Ottawa

Office of the Auditor General

Audit of Corporate Security

Tabled at Audit Committee
April 8, 2019

Table of Contents

Acknowledgements

The team responsible for this audit was comprised of Margaret Sue from the Office of the Auditor General (OAG) and Samson and Associates, under the supervision of Sonia Brennan, Deputy Auditor General and the direction of Ken Hughes, Auditor General. The team would like to thank those individuals who contributed to this project, and particularly, those who provided insights and comments as part of this audit.

Original signed by:

Auditor General

Executive summary

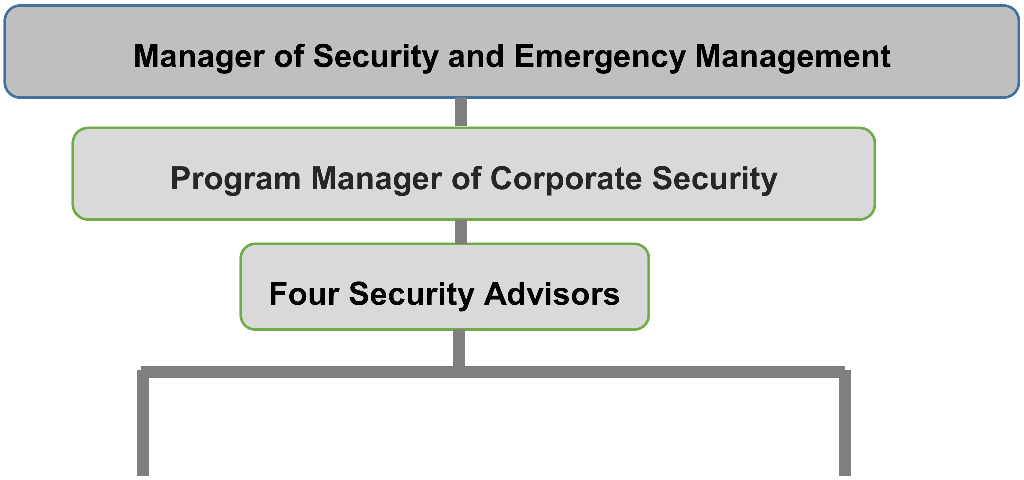
Purpose

The primary objective of the audit was to assess the efficiency and effectiveness of City operations related to Corporate Security. The audit evaluated the adequacy and effectiveness of the governance, internal controls and risk management practices related to physical security management. The Audit of Corporate Security was included in the 2017 Audit Plan of the Office of the Auditor General approved by City Council on December 14, 2016.

Background and rationale

The City of Ottawa's Corporate Security (CS) unit is responsible to provide a safe and secure workplace for City of Ottawa employees, volunteers, clients and assets through the delivery of security services. Sound governance, internal controls and risk management practices are essential to ensure appropriate physical security management. This includes incident management and investigations, event security planning, threat and risk assessments, and security system design, installation, management and monitoring.

The following chart has been developed to communicate the key services that Corporate Security oversees. The Program Manager of Corporate Security reports to the Manager of Security and Emergency Management (SEM). There are four full-time security advisors who report to the Program Manager of Corporate Security.



Manager of Security and Emergency Management

Program Manager of Corporate Security

Four Security Advisors

Done internally	**Contracted out externally**
• Security audits at City facilities to assess overall health of security equipment • Internal investigations resulting from a security incident or a fraud and waste case. The nature of the incident will dictate if it is investigated by a security advisor or outsourced. • Manage the service providers for contracted security guards ○ Provide and coordinate guard services for Council and Committee meetings, special events, security patrols, alarm response • Manage contracted security guards at the Security Operations Centre (SOC) and Photo ID Centre • Manage the design, installation and repair of access control equipment, surveillance systems, intrusion alarm systems, etc. • Provide advice and guidance on the design and construction of new builds or retrofits where the above equipment may be installed • Security education and training for City employees • Develop Security Operations plans for large-scale events	• The Security Operations Centre (SOC) monitors the City's Integrated Security Management System, 24 hours a day, 7 days a week and is the initial contact point for Corporate Security. The SOC is staffed by contracted personnel. The SOC handles: ○ Service requests to repair damaged security equipment ○ Alarm monitoring ○ Temporary door/gate access modifications • Facility security guards ○ Charged back to respective facility who utilizes their services • Photo ID Centre (contracted personnel) ○ Chargeback for creation of photo ID access cards for non-City employees • Mobile alarm response received by the SOC • Service provision for repair, maintenance and installation of equipment used in Integrated Security Management System (CCTV, Access Control, Intrusion System)

For 2016, CS had a budget of $1,990,000, of which $1,227,426 was allocated for purchased security services. Total overall purchases of security services amounted to approximately $2,500,000, with the balance of funds being recovered from other City client departments, primarily Recreation, Cultural and Facility Services Department.

The Corporate Security unit is comprised of the Program Manager of Corporate Security and four security advisors.

Findings

The audit focused on processes, practices and controls in four key areas, which were selected based on risk:

- Governance, roles and responsibilities;
- Physical security risk management processes and practices;
- Physical access to facilities, information and assets; and
- Employee awareness and compliance with policy and practices regarding physical security.

The key findings associated with each area are as follows:

1. A governance and organizational structure to support an effective security program has not been sufficiently developed and documented

We expected CS to have an established governance and organizational structure to support an effective security program with documented security policy, procedures and standards that are applied universally across the organization. Additionally, we expected that CS would present the Community and Protective Services Committee and Council with sufficient information to provide a complete picture of activities, incidents, achievements and outstanding risks, as well as the number of service requests received and processed.

Policy

A by-law of the City of Ottawa respecting the delegation of authority to various officers of the City delegates Security and Emergency Management (SEM) the authority to negotiate, approve, conclude, and execute agreements related to the provision of corporate security services. There is no substantive security related policy to assign responsibility and authority or provide a clear role and mandate for CS. Roles, responsibilities and accountabilities of key stakeholders are not well defined and communicated.

During the course of the audit, Security and Emergency Management engaged a consultant to conduct a benchmarking study of the corporate security function of selected major municipalities in Canada, and to compare the results with the Corporate Security unit of the City of Ottawa. A total of 10 municipalities responded. As stated in the *Security and Emergency Management Corporate Security Benchmarking Study, (the Study)*, Toronto, York and Vancouver have adopted comprehensive corporate security policies.

The Study states that in general Ottawa has significant policy gaps relative to the other municipalities. All other municipalities contacted have developed some security related policies, with photo ID policies in place everywhere except Ottawa and one other municipality. Ottawa also lacks an overarching Corporate Security Policy and a Physical Security Policy.

CS plans

While CS plans have clear objectives, they do not address the scope of services one would expect to see. Plans do not address known security risks or address strategies, goals, objectives and timelines for addressing those risks.

Reporting

Regular reporting to oversight bodies is important to ensure that key decision makers and those responsible for governance are aware of their risks and play a part in accepting or addressing known risks. Information provided to Community and Protective Services Committee and Council is limited to the annual report. This report is very high level and does not permit Committee and Council to appreciate the scope of work carried out by CS, the number of incidents documented within the City, the work left undone, such as security audits and the absence of on-site visits. CS activities and highlights should be provided to the Community and Protective Services Committee and Council, including trends and problem facilities that may warrant more attention from CS.

When requested for support, CS participates in the conduct of fraud and waste investigations within the City through providing camera footage, access card history or other information. External investigative services are utilized to investigate labour relations cases where surveillance of an employee is warranted. The results of these supporting services are forwarded to the originating City department and Labour Relations for inclusion in the investigation report and for final action. However, security risks, incidents and the number of investigations supported are not routinely reported to the Community and Protective Services Committee.

2. Physical security risk management processes and practices are in place

There are several risk management processes and practices established within CS, including monitoring and responding to alarms in a timely fashion, providing additional security for high profile Council meetings and performing threat assessments for major events.

Alarms

Alarms come into the Security Operations Centre (SOC) in real time, and the SOC is staffed 24/7. The SOC receives approximately 1,000 alarms per month.

When an alarm is received at the SOC, staff verify the alarm and mobile patrol will be dispatched if necessary.

Duress alarms are personal alarms used by individuals in vulnerable situations such as reception counters, client service centres, lone worker situations, Ottawa Public Library, sexual health centre). They are treated as “life safety events”, and the SOC will make one attempt to contact the site by phone to verify the alarm, then will immediately contact Ottawa Police Service (OPS).

Our testing found that all of the alarms were satisfactorily resolved in a timely manner.

Although the number of false alarms had been greatly reduced, it was still high. Corporate Security did not differentiate alarms by cause/type until late 2016. From January 1 to October 31, 2017, of 1,669 mobile patrols dispatched, in 1,421 cases, or roughly 85 per cent of the time, the alarm was false. Each dispatch of the mobile patrol costs $40, which amounts to almost $57,000 for false alarms in the 10-month period noted.

We contacted three other municipalities (Mississauga, Hamilton and Vancouver) who advised that they had similar problems with high rates of false alarms, primarily due to propping of doors for convenience.

Security Operations Centre

CS has a primary and an alternate SOC facility capable of coordinating and sustaining response to emergency situations. However, the CS Emergency Operations Plan (EOP) to identify areas of responsibility in an emergency or disaster and Continuity of

Operations Plans (COOP) to describe how essential functions will be continued and recovered are only in draft state.

Major event security

The City has established procedures for major event threat assessments. These are conducted by the Special Events Advisory Team (SEAT), guided by the 2013 Special Events By-law. SEAT reviews events that are outdoors where 500+ people are present at any given time considering factors such as the political environment, number of attendees expected, sale of alcohol, etc. SEAT develops requirements of the event organizer and coordinates the city services response in support of event operations. CS is involved in the review and assessment of any event at a City of Ottawa location.

To ensure the safety and security of staff and facilities, when there are events that may draw protesters or special meetings of Council, OPS is requested to provide an officer on site or is provided with “situational awareness” so that they can be on standby.

3. Systems and processes are in place to limit access to City facilities, to appropriate and approved individuals: however, more oversight is required

CS uses several tools and practices to control physical access to facilities, information and assets. These include issuance of approved access cards, conducting facility security audits, the use of security guards, cameras and electronic security standards.

Access cards

The primary means to limit access to City facilities is the issuance of an approved access card. Changes need to be made to current processes to ensure CS has oversight of the ID access card issuance process and that the termination of ID access cards are performed in a timely manner.

Responsibility for issuing access rights falls primarily on a single contracted commissionaire, acting as the photo ID clerk with little oversight. Given the high turnover in this position, it is important for CS to exercise oversight.

Of the contractor and volunteer access cards sampled, none had expiration dates programmed. Seasonal workers and student access cards are often not cancelled until months after termination. In 4 out of the 10 of the sampled terminations, the time between the retirement/termination date and the cancellation of the ID access card was greater than five weeks.

We found that a secured file room door that required dual authentication (an access card as well as a PIN code) allowed unauthorized persons access. In comparison, for the IT data centres, access readers have automated monthly reports generated showing staff that have access, and any staff that should not have access are removed. This would be a good practice for CS to adopt.

Security audits

Security audits are undertaken to ensure the physical security of persons and assets at City sites by proactively identifying security risks and threats to develop a remedial action plan to address them. The City has only performed security audits on 72 out of a total of 836 City of Ottawa buildings in the last nine years (9 per cent). There is no risk-based process to select priority facilities for security audits. CS only performs security audits at the request of facility and departmental managers.

In September 2017, CS conducted a Threat and Risk Assessment (TRA) for City Hall: *Security Enhancements, Safeguarding Against Vehicular Threats*. The identified risks will be appropriately addressed once the measures identified have been fully implemented. The audit noted that one risk area was not considered. CS advised that this risk area will be reviewed in 2019 to assess the remaining threats in order to develop remedial security measures to reduce the risk to the facility and its occupants.

For the few security audits conducted, there is no requirement for departments to implement the recommendations; and it is up to departments to pay for installing any equipment recommended. Unaddressed risks should be documented, escalated and accepted or rejected at an appropriate level of authority. In addition, CS needs to develop criteria for determining which facilities should be subject to security audits, with risk being the primary criteria.

CCTV cameras, SOC and guards

We conducted unannounced site visits at three works yards. There were sufficient CCTV cameras in evidence, lighting was sufficient and fences were in good condition. At one site, City vehicles were not locked, and keys were found in the ignition of one of three trucks examined.

Other means to limit access to City facilities are the use of guards, cameras and electronic security equipment standards.

Guard services are contracted to staff the SOC, provide facility security, mobile security response and issue access cards.

The SOC is staffed by two contracted personnel 24/7, and there are well-documented operating procedures in place. There is also a back-up SOC in place. Both sites were well organized, equipped and operated.

Guard services are contracted to provide mobile security response and alarm investigation to all City sites 24 hours a day, 7 days a week. The City has also engaged a contractor to provide guard services at the three major administrative buildings: City Hall, Ben Franklin Place and 100 Constellation, and there are good Standard Operating Procedures for each facility.

For contracted guard staff, there are documented problems with turnover and a lack of bilingual capacity. The guard staff at City Hall appears low in the off hours even after going to three, based on the size of the facility.

A City staffed guard service would be preferable, so there would be a dedicated team of professional security officers to be developed and trained for future requirements. City staff would be especially beneficial to provide key front-line security functions e.g. Security Operations Centre staff, photo ID clerk and security guards, particularly at City Hall.

There are approximately 1,200 cameras installed at City facilities (~130 at City Hall). They are for motion detection and not identification and prevention; although, they do act as a deterrent. CS was allocated $350,000 per year for four years for camera upgrades; and at the end of the initiative in 2018, approximately 90 per cent of cameras will have been upgraded.

Our testing determined that cameras provide adequate coverage of key areas of most major facilities. Images were good enough for a general view, but it would be difficult to confirm facial identity.

During our audit work in December 2017, we examined camera views at four locations; Walter Baker Sports Complex, Ottawa Public Library Main Branch, Cyrville Road Elections Office and Champagne Fitness Centre. Of the four client counters where cash handling occurs, the camera views were not clear enough to assess the actual cash handling. However, it is important to note that the volume or value of transactions processed at the client counters may not necessitate high-resolution cameras.

As a result of the Investigation into Three Reported Client Service Centres Deposit Shortages, Tabled at Audit Committee – June 22, 2017, CS responded to the two camera related recommendations. CS updated the quality and angles of security video cameras at the client service centres to ensure deposit preparation is recorded and details can be seen including denominations of notes.

It would still be beneficial to develop a risk-based plan to upgrade cameras in any remaining cash handling areas.

CS has developed electronic security equipment standards for facilities, similar to physical security standards. However, CS cannot compel branches to implement the standards; they can only recommend, as there is no policy to support their authority.

4. While CS has developed a Protective Measures Program (PMP), more work is necessary to ensure individual City facilities implement the program and that staff receive more training related to their security obligations

Auditors expected to find that City employees were aware of the PMP and that a plan was in place for implementation across all City facilities.

In 2013, challenges with regards to warden[1] recruitment, retention and training were identified. Consequently, the City moved from a volunteer-based program for building evacuations to a self-serve program to eliminate the requirement for the Emergency Warden Program.

On October 22, 2014, a series of shootings occurred at the Canadian National War Memorial and Parliament Hill. City Hall was placed in Secure Facility status while police searched for the shooter. An ‘After Action Review’ report examining the City of Ottawa’s response recommended that the City establish formal procedures for threats requiring enhanced security measures.

The PMP defines the following protective measures, as per a best practice review:

- Building Evacuation;
- Shelter in Place;
- Secure Facility and
- Lockdown.

The new PMP policy has been posted on Ozone (the City’s intranet) and communicated to City employees via email. PMP e-training is available on Ozone; however, it is not mandatory for staff.

[1] Wardens were the volunteer staff at a facility who aided and ensured that other staff exited the facility in the event of a fire or other emergency.

The PMP is comprehensive, and the three major administrative buildings have successfully implemented PMP. However, there is currently no schedule to target when each individual City facility plans to implement PMP.

Auditors also expected to find that City employees are occasionally made aware of their requirements in relation to compliance with policies and practices regarding physical security.

As part of orientation for new staff, there is a presentation that includes three slides on general corporate security, security and emergency management and safety in the workplace.

For the three municipalities we contacted (Mississauga, Hamilton and Vancouver), none provides significant security related information to new hires at orientation.

Conclusion

Corporate Security generally makes good use of tools and practices to limit access to facilities to appropriate, approved individuals and facilities and assets are protected through the utilization and implementation of physical security measures.

One area of significant risk identified by this audit are the processes and controls over access card termination. The weaknesses identified require prompt attention from management.

Other areas where improvement is needed includes the development of a Corporate Security Policy, as well as, more substantial planning and objective setting for Corporate Security. With respect to security audits, coverage of risk and follow through is not currently robust. In addition, there needs to be more comprehensive reporting to the Community and Protective Services Committee and Council on all security related activities, especially for unmitigated risks identified.

The City meets many expectations in relation to physical security risk management processes and practices. However, we identified room for improvement regarding formal documentation related to Business Continuity and Disaster Recovery Plans.

We found that the Protective Measures Program is comprehensive and has been implemented at the City’s three major administrative sites. However, there is no plan to ensure its implementation at remaining City facilities. Additionally, there are improvements required to ensure employees receive sufficient training to ensure they are aware of their requirements in relation to compliance with policies and practices regarding physical security.

Recommendations and responses

Recommendation #1

That Corporate Security develop security policy, procedures and standards for universal application across the City. The policy should include clear roles, responsibilities and accountabilities for Corporate Security.

Management response:

Management agrees with this recommendation.

Development of the security policy, procedures and standards is included in the 2019 Corporate Security work plan and, given the scope of work, will be completed by no later than Q2 2020.

Recommendation #2

That Corporate Security provide the Community and Protective Services Committee and Council with sufficient information to provide a complete picture of activities, incidents, achievements, trends and outstanding risks as well as the number of service requests received and processed.

Management response:

Management agrees with this recommendation.

Additional information will be included as part of the 2018 Security and Emergency Management Annual Report, which is expected to be tabled at the Community and Protective Services Committee in Q2 2019, and in subsequent Annual Reports thereafter.

Recommendation #3

That Corporate Security develop risk-based plans necessary to ensure sufficient security related work such as facility security audits and site visits, inclusive of required funding and the impact of not proceeding, for presentation to management and Council. The plans should identify the higher risk activities not conducted currently to meet minimum expectations.

Management response:

Management agrees with this recommendation.

A feasibility review is underway as part of the ongoing Security and Emergency Management Service Review, which is expected to be tabled in Q2 2019. Any funding and/or resource implications resulting from this review will be identified for inclusion in the 2020 draft budget process for consideration.

Recommendation #4

That Corporate Security analyse false alarms on a regular basis and consider implementing a chargeback to facilities with disproportionate false alarms in order to further reduce their frequency and the unnecessary work in the Security Operations Centre (SOC) and wasted resources on unnecessarily dispatching mobile patrols.

Management response:

Management agrees with this recommendation.

Corporate Security is actively working with client groups, collecting metrics and providing reports to select client groups to action security-related trends in their respective areas. Corporate Security will consider the effectiveness and implementation of a chargeback to facilities by Q3 2019.

Recommendation #5

That Corporate Security work with the Office of the City Clerk and Solicitor to review the current practices, develop and document guidelines for the augmentation of security for high profile Council meetings.

Management response:

Management agrees with this recommendation.

Corporate Security has reviewed current practices and provided feedback for the Office of the City Clerk and Solicitor’s consideration. The completion of a revised guideline is expected by the end of Q2 2019.

Recommendation #6

That Corporate Security complete the Business Continuity and Disaster Recovery Plans and a Security Emergency Plan for implementation in 2019.

Management response:

Management agrees with this recommendation and it has been implemented.

The Security and Emergency Management Emergency Plan and the Security and Emergency Management Continuity of Operations Plans were completed as part of the Office of Emergency Management's re-accreditation process in 2018.

Recommendation #7

That Corporate Security improve control over the ID card and access control systems to create an effective tool for recording who, when and for how long access was granted by:

- Programming standardized fields into the system to enable future searches.
- Conducting spot checks to monitor and ensure that the photo ID clerk is verifying the delegated authority.
- Amending the Photo ID Card Policy and Procedures to require the delegated authority to provide a termination date for contractors, volunteers and seasonal employees.
- Annually initiating a risk-based review of access to doors to ensure that the list of people who have access is appropriate.
- Ensure notifications of termination are processed by Corporate Security in a timely manner.
- When an access card is terminated, removing all the individual access points the individual previously had access to. This should also be formalized in the Photo ID Card Policy and Procedures.

Management response:

Management agrees with this recommendation.

The standardization of fields and amendments to the Photo ID Card Policy and Procedures, as described in the recommendation, are complete. Additional resources are required to action the remaining Photo ID items. Two (2) additional FTEs have been included in the 2019 draft budget for consideration by Council.

Recommendation #8

That Corporate Security review the outstanding threats not addressed in the City Hall TRA and develop mitigation measures in order to address the risks identified.

Management response:

Management agrees with this recommendation.

A business case is in development for the procurement of a consultant in Q2 2019, subject to approval, to address these threats and to propose mitigation measures.

Recommendation #9

That Corporate Security develop a policy to ensure that recommendations emanating from facility security audits be subject to implementation.

Management response:

Management agrees with this recommendation.

Development of the policy is included in the 2019 Corporate Security work plan and, given the scope of work, will be completed by no later than Q2 2020.

Recommendation #10

That Corporate Security develop plans for risk-based, cyclical, security audits at City facilities and security awareness refresher training at yards.

Management response:

Management agrees with this recommendation.

A feasibility review is underway as part of the ongoing Security and Emergency Management Service Review, which is expected to be tabled in Q2 2019. Any funding and/or resource implications resulting from this review will be identified for inclusion in the 2020 draft budget process for consideration.

Recommendation #11

That Corporate Security work with Supply Services to ensure that low price is not the sole basis for awarding guard contracts in order to improve overall quality of service and public impression.

Management response:

Management agrees with this recommendation and it has been implemented.

Corporate Security issued one security guard contract in 2018 and the basis of selection was best value, not lowest price. Three additional security guard solicitations are under development for 2019, each of which will also be awarded on the basis of best value.

Recommendation #12

That the City validate the current outsourcing of Corporate Security functions by preparing a business case with all alternatives identified, costed, analyzed and compared with a resulting supported recommendation. Such an evaluation would address the potential introduction of proprietary (in-house) guard staff for high-risk activities such as City Hall facility security, ID card issuance and Security Operations Centre staffing.

Management response:

Management agrees with this recommendation.

The recommended analysis is underway as part of the ongoing Security and Emergency Management Service Review, which is expected to be tabled in Q2 2019. Some of the analysis respecting ID card issuance specifically, has been completed and two (2) additional FTEs to bring these services in-house, have been included in the 2019 draft budget for consideration by Council. Any remaining funding and/or resource implications resulting from the broader analysis will be identified for inclusion in the 2020 draft budget process for consideration.

Recommendation #13

That Corporate Security develop a risk-based plan to upgrade cameras in any remaining cash handling areas and upgrade bandwidth to improve image quality.

Management response:

Management agrees with this recommendation.

Corporate Security will consult Corporate Services to determine the risk tolerance in any remaining cash handling areas and if any camera upgrades are required. Given the number of site visits and risk assessments that are required, this will be completed by Q4 2019.

Recommendation #14

That the City identify a senior manager (member of the executive) to “Champion” security within the organization by demonstrating management’s commitment to security. Someone who will foster security awareness amongst employees at all levels and raise the profile of security across the entire organization and help ensure that all major initiatives are considered through the lens of security.

Management response:

Management agrees with this recommendation and it has been implemented.

The General Manager of Emergency and Protective Services has been designated as the security champion, in collaboration with all members of the Senior Leadership Team.

Recommendation #15

That Corporate Security develop requirements to provide adequate information for new employee orientation to raise awareness of obligations related to security at the City, followed up with a mandatory webinar and testing within 30 days with the City.

Management response:

Management agrees with this recommendation.

Additional security-related information has already been added to new employee orientation. Corporate Security will work with the Service Innovation and Performance Department on the development of a webinar and testing no later than Q4 2019. The rollout of the eLearning module to staff will be determined at that time, based on capacity.

Recommendation #16

That Corporate Security develop a risk-based plan to monitor and ensure that a Protective Measures Program is developed by all City facilities.

Management response:

Management agrees with this recommendation.

The Protective Measures Program has been implemented and its rollout to all facilities is ongoing, based on risk. Full implementation of the recommendation would expand the scope of services offered by Corporate Security and will be considered in the context of the ongoing Security and Emergency Management Service Review, which is expected to be tabled in Q2 2019. Any funding and/or resource implications resulting from this review will be identified for inclusion in the 2020 draft budget process for consideration.

Recommendation #17

That Corporate Security develop a strategy to encourage City staff to take the online training related to the Protective Measures Program processes.

Management response:

Management agrees with this recommendation. A strategy will be completed by Q4 2019.

Detailed audit report

Audit of Corporate Security

Introduction

The primary objective of the audit was to assess the efficiency and effectiveness of City operations related to Corporate Security. The audit evaluated the adequacy and effectiveness of the governance, internal controls and risk management practices related to physical security management. The Audit of Corporate Security was included in the 2017 Audit Plan of the Office of the Auditor General approved by City Council on December 14, 2016.

Background and context

The Office of the Auditor General (OAG) conducted an Audit of Corporate Security to address both the efficiency and effectiveness of City operations. It assessed the adequacy and effectiveness of the governance, internal controls and risk management practices related to physical security management.

The City's Security and Emergency Management branch is responsible for ensuring a secure environment and leads the city services and residents in preventing, preparing, responding and recovering from major emergencies and events.

The Security and Emergency Management branch is comprised of two units – the Office of Emergency Management and the Corporate Security unit. Security and Emergency Management (SEM) Systems and Coordination and Corporate Security (CS) are independent parts of the Security and Emergency Management branch. The work of Security and Emergency Management Systems and Coordination and Corporate Security is complimentary and closely linked.

The CS unit is responsible to provide a safe and secure workplace for City employees, volunteers and clients. CS provides a range of services as described below.

Corporate Security services

Security Operations Centre: The Security Operations Centre (SOC) is responsible for monitoring the City's Integrated Security Management System, 24 hours a day, 7 days a week and is the initial contact point for Corporate Security services.

The SOC provides these additional services:

- Information intake and coordination of service requests to repair damaged security equipment (note: Corporate Security provides a coordination function with respect to service requests and only makes repairs for emergency requests);
- Temporary door/gate access modifications; and
- Access control and alarm monitoring.

Security advisors: Security advisors are available to assist departments with their individual security needs, such as general and specific security education and training for City employees.

Event security planning:

- Develops security operations plans for large-scale events; and
- Provision and coordination of guard services for Council and Committee meetings, special events, security patrols and alarm response.

Internal investigations: Internal investigations resulting from a security incident or a fraud and waste complaint.

Security audits: Security audits assess the physical security of persons and assets at City facilities. The security audit's aim is to identify and evaluate security risks and to develop a remedial action plan. Security audits are conducted using Crime Prevention through Environmental Design (CPTED) principles.

Electronic Security System design and installation:

- Provision of advice and guidance on the design and construction of new builds or retrofits;
- Overall management of the installation or repair of access control equipment, surveillance systems and intrusion alarm systems; and
- Site audits to assess overall health of security equipment.

Audit objectives and criteria

The primary objective of the audit was to assess the efficiency and effectiveness of the Corporate Security function within the City. The audit assessed the adequacy and effectiveness of the governance, internal controls and risk management practices related to physical security management.

The audit criteria were developed based on information gathered and analysed during the audit planning phase as well as document review and research. We were guided where appropriate by the Government of Canada Policy on Government Security, the RCMP Operational Security Standard on Physical Security and the associated RCMP Guide G1-025, Protection, Detection and Response. In addition, we relied on industry best practices and industry knowledge.

As part of the review and analysis, the audit team utilized the services of a subject matter expert (SME). The SME is a former senior manager and Departmental Security Officer of the Canadian Security Intelligence Service with over 40 years of experience. In that capacity, he directed the integrated Corporate Security Program that included physical, personnel and IT security. He is currently involved as a consultant in a number of security program reviews, audits and sensitive administrative investigations within the Government of Canada and the private sector. Our SME is a long-standing member of the American Society for Industrial Security (ASIS).

The audit objectives and criteria included:

Audit objective #1

A governance and organizational structure to support an effective security program is defined and communicated.

Criteria:

- Roles, responsibilities and accountabilities of key stakeholders are well defined and communicated
- Corporate Security's plans have clear objectives that are aligned with corporate policies and established priorities
- The security program is monitored, assessed and reported on to measure progress toward achieving expected results. Committee and Council receive sufficient information to support decision making.
- Security risks, incidents and investigations are reported to senior management, analyzed and action taken to address the risks

Audit objective #2

Physical security risk management processes and practices are in place.

Criteria:

- Appropriate active monitoring processes and procedures are implemented, and alarms are logged and addressed in a timely fashion
- Mechanisms are in place to ensure the provision and coordination of appropriate security for Council, Committee meetings and special events
- Security advisors are available to assist departments to determine their individual security needs and develop risk mitigation plans and measures
- An effective Business Continuity and Disaster Recovery Plan have been developed to provide for the continuity of critical business operations and services within Corporate Security

Audit objective #3

Physical access to facilities and assets is managed on an as needed basis.

Criteria:

- Security limits access to facilities to appropriate and approved individuals in accordance with policy and instructions from managers
- Threat and risk assessments are conducted based on a risk-based plan or process
- Facilities and assets are protected through the utilization implementation of appropriate physical security measures

Audit objective #4

Security awareness and training are provided to ensure that employees understand and comply with their responsibilities and do not inadvertently compromise security.

Criteria:

- The Protective Measures Program (PMP) is comprehensive, appropriately resourced and on schedule
- Security specialists receive effective and timely security training and professional development

- Employees are aware of their requirements in relation to compliance with policies and practices regarding physical security

Scope

The focus of this audit was to examine Corporate Security's roles and responsibilities related to physical security risk management.

The audit period was from January 1, 2016 to November 30, 2017.

Out of scope items

The scope of this audit excluded Emergency Management other than any direct aspects, which affect Corporate Security as well as the security of information management and information technology. OC Transpo is also out of scope as they are responsible for their own security services through their Special Constables program. OC Transpo uses the same Kantech system, but has their own photo ID clerk who is responsible for issuing Transit's access cards.

Audit approach and methodology

The audit work in this report was conducted in accordance with the OAG Audit Standards. While the OAG adopts these standards as the minimum requirement for our audits, we also draw upon the standards and practices of the Institute of Internal Auditors.

As part of our regular audit process, we obtained management's agreement with the findings in this report.

The audit methodology included the following activities:

- Interviews with staff and managers of Corporate Security and those to whom Corporate Security provides services;
- Review of documentation relevant to the audit scope areas;
- Analysis and testing of audit evidence; and
- Obtaining insight and analysis from the SME.

Audit observations and recommendations

Audit objective #1

A governance and organizational structure to support an effective security program has not been sufficiently developed and documented.

We expected CS to have an established governance and organizational structure to support an effective security program. This would include having security policy, procedures and standards that are applied universally across the organization with the expectation that there will be uniform compliance. Established and required security training for new hires as well as for newly implemented security programs such as the Protective Measures Program are other important program elements that were examined.

We also expected that CS would present the Community and Protective Services Committee and Council with sufficient information to provide a complete picture of activities, incidents, achievements and outstanding risks as well as the number of service requests received and processed.

Policy

The audit found that there is no security related policy to assign authority and responsibilities and provide a clear role and mandate for CS. We found that roles, responsibilities and accountabilities of key stakeholders are not well defined and communicated. This is important in order to have all staff and managers aware of their roles in identifying, reporting and addressing security incidents and risks. Policy should also provide examples of behaviours that are unacceptable.

There is little legislation in place to provide guidance in establishing a strategic and operational framework for CS. Unlike the Ontario Emergency Management and Civil Protection Act, which provides detailed requirements to address, there is no specific mention of CS in any legislation we could identify.

A by-law of the City of Ottawa respecting the delegation of authority to various officers of the City delegates Security and Emergency Management (SEM) the authority to negotiate, approve, conclude and execute agreements related to the provision of corporate security services. This includes incident management and investigations, event security planning, threat and risk assessments, and security system design, installation, management and monitoring.

During the course of the audit, Security and Emergency Management engaged a consultant to conduct a benchmarking study of the corporate security function of selected major municipalities in Canada, and to compare the results with the Corporate Security unit of the City of Ottawa. A total of 10 municipalities responded. As stated in the *Security and Emergency Management Corporate Security Benchmarking Study*, (*the Study*), only Toronto, York and Vancouver have adopted comprehensive corporate security policies. All other municipalities contacted have developed some security related policies, with Photo ID policies in place everywhere except Ottawa and one other municipality. *The Study* states that in general, Ottawa has significant policy gaps relative to the other municipalities, for example, the lack of a Corporate Security Policy and a Photo ID Policy among others.

CS plans

While CS plans have clear objectives that are aligned with corporate priorities such as the development of a Protective Measures Program and a sustainable service delivery model, they do not adequately address the scope of services. Plans do not address known security risks or address strategies, goals, objectives and timelines for addressing those risks. There are no plans related to performing security audits, conducting announced and unannounced site visits, training for new hires and refresher training to aid in raising security awareness and operational integrity.

Reporting

Regular reporting to oversight bodies is important to ensure that key decision makers and those responsible for governance are aware of their risks and play a part in accepting or addressing those risks. Information provided to Community and Protective Services Committee and Council is through the Annual Report. This Report is very high level and does not permit Committee and Council to appreciate the scope of work and incidents documented within the City. Nor does it inform them about that work left undone, such as security audits and the absence of on-site visits. Senior management may not be aware of all security related activities, gaps and requirements. *The Study* did not address reporting to Council; however, we contacted three of the respondents (Mississauga, Hamilton and Vancouver). Like Ottawa, none of the three municipalities contacted routinely report to their respective Committees or Council other than through their annual reports, and there is no regular reporting of CS activities or metrics.

There is an incident reporting capacity through the Marval software database for tickets related to requests for services for security advisors. Information is available on many activities. The sample information below is from January 1, 2016 to October 31, 2017. A more complete sample of available information is outlined in Appendix A.

Table 1: Sample data available from Corporate Security - January 1, 2016 to October 31, 2017

Activity	**Number**
CCTV footage requests	258
Duress alarms	18
Break and enter	12
Trespassing	11
Vandalism	53
Fraud and waste investigations	18

Useful information that should be provided to the Community and Protective Services Committee are the number of false alarms, incidents turned over to OPS, trends and facilities with a high number of incidents and/or alarms that may warrant more attention from CS.

When requested for support, CS participates in the conduct of fraud and waste investigations within the City through providing camera footage, access card history or other information. External investigative services are utilized to investigate labour relations cases where surveillance of an employee is warranted. The results of these supporting services are forwarded to the originating City department and Labour Relations for inclusion in the investigation report and for final action. However, security risks, incidents and the number of investigations supported are not routinely reported to the Community and Protective Services Committee.

Recommendation #1

> That Corporate Security develop security policy, procedures and standards for universal application across the City. The policy should include clear roles, responsibilities and accountabilities for Corporate Security.

Management response:

Management agrees with this recommendation.

Development of the security policy, procedures and standards is included in the 2019 Corporate Security work plan and, given the scope of work, will be completed by no later than Q2 2020.

Recommendation #2

That Corporate Security provide the Community and Protective Services Committee and Council with sufficient information to provide a complete picture of activities, incidents, achievements, trends and outstanding risks as well as the number of service requests received and processed.

Management response:

Management agrees with this recommendation.

Additional information will be included as part of the 2018 Security and Emergency Management Annual Report, which is expected to be tabled at the Community and Protective Services Committee in Q2 2019, and in subsequent Annual Reports thereafter.

Recommendation #3

That Corporate Security develop risk-based plans necessary to ensure sufficient security related work such as facility security audits and site visits, inclusive of required funding and the impact of not proceeding, for presentation to management and Council. The plans should identify the higher risk activities not conducted currently to meet minimum expectations.

Management response:

Management agrees with this recommendation.

A feasibility review is underway as part of the ongoing Security and Emergency Management Service Review, which is expected to be tabled in Q2 2019. Any funding and/or resource implications resulting from this review will be identified for inclusion in the 2020 draft budget process for consideration.

Audit objective #2

Physical security risk management processes and practices are in place.

We found that the Security Operations Centre (SOC) has appropriate active monitoring processes, and procedures are in place to signal that an actual or attempted unauthorized access has occurred. This includes real time access to the City’s 800 cameras and 24/7 alarm monitoring. The audit also found that alarms are logged and satisfactorily addressed in a timely fashion.

Alarms

The SOC receives approximately 1,000 alarms per month.

When an alarm is received at the SOC, staff will determine the site and intrusion code, call the site and verify the alarm. If nobody answers, mobile patrol will be dispatched.

Duress alarms are personal alarms used by individuals in vulnerable situations to ensure their security and safety. They are silent alarms used when it may not be safe to call 9-1-1. Duress alarms (found at reception counters, client service centres, lone worker situations, Ottawa Public Library, sexual health centre), are treated as “life safety events” and the SOC will make one attempt to contact the site by phone to verify the alarm, then will immediately contact Ottawa Police Service (OPS).

In order to validate the response and resolution of alarms, we conducted two tests – one for those resolved without the use of mobile response and one test for alarms involving mobile response. All of the alarms tested were satisfactorily resolved in a timely manner.

Auditors did note that although the number of false alarms had been greatly reduced, it was still high. Corporate Security did not differentiate alarms by cause/type until late 2016. The Alarm Dispatch Summary from January 1 to October 31, 2017 notes that of 1,669 situations where there was a mobile patrol sent out, in 1,421 cases, or roughly 85 per cent of the time, it was a false alarm. Each dispatch of the mobile patrol costs $40, which amounts to almost $57,000 for false alarms in the 10-month period noted.

Table 2: Total number of alarms from 2015 to 2017

Year	Total number of alarms
2015	19,452
2016	13,650
2017	10,631

We contacted three other municipalities (Mississauga, Hamilton and Vancouver), who advised that they had similar problems with high rates of false alarms, hundreds per week, primarily due to propping of doors for convenience, adjustments to schedule needed and community users not always familiar with security coding requirements.

Recommendation #4

> That Corporate Security analyse false alarms on a regular basis and consider implementing a chargeback to facilities with disproportionate false alarms in order to further reduce their frequency and the unnecessary work in the Security Operations Centre (SOC) and wasted resources on unnecessarily dispatching mobile patrols.

Management response:

> Management agrees with this recommendation.
>
> Corporate Security is actively working with client groups, collecting metrics and providing reports to select client groups to action security-related trends in their respective areas. Corporate Security will consider the effectiveness and implementation of a chargeback to facilities by Q3 2019.

Council security

The audit found that mechanisms are in place to ensure the provision and coordination of appropriate security for Council, Committee meetings and special events.

To ensure the safety and security of staff and facilities, CS will arrange for additional contract security guards to be on site at City Hall when there are events being held that may potentially draw protesters. When there are special meetings of Council (ex. Uber and move of Salvation Army), Ottawa Police Service is requested to provide an officer on-site or is provided with “situational awareness” so that they can be on standby. When contentious or high profile issues are on Council's agenda, CS is forewarned by the City Clerk's office.

Concerns have been raised regarding security for Council meetings because of the close proximity of the public. We contacted three other municipalities (Mississauga, Hamilton and Vancouver), who advised that there is no screening of the public before their respective Council meetings. However, they do have extra guards on hand, one has a half height glass barrier between Council and the audience, and one does not permit large bags and can direct audience members to a secondary viewing area. *The Study* noted that Toronto and Winnipeg do bag checks for Council meetings, Calgary and Edmonton do bag checks and use metal detectors for Council meetings, and Calgary uses both for Committee meetings as well.

Criteria for the type and level of screening for City Council and Committee meetings should be developed by CS and presented to the Community and Protective Services Committee for consideration.

Recommendation #5

> That Corporate Security work with the Office of the City Clerk and Solicitor to review the current practices, develop and document guidelines for the augmentation of security for high profile Council meetings.

Management response:

> Management agrees with this recommendation.
>
> Corporate Security has reviewed current practices and provided feedback for the Office of the City Clerk and Solicitor's consideration. The completion of a revised guideline is expected by the end of Q2 2019.

Event Security

The audit did find that the City has a well-documented process to ensure that threat assessments are conducted for major events. For special events (a fair or festival, a social, recreational, educational, community or similar event that is occurring outdoors having an expected attendance of at least 500 persons at any one time during the event), the 2013 Special Events By-law sets out the Terms of Reference for the "Special Events Advisory Team" (SEAT), comprised of City staff and external participants, that provides recommendations regarding applications for special events.

SEAT considers factors such as the political environment, number of attendees expected, sale of alcohol, etc. SEAT reviews event plans, develops requirements of the event organizer, provides feedback and coordinates the city services response in support of event operations. CS is involved in the review and assessment of any event at a City of Ottawa location, Marion Dewar Plaza for example.

Private events on City facilities such as Rib Fest and South Asian Fest arrange their own security, but plans are reviewed by SEAT to ensure compliance with by-law requirements.

Security advisors

Security advisors are available to assist departments to determine their individual security needs and develop risk mitigation plans and measures. However, there is no requirement for departments to implement recommendations of the security advisors; and it is up to the departments to pay for installing any equipment recommended.

CS has four security advisors (client advisors). Two client advisors do internal investigations (requests come in through fraud and waste cases, Labour Relations and management). Contracted service providers are brought in to do investigations if surveillance is required. One advisor looks after contract services (guard management strategy), and there is one technical security advisor (expert in security systems).

When personal belongings are stolen on City property, it is a police matter as it is not City assets, and it is therefore reported to OPS for follow up. Theft of personal belongings (non-City property) must be reported to police by the victim directly at their own discretion; therefore, CS is not always aware of whether the report was made or not. The CS Marval database indicates there were approximately 260 incidents indicated as reported to police from January 1, 2016 to October 31, 2017. CS does not actively track whether or not they interacted further with OPS in relation to the reported incidents.

CS also provides employee education sessions when it is requested by the client. Training consists of general security awareness, but there is no formal policy or process to ensure new hires are familiarized with their obligations related to security within the City. The training provided does not address the day-to-day safety/security obligations of managers and employees; much of it is related to being generally aware of what is going on in your environment.

Business Continuity and Disaster Recovery Plans

We expected to find that CS would be in compliance with the City of Ottawa Business Continuity and Disaster Recovery Plan requirement that “Each department within the City is responsible for their individual emergency plans, inclusive of their respective business continuity and disaster recovery.”

An Emergency Operations Plan (EOP) should identify and assign specific areas of responsibility for performing functions in response to an emergency or disaster. Continuity of Operations Plans (COOP) should identify and describe how essential functions will be continued and recovered in an emergency or disaster.

CS documents to address EOP and COOP are in draft state. CS is working on a Security Emergency Plan with planned implementation in 2018. These important documents should be completed in a timely fashion.

To mitigate risk, CS has a primary and an alternate SOC facility capable of coordinating and sustaining response to emergency situations, and all SOC workstations and servers are connected to Uninterrupted Power Supply.

Recommendation #6

> That Corporate Security complete the Business Continuity and Disaster Recovery Plans and a Security Emergency Plan for implementation in 2019.

Management response:

> Management agrees with this recommendation and it has been implemented.
>
> The Security and Emergency Management Emergency Plan and the Security and Emergency Management Continuity of Operations Plans were completed as part of the Office of Emergency Management’s re-accreditation process in 2018.

Audit objective #3

Systems and processes are in place to limit access to City facilities to appropriate and approved individuals; however, more oversight is required.

CS uses several tools and practices to control physical access to facilities, information and assets, access cards, facility security audits, security guards and physical security standards[2].

Access cards

The primary means to limit access to City facilities is the issuance of an approved access card. Various levels of access are issued to City employees, contractors, temporary staff, visitors, students and volunteers. An authorized Photo ID Access Card Request Form (“Request Form”) is required for initial, replacement and access modification requests. Request Forms can be submitted in person, as an attachment to an email, faxed or via internal mail. Once it is received, the photo ID clerk ensures that the form is completed properly and authorized by the appropriate supervisor. The clerk creates the cardholder’s profile in the Kantech system, adds the requested access and creates a card with the client’s photo.

The audit found that changes need to be made to current processes to ensure CS has oversight of the ID access card issuance process and that the termination of ID access cards are performed in a timely manner.

Unauthorized issuance of access ID cards and delayed cancellation of terminated access ID cards leads to inappropriate access and thereby compromises the personal safety and physical security of the City’s staff and property.

The responsibility of issuing access rights falls primarily on a single contracted commissionaire, acting as the photo ID clerk. There is very little oversight of the photo ID clerk’s day-to-day duties of issuing access cards. It should be noted that OC Transpo uses the same Kantech system, but has their own photo ID clerk who is responsible for issuing Transit’s access cards.

A key control in ensuring that access is only granted to appropriate individuals is that an Access Card Request Form must be completed, along with sign off from the appropriate supervisor as per the City’s Corporate Security Delegated Authority list prior to the issuance of an access card. Electronic Access Card Request Forms are not consistently retained within CS and difficult to locate. There is also no requirement to keep the hard copy forms. This makes it difficult to conduct spot checks to ensure that the photo ID

[2] Security standards are a documented approach to identify, apply and manage physical security measures to safeguard an organization’s staff, property and information based in facilities.

clerk is verifying that the appropriate supervisor signed off on the form prior to issuing the access card. Additionally, there are no spot checks conducted by CS.

In 2017, the photo ID clerk position had high turnover; specifically, four contracted personnel went through the position in one year. Given the use of contracted resources and the high turnover in this position, it is important for CS to have the means to exercise oversight. CS needs to know whether the incumbent photo ID clerk is enforcing the controls that have been put in place by CS.

In order for CS to have an effective tool for recording to who and when access was granted, changes are required to the current Marval system to enable future searches. CS could build an online request form, much like the Security Incident Reports that can be accessed through Ozone, the City's intranet. This would standardize the fields making it much easier to search. CS could relabel fields in the current Marvel system making it easier to categorize and locate access requests.

The audit found that of the contractor and volunteer access cards sampled, none had expiration dates programmed, and they would be active indefinitely or until CS was notified by the program area. Access cards are not always sent back to the photo ID office for destruction. Some contractors keep their cards until the next time they perform work for the City. It appears that seasonal workers and student access cards are often not terminated in a timely manner as the photo ID clerk is not informed until many months after termination. In addition, access cards may not have been collected in a timely manner by the supervisor and sent to the photo ID office for destruction. This could lead to inappropriate access to facilities and added liability to the City.

The City has 31 dual authentication readers on access doors that are considered to be "high risk". To gain access to these doors, dual authentication is required (an access card as well as a PIN code is required). Dual authentication doors are used to control access to IT data centres, SOC centres, secure file rooms, server rooms, narcotics boxes, etc.

In one instance, a secured file room door that required dual authentication was found to allow 45 persons access, while only 31 persons should have had access. CS relies on the department to notify them if a person no longer requires access and does not conduct its own assessment of whether people who currently have access are appropriate. For the two IT data centres, five card access readers have automated monthly reports generated showing staff that have access. An IT network analyst then identifies any staff that should be removed. This is a good practice that CS should consider applying to other dual access doors, as noted in Recommendation 6.

CS is able to generate reports that indicate which individuals have access to specific doors. These reports could be sent to the appropriate delegated authority annually for them to verify that the list of people with access is correct. However, given the number of doors within the City, this should be done for the more “high risk” areas.

Human Resources sends electronic transaction notifications (when an employee is terminated, retired or on a long-term leave of absence), through the Marval system, with the employee’s name and termination date. The Photo ID clerk then cancels the access cards. In 4 out of the 10 of the sampled terminations, the time between the retirement/termination date and the cancellation of the ID access card was greater than five weeks.

In one department, it was found that contractors who no longer worked on projects still had access to the front door. More concerning, a temporary full-time employee terminated on July 1, 2017 still had access to both the front door and the file room door as of November 2017, despite the fact that all the proper steps had been taken by the department.

This represents a significant a control weakness in the card termination process. Although the termination email was received and processed, there is no requirement to remove all the specific locations the individual previously had access to in Marval. Even though the card was deactivated and the ID access card was destroyed, when the employee was rehired in a different department, the employee’s profile was reactivated without removing the individual’s previous access.

The situation could be prevented in the future if at the time the access card is terminated, all the historically granted access points were “wiped clean” in the employee’s profile. This would ensure that if the profile were ever reactivated, no inappropriate access would be “preprogrammed” in their profile.

Recommendation #7

That Corporate Security improve control over the ID card and access control systems to create an effective tool for recording who, when and for how long access was granted by:

- Programming standardized fields into the system to enable future searches.
- Conducting spot checks to monitor and ensure that the photo ID clerk is verifying the delegated authority.
- Amending the Photo ID Card Policy and Procedures to require the delegated authority to provide a termination date for contractors, volunteers and seasonal employees.
- Annually initiating a risk-based review of access to doors to ensure that the list of people who have access is appropriate.
- Ensure notifications of termination are processed by Corporate Security in a timely manner.
- When an access card is terminated, removing all the individual access points the individual previously had access to. This should also be formalized in the Photo ID Card Policy and Procedures.

Management response:

Management agrees with this recommendation.

The standardization of fields and amendments to the Photo ID Card Policy and Procedures, as described in the recommendation, are complete. Additional resources are required to action the remaining Photo ID items. Two (2) additional FTEs have been included in the 2019 draft budget for consideration by Council.

Security audits

An additional means used by the City to control physical access to facilities is the conduct of security audits. Security audits are undertaken to ensure the physical security of persons and assets at City sites. The aim is to proactively identify and evaluate security risks and threats to the operation and develop a remedial action plan to address them.

Security audits are conducted using *Crime Prevention Through Environmental Design (CPTED)* Principles[3].

A risk-based approach is not used to select City facilities for security audits.

We expected to find that CS had a risk-based process to select facilities for security audits (Threat and Risk Assessment - TRA), with an annual plan to assess priority facilities. However, we found CS only performs TRAs at the request of facility and departmental managers.

A good practice would be to conduct proactive security audits at City facilities based on reported incident history and trends. However, the City has only performed security audits on 72 out of a total of 836 (9 per cent) City of Ottawa buildings in the last 9 years.

In September of 2017, CS conducted a TRA for City Hall: *Security Enhancements, Safeguarding Against Vehicular Threats*. The identified risks will be appropriately addressed once the measures identified in the drawings have been fully implemented.

The audit noted that one risk area was not considered. CS advised that this risk area will be reviewed in 2019 to assess the remaining threats in order to develop remedial security measures to reduce the risk to the facility and its occupants.

Recommendation #8

> That Corporate Security review the outstanding threats not addressed in the City Hall TRA and develop mitigation measures in order to address the risks identified.

Management response:

> Management agrees with this recommendation.
>
> A business case is in development for the procurement of a consultant in Q2 2019, subject to approval, to address these and to propose mitigation measures.

For the few security audits conducted, there is no requirement for departments to implement the recommendations of the security advisors, and it is up to departments to pay for installing any equipment recommended. We selected three facility security audits recently conducted by CS and interviewed the site manager and conducted a site visit to determine if recommendations had been implemented.

[3] CPTED principles examine how the affects of Natural Surveillance, Access Control and Territorial Reinforcement can play a role in reducing crime at a particular location.

In the case of a yard where unauthorized individuals had gained access, all the recommendations were accepted and implemented. In a second case involving a community and social support centre, all but one of the recommendations were implemented. The site manager believed the situation was long standing and very low risk so did not warrant the cost – which they would have to cover to install additional CCTV cameras. In a third case, a commercial building the City did not have control of due to a third party management agreement, none of the recommendations were implemented. This last case raises concern as to why the security audit was conducted with little likelihood of recommendations being implemented. CS needs to develop criteria for determining which facilities should be subject to security audits, with risk being the primary criteria.

We also selected three works yards and conducted unannounced site visits. There were sufficient CCTV cameras in evidence and fences were in good condition but would benefit from adding barbed wire in two locations (at time of lifecycle replacement) as chain link fence is easily climbable. Lighting was also good. At one site, City vehicles were not locked; and at one site vehicles were not locked and keys were found in the ignition of one of three trucks examined. At this last site, there was a back door that was unlocked. While the entire yard is fenced, the main gates are left open for winter operations and this can be 24 hours a day at times. Therefore, the back door would benefit from a card reader system.

We anticipated that City facilities and assets would be protected through the utilization and implementation of appropriate physical security measures. While facilities and assets are protected through the use of physical security measures such as security guards, cameras and access gates there is room for improvement.

Recommendation #9

> That Corporate Security develop a policy to ensure that recommendations emanating from facility security audits be subject to implementation.

Management response:

> Management agrees with this recommendation.
>
> Development of the policy is included in the 2019 Corporate Security work plan and, given the scope of work, will be completed by no later than Q2 2020.

Recommendation #10

That Corporate Security develop plans for risk-based, cyclical, security audits at City facilities and security awareness refresher training at yards.

Management response:

Management agrees with this recommendation.

A feasibility review is underway as part of the ongoing Security and Emergency Management Service Review, which is expected to be tabled in Q2 2019. Any funding and/or resource implications resulting from this review will be identified for inclusion in the 2020 draft budget process for consideration.

Staffing and SOC

CS has a staff of five and relies on contracted services to meet operational requirements.

The following table summarizes the cost of contracted services for 2016.

Table 3: Corporate Security contracted service costs for 2016

Service	Provider	Cost
Investigative services (five)	Keystone Investigative Services	$35,660
SOC and photo ID services	Commissionaires	$502,639
Facility security	Capital Security	$566,213
Mobile patrols	Iron Horse	$44,680
Security equipment and camera installation and maintenance	360 Advanced Security	$1,420,154
Total cost		$2,569,347

There is a Security Operations Centre that is staffed by two contracted commissionaires 24/7, and there are well-documented operating procedures in place.

Auditors visited both the primary and back-up SOC and observed the systems in operation. We observed operators responding to calls and alarms. Both sites were well organized, equipped and operated. Staff appeared to be motived, well trained and their deportment was very professional.

Guard services are contracted to provide mobile security response and alarm investigation to all City sites situated in both urban and rural areas 24 hours a day, 7 days a week. They go to sites and observe and if possible address the cause.

The City has also engaged a contractor to provide guard services at the three major administrative buildings; City Hall, Ben Franklin Place and 100 Constellation.

- City Hall: Guards are present 24/7; during periods when City Hall is open to the public, the minimum number of guards is two. Management has advised that they plan to increase to three security guards in late 2018 or early 2019. During peak hours, five guards are present. Guards do a cursory walk through of the parking garage as part of their patrol.
- Constellation: Security Guards are physically on site at Constellation from 7 am to 11 pm seven days a week.
- Ben Franklin: Guards are present from 8 am to midnight, seven days a week.

There are specific Standard Operating Procedures for City Hall, Constellation and Ben Franklin. Guards do rounds to check for intruders, fire and water leaks. The supervisor can confirm rounds are conducted by using the CCTV system.

We observed that some of the current guard staff did not present with a professional appearance. In addition, there are problems with turnover and lack of bilingual capacity. The guard staff at City Hall appears low in the off hours even after going to three guards, based on the size of the facility. There are numerous offices and doors to check; and given the building is accessible in the evening, there needs to be a thorough sweep to ensure there is no fire/safety hazards or unauthorized presence.

An in-house protective service of City employees would be preferable, at least at City Hall, to a contracted guard force so there would be a dedicated team of professional security officers to be developed and trained for future requirements. These officers could be given training in use of force to aid in security of Council meetings and training in defusing situations to manage events until OPS arrives. While this would add some cost, there would be an improvement in service and security overall at this key facility.

CS raised their own areas of concern surrounding the use of contracted services to provide key front-line security functions e.g. Security Operations Centre staff, photo ID clerk and facility security guards at City Hall. These core security services require 10 contracted guard staff, and there is a high turnover in general, with nine staff changes in the past 12 months and four different contract staff fulfilling the photo ID role.

The Study conducted by CS determined, “the majority of cities use (or are studying using) in-house security guards for some functions, such as public facing positions (such as City Hall) and routinely scheduled positions, such as Security Operations Centre staffing and issuance of photo ID cards.”

We contacted three municipalities (Mississauga, Hamilton and Vancouver) and determined that one uses a mix of in-house and contracted guard services, one is all contract and one is all in-house.

The Study also states that physical service in Ottawa receives much less funding than those in other municipalities, whether the funding is measured based on the number of facilities secured, or the size of the organizations in terms of staffing levels.

Security cameras

Cameras also play a role in limiting access to City facilities. There are approximately 1,200 cameras installed at City facilities, approximately 130 of which are at City Hall. They are for motion detection and not identification and prevention; for after the fact use to determine cause of incident. Cameras are being replaced over a four-year cycle; CS was allocated $350,000 to spend per year for four years, beginning in 2015. We were advised by CS that, at the end of the initiative, approximately 90 per cent of cameras will have been upgraded.

Factors that went into prioritizing which sites would be replaced first included:

1. Actual status – Camera Quality, Field of View, service/maintenance repair history;
2. Lifecycle – how many years of useful life was left in the camera; and
3. Analytical review of incident history and number of CCTV footage retrieval requests.

Camera analytics are used at pool facilities to identify motion/people outside of business hours. It is difficult to use analytics on other facilities because there are people moving around at all hours of the day (repair people, cleaners, etc.)

Eight general use cameras were selected for testing as well as two cameras that provided coverage to cash handling areas and two additional cameras at client service desks (point of sale).

Testing determined that cameras provide adequate coverage of key areas of most major facilities; although, the image quality of the general view cameras ranged from very sharp or good to blurry or pixilated.

During our audit work in December of 2017, we examined camera views at four locations; Walter Baker Sports Complex, Ottawa Public Library Main Branch, Cyrville Road Elections Office and Champagne Fitness Centre. Of the four client counters where cash handling occurs, the camera views were not clear enough to assess the actual cash handling. However, the volume or value of transactions processed at the client counters may not justify high-resolution cameras. It is up to management at each individual facility to decide their risk tolerance and work with CS to determine the level of monitoring they require.

As a result of the Investigation into Three Reported Client Service Centres Deposit Shortages, Tabled at Audit Committee – June 22, 2017, CS responded to the two camera related recommendations. This required that CS update the quality and angles of security video cameras at the client service centres to ensure deposit preparation is recorded and details can be seen including denominations of notes. Work included the replacement, relocation and/or the addition of digital CCTV cameras throughout the four urban client service centres.

It would still be beneficial to develop a risk-based plan to upgrade cameras in any remaining cash handling areas.

CS advised that some of the cash handling cameras could not be upgraded due to asbestos issues or there was a move in the planning stages. CS also advised that the images downloaded would be superior to the images being streamed and that available bandwidth was a factor in image quality.

We observed a cash handling camera at the Kanata administration building and found that the images were extremely sharp and could be zoomed as wanted to identify bill denominations.

We also observed footage of the Moodie nursery camera where infrared lighting was installed, rather than more physical lighting, with the result that there was better camera footage at night.

The testing supplemented our viewing of multiple cameras and their operation during the site visit to the main and back-up Security Operations Centres. Additional security cameras (six) were observed during a site visit to the Loretta Traffic Yard. This confirmed the testing results in that there were no blank screens; and images were good enough for a general view, but it would be difficult to confirm facial identity.

The City's four long-term care facilities have recently invested significantly in their Physical Security Systems (i.e. Access Control, Nurse Call systems and CCTV). The SOC has access to all exterior cameras at the long-term care facilities. The SOC does not actively monitor CCTV at long-term care; however, several cameras are available for local viewing by on-site staff.

CS has developed electronic security equipment security standards for facilities, similar to physical security standards. However, CS cannot compel branches to implement the standards; they can only recommend, as there is no policy to support their authority.

Recommendation #11

> That Corporate Security work with Supply Services to ensure that low price is not the sole basis for awarding guard contracts in order to improve overall quality of service and public impression.

Management response:

> Management agrees with this recommendation and it has been implemented.
>
> Corporate Security issued one security guard contract in 2018 and the basis of selection was best value, not lowest price. Three additional security guard solicitations are under development for 2019, each of which will also be awarded on the basis of best value.

Recommendation #12

> That the City validate the current outsourcing of Corporate Security functions by preparing a business case with all alternatives identified, costed, analyzed and compared with a resulting supported recommendation. Such an evaluation would address the potential introduction of proprietary (in-house) guard staff for high-risk activities such as City Hall facility security, ID card issuance and Security Operations Centre staffing.

Management response:

Management agrees with this recommendation.

The recommended analysis is underway as part of the ongoing Security and Emergency Management Service Review, which is expected to be tabled in Q2 2019. Some of the analysis respecting ID card issuance specifically, has been completed and two (2) additional FTEs to bring these services in-house, have been included in the 2019 draft budget for consideration by Council. Any remaining funding and/or resource implications resulting from the broader analysis will be identified for inclusion in the 2020 draft budget process for consideration.

Recommendation #13

That Corporate Security develop a risk-based plan to upgrade cameras in any remaining cash handling areas and upgrade bandwidth to improve image quality.

Management response:

Management agrees with this recommendation.

Corporate Security will consult Corporate Services to determine the risk tolerance in any remaining cash handling areas and if any camera upgrades are required. Given the number of site visits and risk assessments that are required, this will be completed by Q4 2019.

Audit objective #4

While CS has developed a Protective Measures Program (PMP), more work is necessary to ensure individual City facilities implement the program and that staff receive more training related to their security obligations.

Auditors expected to find that City employees were aware of the Protective Measures Program and that a plan was in place for implementation across all City facilities. We found that the PMP is comprehensive and that the three major administrative buildings have developed facility specific policy. However, there is no plan to ensure take up of PMP in other facilities.

In 2013, challenges were identified with regards to recruitment, retention and training of “wardens”, the volunteer staff at a facility who aid and ensure that other staff exit the facility in the event of a fire or other emergency. Many employees were participating in Mobile Workforce initiatives and were not signing up or available to act in this capacity. Consequently, Security and Emergency Management recommended that the City move from a volunteer-based program for building evacuations to a self-serve program. The self-serve program would require that employees complete an e-learning training module on fire safety and evacuation procedures, eliminating the requirement for the Emergency Warden Program.

On October 22, 2014, a series of shootings occurred at the Canadian National War Memorial and Parliament Hill compromising public safety and security. Several buildings in the downtown core, including City Hall, were placed in Secure Facility status while police searched for the shooter. An *After Action Review Report* examining the City of Ottawa's response recommended that the City establish formal procedures for threats requiring enhanced security measures such as Building Evacuation, Shelter in Place, Secure Facility and Lockdown.

The PMP defines the following protective measures, as per a best practice review:

- Building Evacuation;
- Shelter in Place;
- Secure Facility; and
- Lockdown.

Through the development of a corporate policy, security and emergency procedures for employees, facility-specific procedures and other tools and resources, the PMP aims to:

- Minimize or eliminate the risk of danger, injuries or accidents to elected officials, employees and visitors in the event of an emergency; and
- Ensure employees are aware of their individual roles and responsibilities in preparing for and responding to emergencies.

SEM required support from senior leaders in identifying a building authority for every City facility and ensuring that facility-specific procedures are developed and implemented. The new PMP policy has been posted on Ozone and communicated to City employees via email. PMP e-training is available on Ozone; however, it is not mandatory for staff. There may be challenges in getting employees to review procedures and e-learning modules.

The PMP is comprehensive, and the three major administrative buildings have developed facility-specific policy and successfully implemented the PMP.

While a PMP framework and toolkit has been developed, there is currently no schedule to target when each individual City facility plans to implement. There is also the concern as to whether there are enough resources within CS to assist in the implementation of the PMP in facilities all across the City. CS needs to develop plans to ensure employee and departmental buy-in to develop facility-specific procedures for other facilities.

Without a detailed implementation plan, it may take a long time to fully implement the PMP at all City facilities.

Auditors expected to find that City employees are occasionally made aware of their requirements in relation to compliance with policies and practices regarding physical security.

The key vehicle for this is the PMP, and there is evidence that employees are aware of their requirements in relation to compliance with policies and practices. However, there has been limited uptake for the available online PMP training, with just over 500 participants as of November 31, 2017.

PMP is admirable; however, it is intended as a plan to address a particular incident or event, and it is not mandatory for employees to familiarize themselves with the program.

It does not address the day-to-day safety/security obligations of managers and employees, much of it related to being generally aware of what is going on in your environment. Things like people found loitering, unescorted visitors, doors propped open, handling suspicious packages/mail, leaving valuable assets unattended and the rules around appropriate usage of electronic devices. Employees need to know that there may be consequences if it were to be discovered that an incident was the result of someone ignoring security procedures or policy. As part of orientation for new staff, there is a presentation that includes three slides on general corporate security, security and emergency management and safety in the workplace.

For the three municipalities we contacted, none provides significant security related information to new hires at orientation.

There needs to be a “champion” for all matters related to security within the City to ensure a sharp continuous focus on security related matters. Someone in senior management to encourage employees to be mindful of good practices and the need to do their part to ensure that employees have a safe and secure workplace.

Recommendation #14

That the City identify a senior manager (member of the executive) to “Champion” security within the organization by demonstrating management’s commitment to security. Someone who will foster security awareness amongst employees at all levels and raise the profile of security across the entire organization and help ensure that all major initiatives are considered through the lens of security.

Management response:

Management agrees with this recommendation and it has been implemented.

The General Manager of Emergency and Protective Services has been designated as the security champion, in collaboration with all members of the Senior Leadership Team.

Recommendation #15

That Corporate Security develop requirements to provide adequate information for new employee orientation to raise awareness of obligations related to security at the City, followed up with a mandatory webinar and testing within 30 days with the City.

Management response:

Management agrees with this recommendation.

Additional security-related information has already been added to new employee orientation. Corporate Security will work with the Service Innovation and Performance Department on the development of a webinar and testing no later than Q4 2019. The rollout of the eLearning module to staff will be determined at that time, based on capacity.

Recommendation #16

That Corporate Security develop a risk-based plan to monitor and ensure that a Protective Measures Program is developed by all City facilities.

Management response:

Management agrees with this recommendation.

The Protective Measures Program has been implemented and its rollout to all facilities is ongoing, based on risk. Full implementation of the recommendation would expand the scope of services offered by Corporate Security and will be considered in the context of the ongoing Security and Emergency Management Service Review, which is expected to be tabled in Q2 2019. Any funding and/or resource implications resulting from this review will be identified for inclusion in the 2020 draft budget process for consideration.

Recommendation #17

That Corporate Security develop a strategy to encourage City staff to take the online training related to the Protective Measures Program processes.

Management response:

Management agrees with this recommendation. A strategy will be completed by Q4 2019.

Appendix A – Sample data available from Corporate Security – January 1, 2016 to October 31, 2017

Sample data available from Corporate Security – January 1, 2016 to October 31, 2017

Activity	**Number**
CCTV	**258**
Footage requests	258
Client management	**266**
Consultation	106
Consultation – security equipment	41
Departmental planning	3
Education	17
Security advisor event attendance	72
Security audit/CPTED site visit	27
Electronic projects	**392**
Access control	117
Card access hardware	1
CCTV	117
Duress	18
Fire panel	41
Integrated projects	33

Activity	**Number**
Intercom	12
Intrusion	53
Incident reporting	**430**
Break and enter	12
Causing a disturbance	103
Demonstration/protest	3
Drug and alcohol on City property	20
Fraud and waste	18
Personal incidents	77
Suspicious activity	48
Theft	85
Trespassing against trespass notice	11
Vandalism	53
Report requests	**226**
Corporate Security generated	226
Grand total	**1,572**