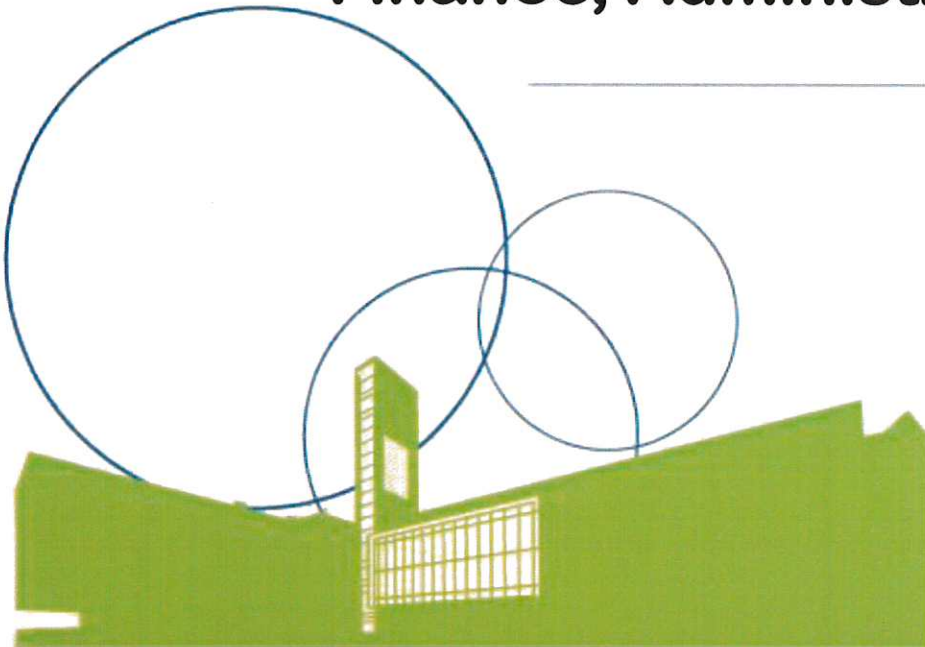
Agenda

- Audit Conclusion

- Audit Objective and Scope

- Audit Approach – Critical Security Control Model

- Observations and Issues

- Action Plans

- Questions

VAUGHAN

Audit Conclusion

Computerized Data Security is in an Evolutionary Phase

- ITM has Good Practices to Help Detect and Prevent Malicious Attacks, has Secure Configuration Standards and has Good Reliable Backup Data

- Key Improvement Opportunities include better Device and Software Management and using a Vulnerability Scanning Tool or Service ["Quick Wins"]

VAUGHAN
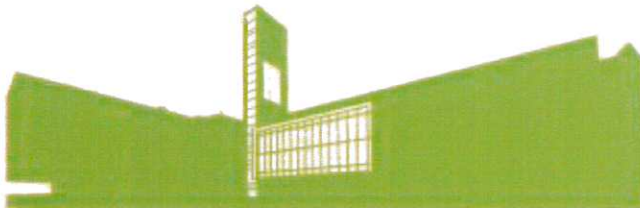
Audit Objective and Scope

- Evaluate the Adequacy and Effectiveness of Processes and Procedures to Mitigate Business Risks Related to Securing **Computerized Information** and Data on City Networks and Computers

- **Not in Scope**: → Paper Based Information Security and Computerized Information Maintained Independently by Users [i.e. – USB Devices, Mobile Devices, Local Drives]

4
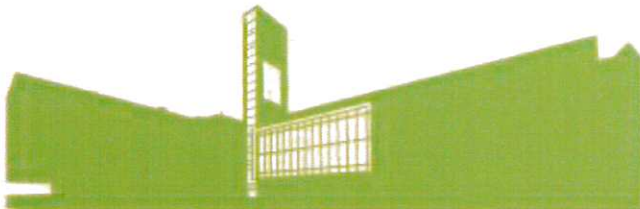
VAUGHAN

Audit Approach – Critical Security Control Model

- ITM Used Third Party Vendor for Independent Review

- City of Vaughan Compared Favourably to Other Municipalities

- Used Critical Security Control Model as Evaluation Tool

- Model Focuses on "High Payback" Controls [20 Controls Based on Common Attack Patterns – "Prioritized Baseline"

- Internal Audit Relied on Evaluation Results

VAUGHAN
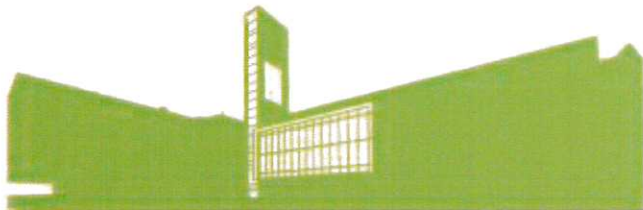
Issues and Observations

- **Implement "Quick Wins"** – Control Improvements Representing the Biggest Impact for Lowest Financial and Optimum Operational Impact

- **Implement Security Policy** – Including Building Security Awareness and Providing User Education

- **Implement Risk Based Security Program** – Standards, Roles and Responsibilities, Compliance with Legislation
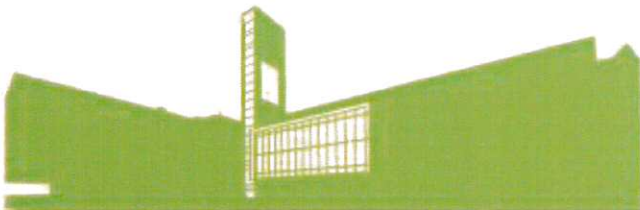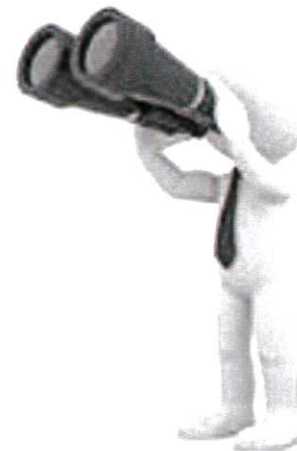
VAUGHAN
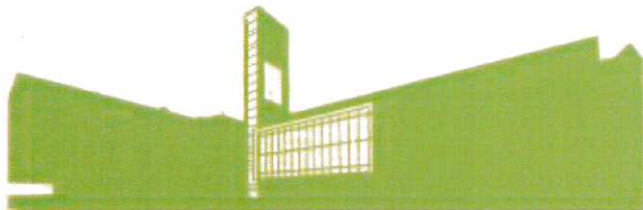
Recommendation: Implement Quick Win

Action #1: Vulnerability Management

- Enable the automation of security updates for new infrastructure and systems
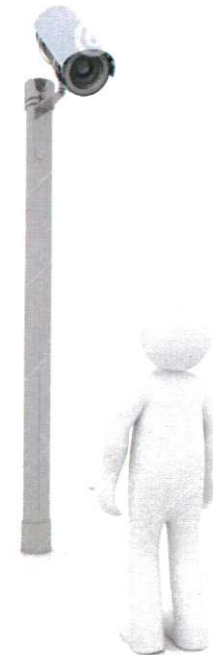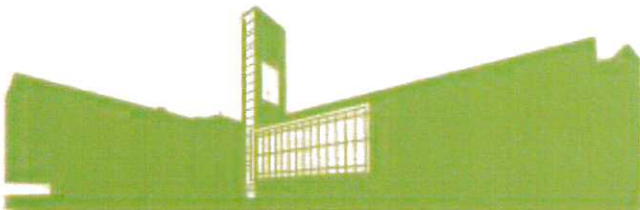- Deploy vulnerability scanning software

Q2 2016

VAUGHAN

Recommendation: Implement Quick Win

Action #2: Unauthorized Devices

- Asset discovery tool
- Deployment of technology preventing unauthorized access to corporate network and resources
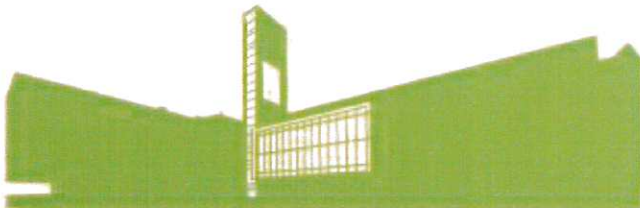
Q1 2017

Recommendation: Implement Quick Win

Action #3: Unauthorized Software

- Software discovery tool
- Deployment of technology preventing unauthorized software to execute on corporate devices
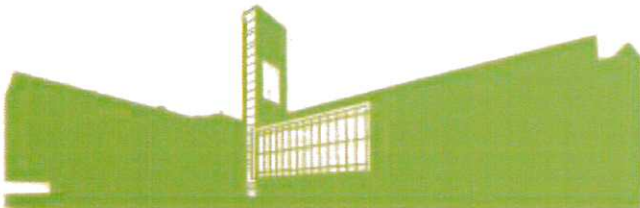
Q4 2017

VAUGHAN

Recommendation: Implement Security Policy

Action: Enhance Existing Security Policy

- Update Acceptable Use Policy
- Update IT Security Policy

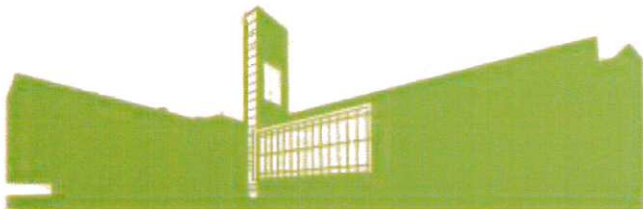**Q4 2016**

SECURITY POLICY

VAUGHAN

Recommendation: Implement Risk Based Security Program

Action Items:

- Perform scheduled penetration testing on IT Infrastructure
- Mitigate risks through security assessments
- Develop IT Security Incident Response Process
- Enhance IT Security Key Performance Indicators
- Create IT Security Awareness Training

On-going

Security Awareness Training

Security Policies

Questions?

VAUGHAN