The Corporation of the City of Windsor

Security incident prevention and mitigation

Distribution list
For action
Jan Wilson, Corporate Leader of Parks, Recreation, Culture, and Facilities
Tom Graziano, Senior Manager Facilities
Adrian Busa, Manager Facilities
Marco Aquino, Executive Initiatives Coordinator

For information
Vincenza Mihalo, Executive Director - Human Resources
Julie Ryckman, Manager - H&S and Wellness

FINAL Internal audit report

April 27, 2020

pwc

Contents

Executive summary

Safety context

Safety and security are closely interrelated concepts that pertain to protection of lives and assets. Security is the broader concept that involves having the infrastructure (both physical and social) in place creating the context for safety.

Safety is the experience of being free from risk of harm, and the knowledge and preparation to deal with risk when it arises.

We focused on the security and safety risks related to eight (8) downtown (including two (2) municipal parking garages) City of Windsor properties.

Safety numbers for the eight sites

- Over 800 employees are accommodated across these City properties.
- Three (3) properties also accommodates third party tenants.
- One (1) property is close to downtown where City Hall staff park their vehicles.
- Across these properties, there are eleven (11) cash stations related to multiple services.
- Six (6) properties offer after hour supervision by guards.
- Ten (10) security service provider staff are assigned across seven (7) properties and increased when required.
- Eleven (11) City supervisors are assigned across these properties for general supervision and safety awareness.
- Over 100 Duress (panic) buttons and around 250 cameras are installed across these properties.
- Subsequent to this audit, one (1) library branch was opened in the downtown area.

Project purpose

We conducted an assessment of the internal controls and processes, assessment management has implemented to achieve the three objectives related to Security Incident Prevention and Mitigation managed by the City of Windsor (the City). These related to:

- resource allocation and safety programs;
- event and incident monitoring; and
- training/awareness.

Specific scope, objectives and exclusions are described in Appendix B.

What we did

To conduct our work we completed various activities to achieve our objectives by covering three (3) risk domains including Workplace, Occupation, and Services. Our activities included, but were not limited to:

- Compiled a list of site inspection requirements based on City policies/procedures as well as good practices and visited two (2) sites (2 different times of the day) to determine if these practices were in place.

- Our visits included knowledge assessment of staff, site profile discussion, site tour, open Q&A session with supervisors and guards, review of demonstration of safety or security components including observation of physical infrastructure, duress buttons, cameras, radios, locks, lights to assess whether they were functioning at the time of visit.
- Reviewed security service provider contracts and performance terms and nature of protection services available.
- Assessed management's oversight/governance process over the security vendor.
- Reviewed City documentation to determine if legislative requirements are incorporated into H&S documentation and procedures.
- Reviewed and analyzed incident management mechanisms including event reporting protocols.
- Reviewed practices in place for evacuation drills.

Scope limitation

Given current funding, a formal risk assessment for site selection and future planned sites has not been completed. As such we are not able to conclude on the sufficiency of the security threat/vulnerability/risk assessments (TRVA) control.

Overall assessment

Overall our assessment of Security Incident Prevention and Mitigation at the City is one of **No Major Concerns**. We identified areas where one significant internal control weakness was noted which is reported in the Private and confidential package.

A total of **four findings** have been identified surrounding the Resource Allocation and Incident Monitoring area whereas **two considerations for improvement** have been provided as well.

Management comments

In the absence of a centralized corporate security division, a single responsible party does not currently exist. A report to council dealing with the results of 5 facility security risk assessments, and a security master plan is anticipated later in the year. Administration will be seeking council direction, including the option to establish a centralized corporate security division.

Management agrees with the recommendations, and has provided specific action plans in the Detailed Observations section, however, pending the outcome of the aforementioned report to council, a responsible party is not identified for some management action plans at this time.

Summary of internal audit results

Based on the controls identified and tested, we have determined that there is reasonable evidence to indicate that:

#	Objective	Report classification				
		Optimally Controlled	Managed	Some Improvement Opportunity	Major Improvement Opportunity	Unacceptable Risk Exposure
1	Resource allocation, and Safety program (including physical factors, safety apparatus and building floor plans) related decisions consider safety hazards and security needs				✓	
2	Security/safety incident monitoring occurs periodically including logging, defined categorization of incidents (e.g. by location), and reporting processes to facilitate timely and appropriate updates to Safety programs			✓		
3	Regular and relevant capacity building/training/awareness provided to exposed positions for responding to safety/security related concerns or priorities		✓			

We identified areas where internal control weakness exists. One was noted as a significant control deficiency. If implemented, our recommendations would serve to provide a more consistent and solid security posture, clarity of responsibility, related framework and service provider governance.

Management has provided comprehensive action plans, which we believe will address the deficiencies noted. Below we provide a summary of the findings noted as part of our work:

Summary of findings

#	Topic	Rating[1]		Management action plan
Resource Allocation & Safety Programs				
1	Establish protocols for joint ownership of security policies and monitoring controls (design effectiveness)		Significant	Council direction on a management report to council will provide further direction as resources and funding are required to address the finding. [Dec 31, 2021] *Council direction will then be used to determine a remedial action plan.*
		X	Moderate	
			Low	
2	Establish define responsibilities to monitor contractual requirements (design effectiveness)		Significant	The responsibilities indicated will be defined and implemented. [Dec 31, 2022]
		X	Moderate	
			Low	
3	Reported in the confidential package	X	Significant	Administration will be seeking council direction, including the option to establish a centralized corporate security division. [Dec 31, 2020]] *Council direction will then be used to determine a remedial action plan.*
			Moderate	
			Low	
Event and Incident Monitoring				
4	Enhance protocols for managing and documenting dynamic security plans (design effectiveness)		Significant	Administration will be seeking council direction, including the option to establish a centralized corporate security division. [Dec 31, 2020] *Council direction will then be used to determine a remedial action plan.*
			Moderate	
		X	Low	
Training/Awareness				
	N/A			

Management comments

Management appreciates the findings and recommendations within this report as a way for the Corporation to pursue continuous improvement in the way it provides a safe and secure environment for its employees and visitors.

In the absence of a centralized corporate security division, a single responsible party does not currently exist. A report to council dealing with the results of 5 facility security risk assessments, and a security master plan is anticipated later in the year. Administration will be seeking council direction, including the option to establish a centralized corporate security division.

Management agrees with the recommendations, and has provided specific action plans in the Detailed Observations section, however, pending the outcome of the aforementioned report to council, a responsible party is not identified for some management action plans at this time.

Name:	Jan Wilson
Title:	Corporate Leader, Parks, Recreation, Culture, and Facilities
Date:	April 27, 2020

1 See Appendix A for Basis of Finding Rating and Report Classification

Overview

Internal Audit selected a sample of two (2) of the eight (8) downtown properties and conducted site visits. The eight (8) downtown properties are listed as follows:

1. 350 City Hall Square*
2. 400 City Hall Square*
3. The Windsor International Aquatic and Training Centre*
4. The Windsor International Transit Terminal*
5. Windsor Museum and Art Gallery*
6. Windsor Water World
7. Pelissier Parking Garage
8. Goyeau Parking Garage

* These represent the five (5) sites for which an external security consulting firm has been retained to conduct security threat/vulnerability/risk assessments (TRVA).

During our visits, we inquired about and observed safety programs available for employees including safety/security related tools and systems that were in place. This included information related to external lighting, alarm system, access mechanisms, inspection system, monitoring by security guard, maintaining visitor logs, availability of emergency manuals, training and support provided to employees, incident reporting and management, security camera installation, etc.

To illustrate how joint/functional responsibility for managing corporate security risks we can summarize management's activities into three (3) categories 1) managing the physical infrastructure 2) managing workplace health and safety and 3) managing contracted services.

The following comments are relevant to these three (3) managed services:

- Physical infrastructure and workplace / occupational health and safety services are governed by the relevant legislative framework, policies, procedures and training content necessary for operationalizing security or safety programs and plans.
- For contracted services, the contracts and relationships are the basis for assessing/managing the corporate security risks and supplemental documents (ie. security guard post orders) provide more site specific guidance.
- Some controls are not being performed in a coordinated manner among the managed service groups. The recommendations in this report aim to improve the coordination and interaction thereof. The City may establish protocols for joint ownership of overlapping/common security policies and controls and improve interaction with health and safety teams.

The table on the following page specifies the department or function responsible for each of the managed service categories until a central owner for managing corporate security risks is defined.

	1. Physical security infrastructure	2. Workplace H&S	3. Contracted security services
Specific Managed Services	• Card access (Hardware) • Duress/panic alarms • Security cameras • Intrusion alarms • Entry points (locks, card access devices)	• Site Management of Access Cards • Safety advisors • Violence risk assessment • Safety site inspections • Evacuation drills • Incident records • Job hazard assessment and training needs	• Professional and protective security services • Security threat assessments • Commissionaire services (contracted by Employment and Social Services) • Armoured Car Services
Function / Department	**Facilities Services**	**Human Resources** ➔ H&S committee/teams ➔ H&S staff advisors ➔ H&S site manager or supervisor	**Purchasing, Facilities Services, Employment & Social Services and Finance**

We noted that policies are less mature given the absence of a corporate security risk owner for developing, maintaining and overseeing policy and procedures for effective implementation of security programs and measures. Currently, the Facilities department is managing the Corporate Security Assessment and Planning process only in context of a corporate project, and currently there is no central ownership for the organization in relation to security policies, programs and control measures.

Security programs and plans

The City has retained an external security consulting firm to document the Security Master Plan by conducting security threat/vulnerability/risk assessments (TRVA) for five (5) selected sites. The assessment will also result in various security related recommendations, including resource allocations. The consultant will also assist the City with documenting necessary corporate security policies and procedures, which are currently not in place. The amended implementation date of these policies and procedures is planned for the 2021 year.

Management should consider the recommendations made by the third party consultant as it pertains to a central/corporate security division or unit. However, in the interim, we recommend drafting a policy to provide clarity with respect to joint and individual responsibilities to staff and the commissionaire. Consideration to grouping the properties in the downtown core should be given, so they are managed with a more specific focus toward central ownership. This may be accomplished initially with a Downtown Security Plan using completed TRVA's for five (5) selected sites. Within the downtown plan, we recommend developing a Security Video Surveillance Policy and Corporate Security Message Center (CSMC) usage procedures.

The City has retained a security service provider to provide professional and protective security services. Communication tools and approaches are established at select sites for escalating or reporting of incidents, and such protocols are documented in security guard post orders (relative to each security guard's post). In addition, a daily communication channel between the City Supervisor and the security service provider's guards exists. A CSMC is installed at the City Hall campus, which assists security guards, the Facility Site Manager and their staff in the event of major staffing issues that require attention. This function provides the above mentioned staff the opportunity to direct emails of concern to the relevant parties. In the event that a panic button is activated, the security guard arrives at the spot and records the actions on the incident record accordingly.

We noted a few control enhancement opportunities including:

- Adding a service hold over clause in the contract to address the time gap associated with going through the process from RFP and entering into a formal contractual agreement with a new vendor, or incumbent.
- Record of common recurring service disruptions should be maintained to document security needs and to handle ad hoc situations.
- A security services contingency plan should be documented as part of vendor risk analysis considering unforeseen situations.
- Security planning/change management and risk assessments should be coordinated across functions.

Incident management process is in place to detect, respond and report on physical security incidents.

Health and Safety programs

The City safety programs are managed by the Manager H&S. This manager is actively involved in conducting various safety related programs such as delivering training, facilitating drills, threat assessment and safety inspections.

Training needs are identified by the Manager H&S by conducting job hazard assessments which identify training measures/physical measures. The Job Hazard Assessments are provided to the Executive Director of the affected position and posted on Dashboard. The job hazard assessment also incorporates consideration of the past three years' incidents reported in the respective site. The Manager H&S provides training to staff including communications such as handling situations, working alone, safety in parking lots, etc. In addition, mandatory training on respectful workplace is also delivered at the time of hiring and is repeated every five years.

At a minimum, once a year, an evacuation/emergency drill is performed as evidenced by the City of Windsor Emergency Response Manuals. A debrief session is conducted after the drill by the responsible person assigned by the Site Manager for lessons learned. Emergency Manuals (EM) are accessible to employees via the City dashboard as well as the departmental Code of Conduct policies. The Code of Conduct is also physically posted on bulletin boards within the facilities.

Workplace Violence Threat Risk Analysis are conducted by the occupational H&S advisors every five years to observe and assess department work sites and recommend potential considerations regarding employee training/safety, or improvement to building efficiencies. This assessment is also conducted specifically when a violent incident occurs at a specific site. The Workplace Violence Threat Risk Analysis' are provided to the Executive Director or Senior Manager of the site, and the JHSC, etc.

Safety inspections are performed by the Joint H&S Committee on a monthly basis. The Committee members perform this assessment along with the site supervisor. These inspections may identify security concerns. As documented in the minutes of the Joint H&S Committee, the Committee also follows up on past observations and work orders (if any) are tracked to completion in subsequent assessments.

Change management protocols are in place to address changes being made to safety and security procedures. Facility assessment was conducted after the construction of a new facility in 2013. This was observed by inspecting the Joint H&S Committee meeting minutes. Also, when the use of a site changes, a new Workplace Violence Risk Assessment is completed.

In order for management to identify security specific trends and to inform long term security master planning, inputs such as: drills, site inspections, incidents, duress logs, job hazard summaries and number of occupants could be compiled by site and shared where appropriate. These items are currently posted on dashboard, site bulletin boards, and provided to onsite JHS committees.

Detailed observations

1. **Establish protocols for joint ownership of security policies and monitoring controls (design effectiveness)**			**Overall rating:** Moderate
Impact:	Medium	**Likelihood:**	Likely

Observation:
Currently there is no central ownership for the organization in relation to security policies, programs and plans associated with enterprise security risk. The Facilities department manages building security infrastructure for facilities within its budgeted portfolio (not all City facilities; for example, wastewater treatment plants), including key card hardware system, duress/panic alarms, security cameras and intrusion alarms.

a) When it comes to employee health and safety, policies and procedures are centrally maintained and updated with clear joint responsibilities outlined. However, in regards to how security related procedures are managed we noted the following:

- some procedures were outdated (more than 10-15 years old) including visitor log, duress system, emergency blue lights, key/access card; and
- specific policies which were observed in other comparable municipalities not available (Security Video Surveillance Policy and Corporate Security Message Center (CSMC) Policy).

b) While processes exist in some facilities to test security infrastructure, a consistent methodology for performing threat/vulnerability/risk assessments (TRVA) and periodic hardware/infrastructure inspections was not in force at the time of the audit and we understand more formal risk assessments may occur after the master plan is finalized, subject to funding approval. While there is health and safety hazard/risk information gathered from the H&S teams managed by the HR function, the interaction points to share this information with other functions (e.g. facilities) are not clearly defined. Management on site is currently responsible to ensure the work is completed for their site with follow up provided by the JHS committees.

Implication
Security policies and procedures, roles and responsibilities as well as accountabilities and expectations are not sufficient for the security risks present.

Recommendation
a) Management should consider the recommendations made by the third party consultant as it pertains to the central/corporate security division or unit. However in the interim we recommend drafting a policy to provide clarity with respect to joint and individual responsibilities to staff:

- the ownership of security risks should rest with the facilities department when it pertains to managing security infrastructure (cameras, doors, lighting, emergency duress system, key card hardware system, etc.);
- where there is joint responsibility, a policy should be developed articulating the responsibilities by workplace, occupation or services with consideration for assessing risk/hazards, recommending security measures/needs, performing regular testing and reviews; and
- criteria for assigning responsibilities may also need to be developed such as a focus on the department occupying each facility.

Management should consider grouping the properties in the downtown core so they are managed with a more specific focus toward central ownership. This may be accomplished with a Downtown Security Plan, which would incorporate downtown posts including the posts managed via a contracted service provider.

Within the downtown plan, we recommend developing a Security Video Surveillance Policy and CSMC usage procedure for effective communication. New/updated policy/procedure should be communicated to relevant employees on a timely basis.

b) Management should consider formalizing periodic security audits to assess effectiveness of procedures/policies and consider spot audits for risks such as: handling of security incidents, vendor performance, camera systems functionality, duress system functionality, etc. Assign a central role (security technician) who may be responsible for monitoring security specific trends and to inform long-term security master planning. The central role could be responsible for one or more of the following activities:

- spot inspections and walkthroughs of facilities, hardware/equipment and real property;
- perform check-ins with key stakeholders to inquire about security incidents;
- aggregate information per facility such as: drills, site inspections, incidents, duress logs, job hazard summaries and number of occupants;
- review records from the inspections of other functions from a security point of view; and
- perform threat/vulnerability/risk assessments (TRVA) to determine if inspection routines should be adjusted based on incidents/findings.

Management action plan		
a) Resources and funding do not currently exist for Facilities to maintain security infrastructure beyond its operating budget. Pending a report to council that will deal with a security master plan, corporate responsibility for security will be determined. A Security Video Surveillance Policy will be developed via the security assessment and master planning project.	**Responsible party:**	Senior Manager, Facilities
	Due date:	December 31, 2020
b) A report to the council dealing with security is forthcoming. Administration will be seeking council direction, including the option to establish a centralized corporate security division. Although management agrees with the principle of the recommendation, the responsible party for corporate security is still to be determined. Subsequent to the Council direction the remaining action plans or risk acceptance will be determined.	**Responsible party:**	Senior Manager, Facilities
	Due date:	December 31, 2021

2. Define responsibilities to monitor contractual requirements (design effectiveness)			Overall rating: Moderate
Impact:	Medium	**Likelihood:**	Likely

Observation:
While reviewing the relevant third party risks with respect to contracts with outsourced security service provider, we noted the following:

a) The contract with the current security service provider was not signed until 56 days subsequent to the commencement of services. The service date was also changed from what was in the original RFP (Aug 26, 2019 to Oct 1, 2019).

b) Site specific emergency management (including drills by HR) training were not provided consistently across all facilities to security service provider's staff.

c) Service level performance measures are not clearly documented in the contract nor are designated roles for monitoring service levels clearly defined.

d) Post orders were not ready for release to security service provider's staff prior to their allotment (as of the date of fieldwork). It is also not clear whether the security provider staff signed the post order acknowledgement form prior to commencement of duty.

e) A third party security consulting firm has been retained to document the Security Master Plan via conducting security threat/vulnerability/risk assessments (TRVA) of five (5) selected sites as per the RFP. It was noted:

- a standard template for conducting assessments has not been shared with the City as of our fieldwork; and
- meetings with the consultant regarding discussion and updates are not documented/tracked.

f) Mobile patrolling units are primarily used for alarm response, and occasionally for fire watch. These units are equipped with GPS however, the City does not have direct access to the GPS data. Mobile patrol usage by the contractor is not tracked.

Please also refer to consideration for improvement #2 related to vendor performance evaluation.

Implication:
Inappropriate response or service impacting City brand and/or financial obligations. The security master planning process may be delayed.

Recommendation:
Management should:

a) Consider updating the existing contract to add a service hold clause with respect to the time gap of going through the process from RFP to entering into formal contractual agreement with future vendors (including incumbent).

b) Facilitate site specific emergency management (including drills by HR) to be provided consistently across all facilities to security service provider's staff.

c) Designate roles for monitoring service levels should be defined accordingly and consider updating the existing contract to add service level measures with respect to prevention and/or mitigation of security events, including:

- Regulations Management,
- Quality Management Systems & Continuous Improvement,
- Cost Management and Non-conformance Reporting,
- Performance/Schedule/Timeline,
- Management and Allocation of Resources, and
- Communication.

d) Provide post orders to any new security service provider's staff prior to their allotment at respective posts. For future practice, prepare and release security service provider post orders prior to post allotment. Post order acknowledgement form should be signed off by the respective security staff prior to commencement of duty.

e) Obtain standard template from the third party security consulting with respect to security assessment to independently conduct similar future security assessments, document and track progress of service received and also maintain agenda items and/or minutes for meetings held.

f) Have arrangements with the contractor to have access to the source GPS data from regularly deployed mobile patrolling

units. Formalize tracking of mobile patrol usage.		
Management action plan		
a) Facilities will endeavour to ensure that security guard services contracts are fully executed prior to the expiry of the previous contract as the transition is made from one to the next. Adding a "service hold clause" will be reviewed and considered in the next RFQ.	**Responsible party:**	Manager, Parks & Facilities, Projects and Assets
	Due date:	December 31, 2022
b) Contracted security guards will participate in future emergency management drills, which are coordinated with the department using the services.	**Responsible party:**	Manager, Health and Safety; Departments using guard services
	Due date:	December 31, 2020
c) Service level performance metrics will be reviewed and may be added to the next security guard services contract. Departments that are users of the services will monitor performance and provide performance feedback annually in accordance with Purchasing policies.	**Responsible party:**	Senior Manager, Facilities; Departments using guard services
	Due date:	December 31. 2022
d) Post orders will be provided to the security guard services contractor prior to guards starting in their respective posts. The contractor is responsible to ensure that the guards assigned to a post are aware of, and understand the post orders.	**Responsible party:**	Senior Manager, Facilities; Departments using guard services
	Due date:	December 31. 2020
e) The Corporation will utilize a format similar to that used by the consultant for future assessments. Meeting minutes for future meetings will be prepared.	**Responsible party:**	Senior Manager, Facilities; Future Corporate Security Manager
	Due date:	December 31. 2020
f) Access to the source GPS for mobile patrolling units is not required due to the limited amount of mobile patrols. The additional cost of the service is not warranted at this time, but will be considered if required in the future.	**Responsible party:**	Manager, Parks & Facilities, Projects and Assets
	Due date:	Complete

3. Reported in the confidential package		
Management action plan		
A report to the council dealing with security is forthcoming. Administration will be seeking council direction, including the option to establish a centralized corporate security division. Although management agrees with the principle of the recommendations, the responsible party for corporate security is still to be determined. Subsequent to the Council direction the remaining action plans or risk acceptance will be determined.	**Responsible party:**	Senior Manager, Facilities
	Due date:	December 31, 2020

4. Enhance protocols for managing and documenting dynamic security plans (design effectiveness)			Overall rating: Low
Impact:	Low	**Likelihood:**	Likely

Observation:
When reviewing the resource/security planning processes we noted that:

a) Standard procedure and record of common recurring service disruptions is not maintained to document security needs, to handle ad hoc situations (e.g., protests, elections, postal strike, temporary displacement, construction/decommissioning, special ceremonies etc), and to inform annual security planning and resource allocation.

b) A security services contingency plan is not documented as part of vendor risk analysis.

Implication:
The City may not be able to carry out necessary security arrangements in an event when a security service provider under-performs or is unable to deliver for any reason.

Recommendation:
Management should formalize the the security planning process by considering the following:

a) A template “request form” or “security needs analysis” for assigning/deploying temporary security measures (e.g. when the workplace is displaced) should be established. This may include options for selection of services (e.g. on-site guard service, alarm response, mobile patrol need, pre-planned temporary guard service, emergency callout, crossing guard needs, etc.) available within the contract. The template may also include: approval, department requesting, nature of event, number of venues, frequency, timings, nature and number of occupations impacted. City may allow exemption to this form if event characteristics have already been logged. Special events log for recurring events should also be maintained.

b) Develop security contingency plans to address unforeseen security needs in the event of vendor substandard performance or contract termination. Such a plan may include prioritized high ranking expectations and assigning certified/trained guards employed by the city or deploy certified security trainers to build temporary capacity or an alternate service provider or solution. The contingency plan could be an extension of the previous recommendation as to responding to areas which may need security without delay or lapse.

Continued from finding 1 regarding a Corporate Security Message Center (CSMC) usage procedure, we recommend the contingency plans or temporary/ad hoc changes be communicated using the CSMC for purposes of maintaining a repository for security requests placed to central.

Management action plan		
a) A report to the council dealing with security is forthcoming. Administration will be seeking council direction, including the option to establish a centralized corporate security division. Although management agrees with the principle of the recommendation, the responsible party for corporate security is still to be determined. Subsequent to the Council direction the remaining action plans or risk acceptance will be determined.	**Responsible party:**	Senior Manager, Facilities
	Due date:	December 31, 2020
b) In the event that the contracted security vendor was unable, or unwilling to provide services, the Corporation would use emergency and sole source procedures, outlined in the Purchasing By-Law, to hire another security guard service until a permanent solution can be implemented.	**Responsible party:**	Senior Manager, Facilities
	Due date:	Complete

Considerations for improvement

1. Establish quantifiable expectations/goals for drills

Observation
At a minimum, once a year an evacuation/emergency drill is performed as evidenced by the City of Windsor Emergency Response Manuals. It was noted that no quantifiable expectations/goals are established to benchmark the results of these drills.

Consideration
Management should consider developing clearly defined measures for the drills. This may benefit management in directing its efforts in improving evaluation times by implementing measures like the PA system etc. These measures may be extended to other security measures, such as the number of times trespass policy was applied etc. Examples of measures could include but are not limited to:

- number of reported cases where staff could not hear the alarm or were not reachable by radio or by designated informer;
- number of minutes building evacuated/locked down (for comparison against sites with similar characteristics);
- number of days between drill and communication of lessons learned;
- number of near miss events originating around or on city properties; and
- average number of occupants for each marshaling areas.

2. Readiness to adopt the mandatory vendor performance management controls

Observation
A set of Vendor Relationship Management Procedures and Guidelines have been drafted and will be presented to the Council in the upcoming months (preferably April 2020 or May 2020) as indicated by management. We noted that protocols for vendor performance evaluation for service providers have been established in the draft procedures and would be communicated to contract/vendor relationship owners once approved.

Consideration
We recommend that the owners of significant contracts start to prepare for the implementation by reviewing vendor performance expectations and documenting baseline performance results/evaluations informally prior to the formal requirement.

The City may wish to anticipate contracts with joint responsibilities and whether this impacts the process for evaluations.

Appendix A: Basis of findings rating and report classification

Finding rating matrix	Low Impact	Medium Impact	High Impact
Highly likely ● History of regular occurrence of the event. ● The event is expected to occur in most circumstances.	Moderate	Significant	Significant
Likely ● History of occasional occurrences of the event. ● The event could occur at some time.	Low	Moderate	Significant
Unlikely ● History of none or seldom occurrence of the event. ● The event may occur only in exceptional circumstances.	Low	Low	Moderate

Impact	Impact Consideration
High	**Financial impact** likely to exceed $250,000 in terms of direct loss or opportunity cost. **Internal Control:** Significant control weaknesses, which would lead to financial or fraud loss. **An issue that requires a significant amount of senior management/Board effort to manage such as:** ● Failure to meet key strategic objectives/major impact on strategy and objectives. ● Loss of ability to sustain ongoing operations: - Loss of key competitive advantage/opportunity - Loss of supply of key process inputs ● A major reputational sensitivity, e.g. market share, earnings per share, credibility with stakeholders and brand name/reputation building. **Legal/regulatory:** Large scale action, major breach of legislation with very significant financial or reputational consequences.
Medium	**Financial impact** likely to be between $75,000 to $250,000 in terms of direct loss or opportunity cost. **Internal Control:** Control weaknesses, which could result in potential loss resulting from inefficiencies, wastage, and cumbersome workflow procedures. **An issue that requires some amount of senior management/Board effort to manage such as**: ● No material or moderate impact on strategy and objectives. ● Disruption to normal operation with a limited effect on achievement of corporate strategy and objectives ● Moderate reputational sensitivity. **Legal/regulatory:** Regulatory breach with material financial consequences including fines.

Impact	**Impact Consideration**
Low	**Financial impact** likely to be less than $75,000 in terms of direct loss or opportunity cost. **Internal Control:** Control weaknesses, which could result in potential insignificant loss resulting from workflow and operational inefficiencies. **An issue that requires no or minimal amount of senior management/Board effort to manage such as:** ● Minimal impact on strategy ● Disruption to normal operations with no effect on achievement of corporate strategy and objectives ● Minimal reputational sensitivity. **Legal/Regulatory:** Regulatory breach with minimal consequences.

Audit report classification

Report Classification	The internal audit identified one or more of the following:
Optimally Controlled	• Well-structured design effectively achieves fit-for purpose control objectives • Controls consistently applied and operating at optimum level of effectiveness.
Managed	• Sound design achieves control objectives. • No control design improvements identified. • Controls consistently applied. • Only minor instances of controls identified as not operating, which have mitigating back-up controls or the risk of loss is immaterial. • All previous significant audit action items have been closed.
Some Improvement Opportunity	• Control design improvements identified, however, the risk of loss is immaterial. • Isolated or “one-off” significant controls identified as not operating for which sufficient mitigating back-up controls could not be identified. • Numerous instances of minor controls not operating for which sufficient mitigating back-up controls could not be identified. • Some previous significant audit action items have not been resolved on a timely basis.
Major Improvement Opportunity	• Design is not optimum and may put control objectives at risk. • Control design improvements identified to ensure that risk of material loss is minimized and functional objectives are met. • A number of significant controls identified as not operating for which sufficient mitigating backup controls could not be identified which may put control objectives at risk. • Losses have occurred as a result of control environment deficiencies. • Little action taken on previous significant audit findings to resolve the item on a timely basis.
Unacceptable Risk Exposure	• Control design leaves the opportunity for loss, error or abuse. • Significant control design improvements identified to ensure that the risk of material loss is minimized and functional objectives are met. • An unacceptable number of controls (including a selection of both significant and minor) identified as not operating for which sufficient mitigating back-up controls could not be identified creating the opportunity for loss, error or abuse. • Material losses have occurred as a result of control environment deficiencies. • Instances of fraud or significant contravention of corporate policy detected. • No action taken on previous significant audit findings to resolve the item on a timely basis.

Appendix B: Background, Scope and Objectives

Background

The Security Incident Prevention and Mitigation audit is based on the risks identified through the 2019-2020 City of Windsor Internal Audit Risk Assessment and Plan approved by the Corporate Services Standing Committee on May 6, 2019. This was a value protection audit where the IA addressed risks including: Vandalism, Public Facilities, Terrorism, Training and development, and physical security of facilities.

Scope

The scope of this internal audit included an assessment of the controls in effect as of December 2019.

Internal audit objectives

The focus of this internal audit was to provide a current state assessment of the design and operating effectiveness of controls management has implemented to achieve the following objectives related to Staff Safety Incident Prevention and Mitigation managed by the City:

- Resource allocation, and Safety program (including physical factors, safety apparatus and building floor plans) related decisions considering safety hazards and security needs.
- Security/safety incident monitoring occurs periodically including logging, defined categorization of incidents (e.g. by location), and reporting processes to facilitate timely and appropriate updates to Safety programs.
- Regular and relevant capacity building/training/awareness provided to exposed positions for responding to safety/security related concerns or priorities.

Specific scope exclusions

Given the nature of the work and budgeted effort, the following elements are explicitly excluded from the scope of this internal audit:

- Emotional or verbal abuse unless threat of security to staff, logical security and access controls
- Developing/executing Business Continuity and Disaster Recovery Plans
- Investigations and reporting of incidents at an incident level
- Enterprise wide risk assessment process
- Nuclear Safety and Control Act (federal)
- Municipal Evacuation Plan
- Hazard Prevention and Mitigation
- Normal occupational hazards

Appendix C: Limitations and responsibilities

Limitations inherent to the internal auditor's work

Internal control

Internal control systems, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgment in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

Future periods
Our assessment of controls is for the period specified only. Historic evaluation of effectiveness is not relevant to future periods due to the risk that:

- the design of controls may become inadequate because of changes in operating environment, law, regulation or other; or
- the degree of compliance with policies and procedures may deteriorate.

Responsibilities of management and internal auditors
It is management's responsibility to develop and maintain sound systems of risk management, internal control and governance and for the prevention and detection of irregularities and fraud. Internal audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems.

We endeavour to plan our work so that we have a reasonable expectation of detecting significant control weaknesses, and if detected, we shall carry out additional work directed towards identification of consequent fraud or other irregularities. However, internal audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected.

Accordingly, our examinations as internal auditors should not be relied upon solely to disclose fraud, defalcations or other irregularities which may exist.