Fisheries and Oceans Canada | Pêches et Océans Canada

Internal Audit Report

Audit of Physical Security

Project 2018-6B300

June 2019

EKME# 4073008

Canada

Table of Contents

Executive Summary

The objective of this audit was to determine whether Fisheries and Oceans Canada had implemented physical security governance and risk management processes to protect its employees and safeguard its assets. The audit examined Departmental oversight over physical security and the planning, conduct, reporting and monitoring of security assessments for Category 1 facilities.

Key Findings

Physical Security Governance

The audit found:

1) The Department is finalizing the implementation of a Safety, Security and Emergency Services Policy Committee (SSEMPC) to oversee Department-wide security policy collaboration and consultations between National Headquarters (NHQ), regional Safety, Security and Emergency Services (SSES), Canadian Coast Guard (CCG) and other sectors.
2) Physical security activity accountabilities, roles and responsibilities have been defined Department-wide. However, effective planning and collaboration and the achievement of security priorities are being limited by:
   - Inconsistent communication between the Office of the Departmental Security Officer (DSO) and regional SSES representatives to discuss and collaborate on security initiatives, priorities and plans;
   - Inadequate planning of security priorities and activities required Department-wide relative to the capacity and capability of regional SSES functions to achieve them; and
   - Inconsistent SSES operating and reporting models between NHQ and the regions.

Management of Physical Security Risks

The audit found:

1) The Department has developed a Safety, Security and Emergency Management plan that identifies and sets out strategies for managing security risk areas related to employee safety, information security, assets, and critical services delivery.
2) The Department has also developed a plan and a threat risk assessment methodology for conducting security assessments. However, the Department is not completing Category 1 facility security assessments according to its five-year plan. The methodology is not followed consistently across the regions and the results of facility security assessments are not monitored to identify risk trends or vulnerabilities that would support Department-wide physical security decision-making.

Conclusion

The audit concluded that Fisheries and Oceans Canada has implemented physical security governance and risk management processes to protect employees and safeguard assets. The audit also found opportunities to improve:

- Communication, collaboration and planning of physical security activities between NHQ, Regional Director Generals (RDGs) and regional SSES functions; and
- Monitoring of facility security assessment results to identify risk trends or vulnerabilities to support Department-wide physical security decision-making.

Statement of Conformance

This audit was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing as supported by the results of the Quality Assurance and Improvement Program of Fisheries and Ocean Canada's Internal Audit Directorate.

Introduction

This audit was initiated in accordance with the Risk-Based Audit Plan 2018–2020 for Fisheries and Oceans Canada (DFO). This is the first audit conducted by the Internal Audit Directorate (IAD) that has examined physical security governance and risk management processes within the Department.

Government security is defined in the Treasury Board *Policy on Government Security* as the assurance that information, assets and services are protected against compromise and individuals are protected against workplace violence. The Treasury Board *Operational Standard on Physical Security* provides the baseline requirements to counter physical security risks and threats to government employees, assets and service delivery.

At the Departmental level, the Safety, Security and Emergency Services (SSES) directorate coordinates security committees, develops security policies, provides strategic advice on policy implementation, and coordinates Departmental security planning, monitoring and reporting activities. The Directorate is led by the Departmental Security Officer (DSO) who reports to the Assistant Deputy Minister (ADM) of Human Resources and Corporate Services (HRCS). While SSES is the lead Departmental Directorate, awareness and understanding of the Department's security position and policies is a shared responsibility among all employees.

Why this audit is important

Physical security measures towards protecting employees, as well as safeguarding facilities, assets and information, has gained increased awareness given recent security incidents in Canada and globally. The extent to which government can ensure its own security directly affects its ability to ensure the continued delivery of services that contribute to the health, safety, economic well-being and security of Canadians. At the departmental level, it requires the effective governance and implementation of measures to ensure the security of departmental personnel, facilities, assets and information.

This audit is important for Fisheries and Oceans Canada given the over 11,000 people employed by the Department [2017-18 Departmental Results Report][1]; the value of its capital assets over $4.35 billion

[1] Fisheries and Oceans Canada, 2017-18 Departmental Results Report, Operating Context

[Financial Statements, Year ended March 31, 2018][2]; the value of its scientific research and information; its wide geographic reach; and the nature and scope of its legislated mandate.

Fisheries and Oceans Canada is the lead federal organization responsible for managing Canada's fisheries and safeguarding Canadian waters from coast to coast and the arctic. The Department's national presence spreads across six geographically dispersed regions and operates in over 400 locations including over 130 offices. The Canadian Coast Guard represents the Government of Canada's maritime sovereignty and emergency presence across three regions covering 243,000 kilometers of coastline – the longest of any country in the world. Fisheries and Oceans Canada enforces the *Fisheries Act* and other key legislation. Across all regions, fishery officers have been confronted while undertaking enforcement activities and protests have occurred at Departmental facilities. These incidents highlight the importance of physical security safeguards.

Audit Objective

The objective of this audit was to determine whether Fisheries and Oceans Canada had implemented physical security governance and risk management processes to protect its employees and its safeguard assets.

Audit Scope and Approach

The audit examined Departmental oversight over physical security and the planning, conduct, reporting and monitoring of security assessments for Category 1 facilities. The audit did not examine physical security risks related to facility design, access controls, or specific employee, asset or information security elements.

See Appendix A for Lines of Enquiry and Audit Criteria.

Audit work was carried out through:

- Interviews with Departmental Safety, Security and Emergency Service (SSES) representatives at National Headquarters (NHQ) and in all six DFO regions and all four Canadian Coast Guard regions;
- Review of Departmental governance mechanisms mandated with overseeing security, specifically the Safety, Security and Emergency Services Policy Committee (SSEMPC);
- Review of Departmental security plans;
- Review of the Department's threat and risk assessment methodology for conducting facility security assessments; and
- Fifteen (15) site visits across four DFO regions and four Coast Guard regions at selected Departmental facilities where security assessments have been completed including ten(10) which were classified as Category 1.

[2] Financial Statements of Fisheries and Oceans Canada, Year ended March 31, 2018, Statement of Financial Position (Unaudited); Non-financial assets – Tangible capital assets (Note 14)

Category 1 facilities include DFO laboratories, offices, warehouses and Coast Guard bases which have been ranked as higher risk and have therefore undergone facility security assessments as required by the Treasury Board Management Accountability Framework (MAF).

The selection of site visit locations was based upon the Department's threat risk assessment (TRA) methodology for ranking facilities. Facilities are ranked on a five-point scale ranging from very high (5) to very low (1) using risk-based classification criteria, including criticality (importance to operations), vulnerability (extent of protection, detection and response safeguards), and the number of employees. Site visits involved interviews with SSES and Real Property staff, as well as the conduct of walkthroughs of the facilities to observe security controls and the extent to which security assessment recommendations have been implemented and are being monitored.

See Appendix B for Recommendations and Management Action Plans.

Audit Findings

Physical Security Governance

Accountabilities, roles and responsibilities for physical security have been defined Department-wide.

The audit examined whether:

- Physical security accountabilities, roles and responsibilities have been defined, documented and communicated to SSES employees as required by the Treasury Board *Directive on Departmental Security*.
- The Department has adopted an integrated approach to the planning, operation and monitoring of security activities to ensure they are effectively and efficiently managed, as required by the Treasury Board *Policy on Government Security* and *Directive on Departmental Security*.

The audit found the Department's *Policy on Departmental Safety, Security and Emergency Management* and Safety, Security and Emergency Management Plan defines expected accountabilities, roles and responsibilities for NHQ and regional SSES employees.

Communication, collaboration and planning between NHQ and the regions can be improved to support the achievement of physical security priorities.

Through interviews with SSES employees in NHQ and across all regions, the audit found that effective planning and collaboration between the regions and NHQ and the achievement of security priorities are limited by:

1) Infrequent communication between the Office of the DSO and regional SSES functions to discuss and collaborate on security initiatives, priorities and plans. Monthly security teleconferences have not been scheduled consistently by the Office of the DSO; however, this was in part due to inconsistent attendance by regional SSES employees.
2) Not undertaking a strategic, Department-wide security review to assess if the current SSES operating model between NHQ and the regions can deliver on established priorities and plans relative to the existing staffing capacity and resourcing plans.

The audit also found:

a) The operating and reporting models between NHQ and regional SSES are not consistent as evidenced by the following examples:
   - SSES at NHQ has operated as a separately-funded Directorate since April 2016. However, within each region, SSES continues to operate under a merged function with Real Property;
   - No direct or functional reporting relationship exists between regional SSES employees and the Office of the DSO with regard to the planning, conduct, reporting or monitoring of facility security assessments and other critical security activities; and
   - Many regional offices do not have a dedicated, full-time security officer, resulting in split duties across multiple offices and using external resources to conduct facility security assessments, personnel screening and other security activities.

b) Year over year, regional SSES functions have been under-funded to perform security activity priorities mandated by both Regional Director Generals (RDGs) and the Office of the DSO.
   - Regional SSES employees provide security related services for Coast Guard facilities as they have no dedicated off-vessel security officers. However, neither NHQ or the Coast Guard provide additional funding support the costs of providing these services, including conducting facility security assessments.
   - To deliver on mandated security priorities, most regional SSES functions receive supplementary funding from regional Real Property budgets – a practice which, we were told is not compliant with Departmental financial management practices as it does not accurately account for the cost of SSES activities, and limits funding reallocation to other regions for Real Property priorities.

During the conduct of the audit, we noted that the Office of the DSO has undertaken two initiatives to improve collaboration between NHQ and regional SSES functions, as well as to improve SSES operations Department-wide:

1) In Fall 2018, a national SSES meeting was held at NHQ to discuss the Departmental security plan, policy updates and other security priorities. Regional SSES representatives noted that this meeting was a step towards rebuilding an effective working relationship with the Office of the DSO. For the Office of the DSO, this meeting was valuable to understand regional operational challenges with managing security priorities.

2) In Summer 2018, an external firm was contracted by the Office of the DSO to conduct an assessment of the current SSES structure, governance and decision-making practices, NHQ and regional staff distribution and competencies including the Coast Guard, and to identify training and support requirements. Assessment results are expected in Spring 2019 following NHQ consultations involving DFO, Coast Guard, RDGs and SSES representatives.

These findings are important because without an integrated approach supported by communication and collaboration, Departmental SSES activities cannot be effectively planned, coordinated and monitored, support security decision-making, and may not be consistently carried out Department-wide which could result in failure to detect and prevent security incidents.

Recommendations:

1) The Assistant Deputy Minister, Human Resources and Corporate Services, should consider undertaking a strategic Department-wide assessment of security priorities, needs and resources to better align both the NHQ and regional SSES functions.
2) The Assistant Deputy Minister, Human Resources and Corporate Services, in collaboration with Regional Director Generals, should establish formal mechanisms to improve Department-wide communication and collaboration on security initiatives, and clarify roles, responsibilities and performance expectations.

Management's Response:

Management agrees with the recommendations.

In response to Recommendation #1) the Assistant Deputy Minister, Human Resources and Corporate Services will:

- Conduct a third-party organizational review of the Safety, Security and Emergency Services Directorate (SSES) to assess national gaps in the organizational structure, governance and security competencies.
- Prepare a national costed business case to address Departmental security resource gaps including physical security identified in the third-party review above.
- Review and update physical security requirements as part of the planned refresh cycle for the Departmental Safety, Security and Emergency Management Plan (DSSEMP).
- Conduct a national prioritization exercise aligned with DSSEMP and Regional SSES functions.

In response to Recommendation #2) the Assistant Deputy Minister, Human Resources and Corporate Services will:

- Renew the SSES governance structure as outlined in the SSES Organizational Review including DG level committee and sub-working groups.
- Review and update the Policy on Departmental Safety, Security and Emergency Management including roles, responsibilities and performance expectations. This will be done in consideration of the new TBS Policy on Government Security.

A governance committee is being developed to oversee Departmental security policies, priorities and plans.

Establishing security governance is a requirement of the Treasury Board *Policy on Government Security* and *Directive on Departmental Security* and is essential to help ensure coordination and integration of all security related activities with Departmental operations, plans, priorities and functions to facilitate decision-making.

The audit examined whether the Department has established governance mechanisms to oversee security related activities, policies, priorities and plans, as well as to monitor and report on the performance of security activities.

Until recently, security discussions have occurred at the Executive table and Operations Committee. The Office of the DSO is finalizing the creation of the Safety, Security and Emergency Services Policy Committee

(SSEMPC). The Committee's mandate is to develop and maintain a coherent and integrated SSES policy suite which meets both Departmental needs and Treasury Board requirements. Beginning in Spring 2019, SSEMPC will oversee Department-wide policy collaboration and consultations between NHQ, regional SSES, Coast Guard and other sectors. It is unclear at this time whether the SSEMPC will oversee and monitor physical security related matters as one of its roles. However, the ADM-HRC and the Office of the DSO have been advised that as the Department's security governance committee, it is important that the SSEMPC oversee and monitor all relevant aspects of Departmental security, inclusive of physical security.

Management of Physical Security Risks

A Departmental security plan has been developed and is contributing to the identification and management of security related risks

The Treasury Board *Policy on Government Security* and Management Accountability Framework (MAF) requires federal departments to develop a departmental security plan to protect information, assets and services against compromise and protect individuals against workplace violence.

The audit examined whether the Department has developed and implemented a Departmental security plan, whether periodic reviews are conducted to assess effectiveness and appropriateness of the plan relative to Departmental needs, and whether the goals, strategic and control objectives of the plan are being achieved.

The audit found that the Department has met this Treasury Board requirement through the implementation of its 2018-20 Departmental Safety, Security and Emergency Services plan (DSSEMP) which identifies and sets out strategies for managing security risks related to employee safety, information security, assets, and critical services delivery. The DSSEMP is an integral component of the Department's security program to support management decision-making, and provide assurance on the effectiveness of security initiatives. The DSSEMP also identifies performance metrics, including expected results, indicators and timeline targets for each Departmental security risk area.

Responsibility for managing the DSSEMP has been delegated by the Deputy Head to the Office of the DSO who is responsible for:

- Managing the Departmental security program, as well as monitoring and annually updating the DSSEMP based on performance measurements, evaluations and risk assessments; and
- Communicating the performance metrics to the regions who are responsible for monitoring and reporting regionally and back to NHQ for annual performance reporting.

The Department has developed a plan and a threat risk assessment methodology for conducting facility security assessments.

The audit examined whether the Department has developed a plan and methodology for conducting facility security assessments to support the management of security risks.

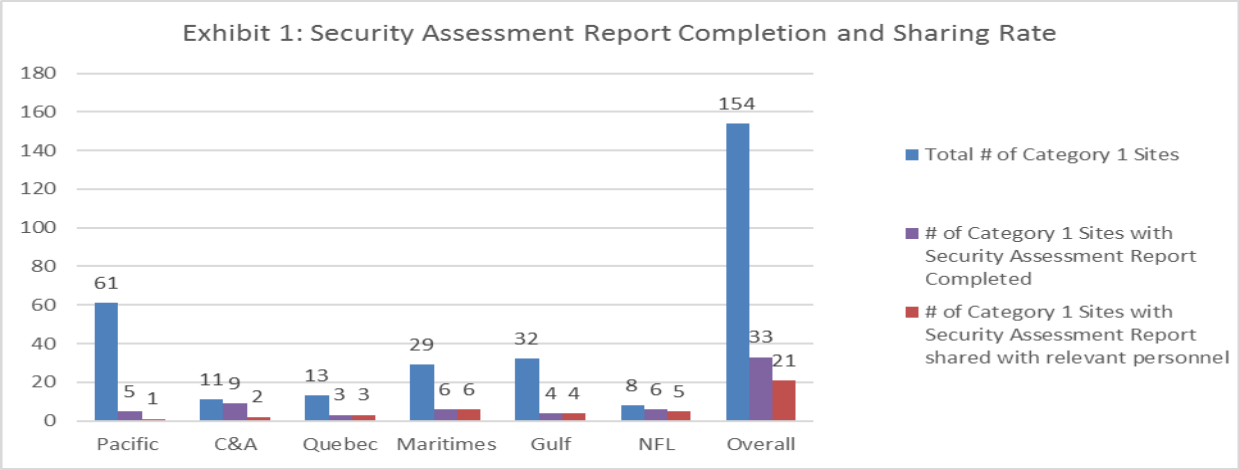
The audit found the Department has developed a five-year plan (2017-22) to conduct facility security assessments at all 154 locations classified as Category 1 facilities as part of its MAF compliance reporting strategy**.** In Summer 2017, the Department developed and communicated a new threat risk assessment (TRA) methodology to be used by all regions, consisting of risk-based criteria for classifying facilities into

categories; a revised security questionnaire for conducting facility security assessments; and a reporting tool to enter the results and track progress. It was intended that this methodology and plan would be implemented consistently across all regions.

However, the audit identified **three findings** impacting the achievement of the Department's Category 1 facility security assessment plan and the consistent use of the methodology:

1) The Department is not completing Category 1 facility security assessments according to its five-year plan

Of the 154 Category 1 facilities, security assessments have been completed for only 33 (21%). Of these 33, only 21 (64%) of security assessment reports have been shared with facility management – **See Exhibit 1.** We were told this was due to regional SSES function resource pressures and split duties of security officers across multiple regional offices to perform security activity priorities mandated by both RDGs and the Office of the DSO.



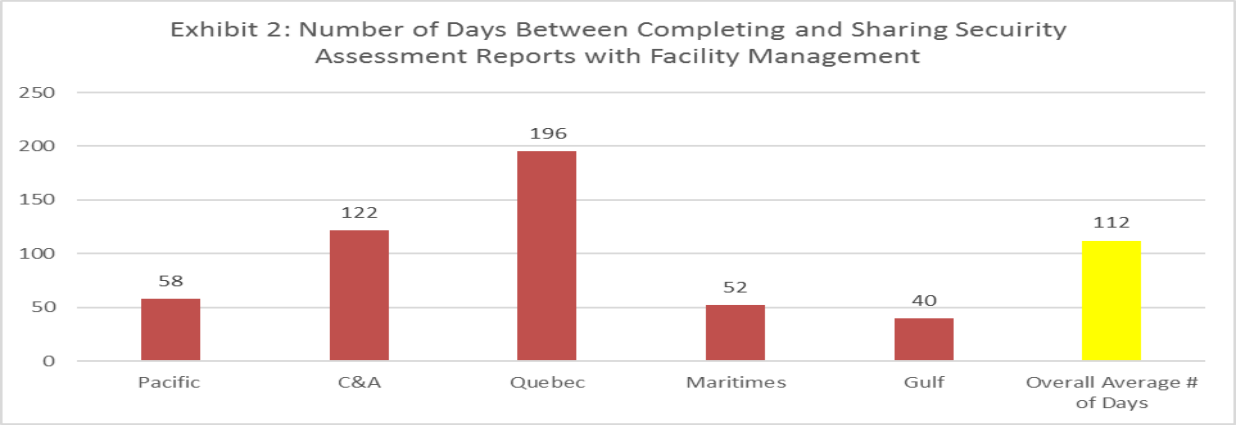
2) The Department's threat risk assessment methodology is not consistently followed across the regions.

The audit found inconsistent practices across the regions with regard to using the questionnaire to conduct Category 1 facility security assessments as well as using the reporting tool to enter their results in a timely manner. Of the ten (10) Category 1 facility security assessment reports reviewed, the audit team found:

- All 10 contained data integrity issues, resulting from missing or incomplete information entered into the reporting tool. For example, all 10 were missing recommendations for security control areas identified as non-compliant which should be automatically generated for areas of non-compliance.
- One region is using the previous TRA methodology to conduct their Category 1 facility security assessments which does not include updated questions. Therefore, results entered into the reporting tool are incomplete and will not highlight and provide recommendations for all areas of non-compliance.
- In one region, three of five completed security assessment reports were not entered into the reporting tool.

All regional security officers noted that that the TRA methodology has been communicated and training has been provided on an as needed basis on how to use the revised security assessment questionnaire and reporting tool.

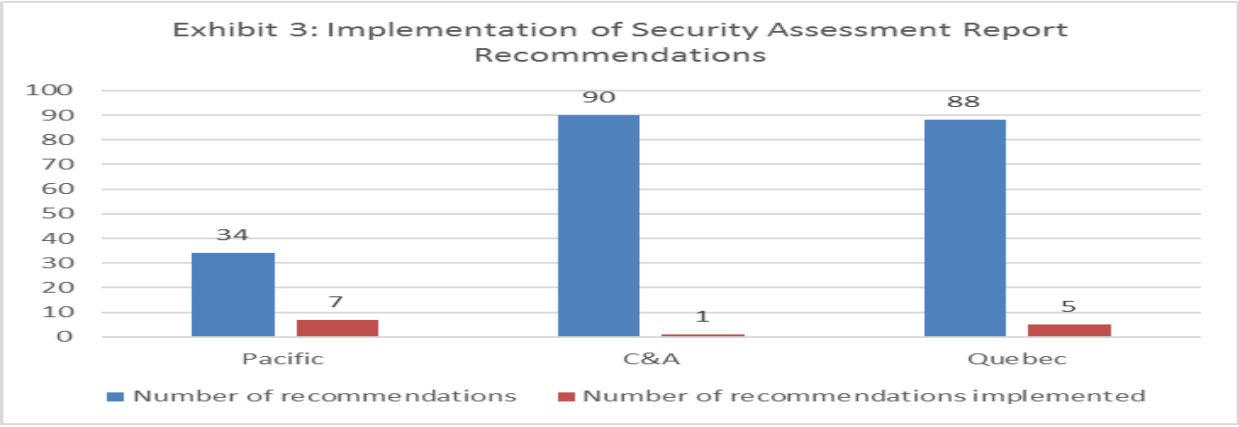
The audit also found that Department-wide, security assessments are taking on average 112 business days to complete, report and share with site management – **See Exhibit 2**. The cause of this finding was attributed to the Department having no established guidelines or timelines to require that security assessment reports are completed and shared with facility management within a specified time.



3) Results of facility security assessments are not monitored to identify risk trends or vulnerabilities to support Department-wide physical security decision-making.

Apart from reporting completion rates for MAF compliance reporting, facility security assessment report results are not monitored to identify risk trends or vulnerabilities to support Department-wide physical security decision-making. Through the review of the security assessment reporting process and the 10 facility security assessment reports, the audit team found that Department-wide:

- There is not a formal or consistent process to analyze, prioritize and monitor risk trends or vulnerabilities resulting from facility security assessment report non-compliance findings or recommendations, including office access controls, perimeter security, emergency and hazardous materials, and security awareness. The current report format does not analyze vulnerabilities resulting from non-compliance or assign a priority rating for recommendations based on risk; and
- The implementation of facility security assessment recommendations is low relative to the actual number of recommendations. Of 212 recommendations from all of the facility security assessment reports across three regions, only 13 (6.1%) have been implemented – **See Exhibit 3**.



The cause of this finding was attributed to the Department having no established process or responsibility at the Office of the DSO, for RDGs or their regional SSES functions to monitor risk trends, vulnerabilities and recommendations identified by facility security assessments to support prioritization, mitigation and monitoring plans.

The audit team noted a good practice in the Quebec and Gulf regions where a monitoring tool is used to prioritize, track and monitor implementation of recommendations for Category 1 security assessments.

Three regions are not represented in Exhibit 3 (Gulf, Maritimes and Newfoundland & Labrador). One region did not use the required security assessment methodology and was excluded. Two other regions were excluded because the audit team did not conduct site visits in these regions and did not review any completed security assessment reports.

These findings are important because significant security risks and vulnerabilities are being identified through facility security assessments. Facility security assessments provide the opportunity to prioritize, mitigate and monitor security risks and vulnerabilities in a timely manner. Without a consistent Department-wide process, security risks and vulnerabilities may not be prioritized and mitigated in a timely manner which could impact the Department's ability to protect employees and safeguard assets and information.

Recommendations:

3) The Assistant Deputy Minister, Human Resources and Corporate Services, should establish, in collaboration with RDGs:
   a) A data integrity monitoring process over information entered into the security assessment reporting tool;
   b) A monitoring process to ensure that Departmental security assessments are completed consistently;
   c) Guidelines for the completion of security assessments, entry into the reporting tool and sharing of security assessment results with site management within a reasonable timeframe; and
   d) A common process to monitor risks trends, vulnerabilities and recommendations identified by security assessments to support prioritization, mitigation and monitoring plans.

Management's Response:

Management agrees with the recommendations.

In response to Recommendation #3, the Assistant Deputy Minister, Human Resources and Corporate Services will:

- Develop a security assessment management review process (#3a & b).
- Develop a service standard for security assessment services (#3c).
- Review and update the Departmental Security Assessment Strategy (#3d), which will include:
  - A feasibility assessment to implement the new Royal Canadian Mounted Police (RCMP) information technology – threat risk assessment application; or
  - Continued development of the current Departmental security assessment information management and reporting tool.

Conclusion

The audit concluded that Fisheries and Oceans Canada has implemented physical security governance and risk management processes to protect employees and safeguard assets. The audit found opportunities to improve:

- Communication, collaboration and planning of physical security activities between NHQ, RDGs, and regional SSES functions; and
- Monitoring of facility security assessment results to identify risk trends or vulnerabilities to support Department-wide physical security decision-making.

Appendix A: Lines of Enquiry and Audit Criteria

The audit criteria were developed using the following sources:

- Treasury Board *Policy on Government Security*
- Treasury Board *Directive on Departmental Security Management*
- Treasury Board *Operational Standard on Government Security*
- Treasury Board *Security Organization and Administration Standard*

Line of Enquiry 1 – Security Governance
Criterion 1.1: Accountabilities, delegations, reporting relationships, and roles and responsibilities of Departmental employees with security responsibilities are defined, documented and communicated to relevant persons.
Criterion 1.2: Security governance mechanisms are established to ensure the coordination and integration of security activities with Departmental operations, plans, priorities and functions to facilitate decision-making.
Criterion 1.3: A Departmental security plan has been developed and implemented.
Criterion 1.4: Managers at all levels integrate security and identity management requirements into plans, programs, activities and services.
Line of Enquiry 2 – Management of Security Risks
Criterion 2.1: Processes for the systematic management of security risks have been developed, documented, implemented and maintained to ensure continuous adaptation to the changing needs of the Department and threat environment.
Criterion 2.2: A threat and risk assessment has been completed for the Department, as well as for specific facilities, areas, systems or functions.
Criterion 2.3: Periodic reviews are conducted to assess whether the Departmental security plan is effective, whether the goals, strategic objectives and control objectives of the plan are being achieved, and whether the plan remains appropriate to the needs of the Department.

Appendix B: Recommendations and Management Action Plans

Recommendations	Management Action Plan
1. The Assistant Deputy Minister, Human Resources and Corporate Services, should consider undertaking a strategic Department-wide assessment of security priorities, needs and resources to better align both the NHQ and regional SSES functions.	Conduct a third-party organizational review of the Safety, Security and Emergency Services Directorate (SSES) to assess national gaps in the organizational structure, governance and security competencies (February 2019). Prepare a national costed business case to address Departmental security resource gaps including physical security identified in the third-party review above (October 2019). Review and update physical security requirements as part of the planned refresh cycle for the Departmental Safety, Security and Emergency Management Plan (DSSEMP) (March 2020). Conduct a national prioritization exercise aligned with DSSEMP and Regional SSES functions (March 2020).
2. The Assistant Deputy Minister, Human Resources and Corporate Services, in collaboration with Regional Director Generals, should establish formal mechanisms to improve Department-wide communication and collaboration on security initiatives, and clarify roles, responsibilities and performance expectations.	Renew SSES governance structure as outlined in the SSES Organizational Review including DG level committee and sub-working groups (June 2019). Review and update the Policy on Departmental Safety, Security and Emergency Management including roles, responsibilities and performance expectations. This will be done in consideration of the new TBS Policy on Government Security (October 2020).
3. The Assistant Deputy Minister, Human Resources and Corporate Services, should establish, in collaboration with RDGs: a) A data integrity monitoring process over information entered into the security assessment reporting tool; b) A monitoring process to ensure that Departmental security assessments are completed consistently;	a) & b) Develop a security assessment management review process (March 2020). c) Develop a service standard for security assessment services (March 2020). d) Review and update the Departmental Security Assessment Strategy (December 2019). This will include:

Recommendations	Management Action Plan
c) Timelines for the completion of security assessments, entry into the reporting tool and sharing of security assessment results with site management within a reasonable timeframe; and d) A common process to monitor risks trends, vulnerabilities and recommendations identified by security assessments to support prioritization, mitigation and monitoring plans.	• A feasibility assessment to implement the new Royal Canadian Mounted Police (RCMP) information technology – threat risk assessment application, or • Continued development of the current departmental security assessment information management and reporting tool. Note: The conduct of a feasibility assessment will be dependent on the implementation timelines by the RCMP. Consideration is being given to being a participating department in the pilot project. A decision on which option to pursue should be within the next 6 months.